Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECCIÓN 5
HERRAMIENTAS PARA EL TRATAMIENTO DE LOS RIESGOS SSI

Versión 2 – 5 de febrero de 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Este documento ha sido realizado por la oficina de consultoría de la DCSSI
(SGDN / DCSSI / SDO / OCS)
en colaboración con el Club EBIOS

Rogamos nos haga llegar sus comentarios y sugerencias a la siguiente dirección
(ver formulario de recogida de comentarios que se encuentra al final del compendio):

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Histórico de las modificaciones

Versión	Motivo de la modificación	Situación
02/1997 (1.1)	Publicación de la guía para la expresión de las necesidades e identificación de los objetivos de seguridad (EBIOS).	Validado
23/01/2004	Revisión general: - Explicaciones y armonización con las normas internacionales de seguridad y de gestión de los riesgos. - Identificación del referencial reglamentario respecto al conjunto de restricciones que deben tenerse en cuenta - Integración de los conceptos de hipótesis y normas de seguridad (ISO/IEC 15408) - Transferencia de la selección de elementos esenciales al Estudio del sistema evaluado. - Perfeccionamiento de la elaboración de la escala de necesidades: los valores que representan los límites aceptables para el organismo con relación a impactos personalizados - Integración de la determinación de las necesidades por elemento en la siguiente actividad. - Integración de la determinación del modo de funcionamiento en las hipótesis. - Adaptación de los conceptos a la ISO/IEC 15408: se estudia el origen de las amenazas, es decir, los métodos de ataque y elementos peligrosos, así como sus características, que pueden incluir un tipo (natural, humano, ambiental), una causa (accidental, deliberada, afinando: en exposición, recursos disponibles, pericia, motivación), un potencial de ataque. - Identificación de los métodos de ataque no considerados. - Formalización de las amenazas, según la orientación de la ISO/IEC 15408 (elemento peligroso, ataque y bien, en forma de entidades), antes de la confrontación con las necesidades de seguridad. - Modificación de la confrontación de las amenazas con las necesidades, que permite identificar los riesgos. - Identificación de los riesgos no considerados. - Integración de la determinación de los objetivos de seguridad mínimos en las actividades de formalización de los objetivos de seguridad, y determinación de los requerimientos funcionales. - Modificación de la determinación de los objetivos de seguridad, que toma en cuenta las hipótesis, las normas de la política de seguridad, las restricciones, el referencial reglamentario y los riesgos. - Incorporación de la determinación de los niveles de seguridad, que permite determinar el nivel de los objetivos de seguridad (especialmente en función de los potenciales de ataque) y elegir un nivel de aseguramiento. - Incorporación de la determinación de los requerimientos de seguridad funcionales, que permite determinar los requerimientos funcionales que cubren los objetivos de seguridad y presentar esta cobertura. - Incorporación de la determinación de los requerimientos de seguridad de aseguramiento, que permiten determinar los eventuales requerimientos de aseguramiento. Mejoras formales, ajustes y correcciones menores (gramática, ortografía, redacción, presentaciones, coherencia...)	Validado por el Club EBIOS
05/02/2004	Publicación de la versión 2 de la guía EBIOS	Validado

Índice

1 Introducción

El método EBIOS[1] está formado por cinco secciones complementarias.

- Sección 1 – Introducción
  Esta sección presenta el contexto, el interés y la disposición del procedimiento EBIOS. También contiene una bibliografía, un glosario y presenta acrónimos.

- Sección 2 – Procedimiento
  Esta sección explica el desarrollo de las actividades del método.

- Sección 3 – Técnicas
  Esta sección propone medios para realizar las actividades del método. Será conveniente adaptar estas técnicas a las necesidades y prácticas del organismo.

- Sección 4 – Herramientas para la apreciación de los riesgos SSI
  Esta sección constituye la primera parte de la base de conocimientos del método EBIOS (tipos de entidades, métodos de ataques, vulnerabilidades).

- Sección 5 – Herramientas para el tratamiento de los riesgos SSI
  Esta sección constituye la segunda parte de la base de conocimientos del método EBIOS (objetivos de seguridad, requerimientos de seguridad, cuadros de determinación de los objetivos y requerimientos de seguridad funcionales).

El presente documento constituye la quinta sección del método.

Presenta:
- una base de objetivos de seguridad,
- una base de requerimientos de seguridad,
- cuadros que permiten determinar los objetivos de seguridad en función de los métodos de ataque y las vulnerabilidades,

cuadros que contribuyen a determinar los requerimientos de seguridad que permitirían alcanzar los objetivos de seguridad.

[1] EBIOS es una marca registrada de la Secretaría General de Defensa Nacional de Francia.

2 Objetivos de seguridad genéricos

Los objetivos de seguridad se presentan en función de los tipos de entidades. Se describen mediante un código y una denominación. Para el tipo de entidad SYS (sistema), utilizaremos los objetivos de seguridad de los otros tipos de entidades.
Aunque este conjunto de objetivos de seguridad no sea, evidentemente, exhaustivo, nos permitirá cubrir la mayor parte de los temas de SSI.
Estos objetivos de seguridad deben ajustarse para adaptarlos al contexto particular del estudio EBIOS.

2.1 MAT : Hardware

MAT_01	
Contenido	Debe existir una reserva de hardware de emergencia en caso de fallo de un equipo
MAT_02	
Contenido	Debe ser posible restaurar todo o una parte del sistema, de una aplicación, de un conjunto de datos y de trazas en caso de siniestro, fallo o negligencia
MAT_03	
Contenido	Las modificaciones moderadas del entorno (temperatura, humedad, composición del aire) no deben acarrear un comportamiento anormal de los equipos electrónicos y de los soportes de información
MAT_04	
Contenido	Debe garantizarse la integridad de lectura de los soportes de archivo durante todo el período de conservación
MAT_05	
Contenido	Los equipos y soportes de información deben poder ser nuevamente utilizados en cualquier momento y en todo tipo de condiciones, aun en condiciones excepcionales
MAT_06	
Contenido	Se debe garantizar la descripción de todos los equipos informáticos y su localización
MAT_07	
Contenido	Los equipos informáticos y los soportes de información (cartuchos de respaldo de datos, discos duros, microordenadores portátiles) deben estar protegidos contra robos
MAT_08	
Contenido	Debe ser imposible reconstituir cualquier información delicada eliminada de un soporte
MAT_09	
Contenido	El dimensionamiento del hardware debe adecuarse a los servicios que debe prestar y debe contemplar los eventuales períodos de sobrecarga
MAT_10	
Contenido	Los sistemas operativos de los equipos deben estar protegidos contra su uso por parte de personas no autorizadas
MAT_11	
Contenido	La ergonomía y la facilidad de mantenimiento deben ser tomados en cuenta para la elección del hardware, de los soportes y del software
MAT_12	
Contenido	El hardware debe estar conforme con la reglamentación en materia de higiene y

	seguridad vigente en la empresa
MAT_13	
Contenido	Se debe garantizar la supervisión y el mantenimiento del hardware aun durante el período de vacaciones, en días feriados o fuera de los horarios laborales
MAT_14	
Contenido	Debe garantizarse el respeto de los requerimientos de seguridad para la instalación, el uso y el mantenimiento del hardware
MAT_15	
Contenido	La fiabilidad debe ser tomada en cuenta para la elección del hardware, del software y de los soportes

2.2 LOG : Software

LOG_01	
Contenido	Debe garantizarse la integridad del software y de los datos debe ser garantida
LOG_02	
Contenido	Las actualizaciones del software no deben degradar ni la seguridad, ni las funcionalidades de las anteriores versiones
LOG_03	
Contenido	Todas las operaciones de actualización realizadas en el software deben estar identificadas y justificadas
LOG_04	
Contenido	La configuración de los sistemas y aplicaciones debe realizarse conforme a los requerimientos de la política de seguridad
LOG_05	
Contenido	Se debe detectar cualquier acción maliciosa o negligencia que afecte a las aplicaciones delicadas así como a los sistemas que las alojan
LOG_06	
Contenido	La puesta en servicio de una nueva herramienta debe estar precedida de una garantía de conformidad con los requerimientos de la política de seguridad
LOG_07	
Contenido	Debe existir una gestión de las licencias, de su registro y de su conservación
LOG_08	
Contenido	El organismo debe manejar el listado de las configuraciones instaladas en sus equipos y garantizar su conformidad en el tiempo
LOG_09	
Contenido	Todo software debe ser instalado conforme a los requerimientos de seguridad y debe disponer de un mantenimiento que asegure su actualización permanente
LOG_10	
Contenido	Debe ser posible analizar las trazas de las operaciones aún si éstas son generadas por diferentes sistemas (posibilidad de reconstruir la cadena de acontecimientos)
LOG_11	
Contenido	Debe existir una gestión activa de los permisos dentro de los sistemas para el procesamiento de datos en función de las necesidades de conocer y modificar la información
LOG_12	
Contenido	El uso de los medios de comunicación o de trabajo en colaboración que no satisfaga los requerimientos de la política de seguridad debe someterse a

	normas y condiciones particulares
LOG_13	
Contenido	Todo acceso a los sistemas debe estar protegido por un dispositivo de autenticación y de identificación.
LOG_14	
Contenido	Deben prevenirse los fallos o desbordamientos del rendimiento de los sistemas
LOG_15	
Contenido	Todo sistema debe poder detectar en tiempo real o a posteriori un comportamiento anormal, rastrear las operaciones realizadas e identificar a sus autores
LOG_16	
Contenido	La visualización de los datos delicados no debe constituir una falla de seguridad para la confidencialidad de los datos
LOG_17	
Contenido	El diseño del software debe apuntar a reducir los errores de uso

2.3 RES : Red

RES_01	
Contenido	Los accesos a las interfaces de comunicación deben ser protegidos contra usos maliciosos o abusos
RES_02	
Contenido	Las interfaces de comunicación deben proteger la confidencialidad, integridad y disponibilidad de las transmisiones
RES_03	
Contenido	La autenticación y el no repudio de las comunicaciones debe poder determinarse en caso de necesidad
RES_04	
Contenido	Se debe garantizar la compatibilidad de los elementos interconectados (lenguajes, husos horarios, normas...)
RES_05	
Contenido	Debe existir un plan de encaminamiento actualizado y claro
RES_06	
Contenido	Los accesos a la red deben estar previstos y controlados

2.4 PER : Personal

PER_01	
Contenido	Fuera de los locales del organismo, el personal debe garantizar la protección de los equipos y soportes de información contra robos o intrusiones
PER_02	
Contenido	El personal que tenga acceso a información delicada debe estar claramente identificado y debe ser concienciado
PER_03	
Contenido	El personal debe respetar el buen uso de las herramientas informáticas, de los medios de comunicación y la manipulación de los soportes así como las disposiciones de seguridad vinculadas con la clasificación de la información
PER_04	
Contenido	Debe existir personal polivalente para garantizar la continuidad de las tareas en

	caso de ausencia de algún miembro del personal
PER_05	
Contenido	El personal debe adherir al procedimiento de seguridad y los roles y responsabilidades deben ser claros y conocidos
PER_06	
Contenido	El personal nuevo o suplente debe poder cumplir con sus tareas respetando la política de seguridad
PER_07	
Contenido	Debe existir una separación entre los poderes de decisión, de ejecución y de control
PER_08	
Contenido	El personal debe responsabilizarse y estar informado sobre las sanciones vigentes
PER_09	
Contenido	Debe concienciarse al personal sobre el respeto del secreto profesional y la discreción
PER_10	
Contenido	Debe concienciarse y formarse al personal en el respeto de las normas del organismo
PER_11	
Contenido	El personal debe mostrar reacciones reflejas en caso de incidente (deber de información, medios de envío de informes...)
PER_12	
Contenido	El personal debe recibir formación en el uso del hardware y del software que requiere para su actividad
PER_13	
Contenido	El compromiso de la dirección en cuanto al procedimiento de la seguridad debe ser real y visible

2.5 PHY : Establecimiento

PHY_01	
Contenido	El organismo debe garantizar y controlar el aprovisionamiento de servicios esenciales (por ejemplo, electricidad, comunicación, aire acondicionado...) de buena calidad para el buen funcionamiento del hardware
PHY_02	
Contenido	El establecimiento no debe permitir la observación de datos confidenciales desde el exterior
PHY_03	
Contenido	El establecimiento y los locales del organismo deben proteger el hardware contra las agresiones, incendios, inundaciones, perturbaciones electromagnéticas...
PHY_04	
Contenido	La elección del establecimiento debe permitir limitar los riesgos (dificultad de acceso al establecimiento, inundación, incendio, contaminación, sismo, tormenta...) y considerarlos dentro de los requerimientos previos para su construcción
PHY_05	
Contenido	No debe existir posibilidad de aprovechar ninguna emisión electromagnética comprometedora desde el exterior de los locales delicados

PHY_06	
Contenido	El almacenamiento y la manipulación de material o de hardware potencialmente peligroso no debe generar riesgos para el sistema de información
PHY_07	
Contenido	El establecimiento debe estar conforme a las normas de seguridad del organismo
PHY_08	
Contenido	Se debe prohibir el consumo de tabaco, alimentos y bebidas en los locales que alojen material informático
PHY_09	
Contenido	Los locales deben estar protegidos contra el inicio y la propagación de incendios
PHY_10	
Contenido	La instalación y el uso del hardware deben realizarse conforme los estándares y normas vigentes (recomendación del fabricante, normas de la PSSI, normas de seguridad...)
PHY_11	
Contenido	Se debe planificar y controlar la instalación del hardware
PHY_12	
Contenido	Los locales y su disposición deben adaptarse a las misiones del organismo

2.6 ORG : Organización

ORG_01	
Contenido	La organización debe proteger los equipos y soportes de información contra el acceso físico de personas no autorizadas
ORG_02	
Contenido	Los procedimientos de entradas y salidas deben combatir el robo de hardware
ORG_03	
Contenido	Los medios de transmisión (según su naturaleza) y el uso de los mismos deben garantizar la protección de su contenido contra riesgos de divulgación, robo, alteración, denegación y pérdida
ORG_04	
Contenido	La organización debe hacer respetar los requerimientos de la política de seguridad en el desarrollo, el uso y la gestión de los sistemas (hardware y software)
ORG_05	
Contenido	La política de restauración debe garantizar la recuperación íntegra de las copias de seguridad, incluso luego de la evolución de los sistemas (hardware, software)
ORG_06	
Contenido	La política antivirus debe impedir la introducción y la difusión en los sistemas de cualquier código malicioso
ORG_07	
Contenido	Debe existir una política de archivado que garantice la recuperación íntegra de los datos durante todo el período fijado para su conservación
ORG_08	
Contenido	La organización debe asegurarse de respaldar todos los datos siguiendo una frecuencia adecuada (incluidos los datos no centralizados)
ORG_09	

Contenido	La organización debe adoptar una política preventiva contra la saturación y los fallos de los equipos (sistema informático, aire acondicionado, energía, comunicación)
ORG_10	
Contenido	La organización debe asegurarse de realizar una correcta gestión y un uso suficientemente seguro de las contraseñas
ORG_11	
Contenido	La política de gestión de las trazas informáticas debe asegurar su conformidad con la reglamentación vigente
ORG_12	
Contenido	La organización debe luchar contra la recepción de mensajes no solicitados (spam) y contra la desinformación, utilizando medios de comunicación interna
ORG_13	
Contenido	La organización debe asegurarse de la actualización permanente de las soluciones implementadas, teniendo en cuenta las últimas novedades en esta área y la evolución del sistema de información
ORG_14	
Contenido	Cada función vinculada con la seguridad del sistema de información (aún en caso de falta del titular) debe estar siempre bajo responsabilidad de al menos una persona que tenga los conocimientos técnicos requeridos o la posibilidad de remitirse a una documentación adecuada
ORG_15	
Contenido	La organización debe asegurarse de la identificación del carácter confidencial de toda información y de la aplicación de las normas de protección adecuadas
ORG_16	
Contenido	La organización debe garantizar que los medios de emergencia sean operativos y que aseguren, si fuese posible, la continuidad de servicio de las actividades delicadas del organismo en caso de fallo, siniestro o delito informático mayor
ORG_17	
Contenido	La organización debe asegurarse de que, en caso de incidente o de acción delictiva, se respeten las instrucciones de seguridad
ORG_18	
Contenido	La organización debe garantizar que todos respeten los requerimientos mínimos de seguridad de los sistemas de información
ORG_19	
Contenido	La organización debe implementar las medidas necesarias para impedir la presencia de personas no autorizadas en el establecimiento
ORG_20	
Contenido	La organización debe controlar la integridad y la autenticidad de los suministros (hardware, software)
ORG_21	
Contenido	La organización debe asegurar el tratamiento y el seguimiento de todo incidente de seguridad identificado en el organismo
ORG_22	
Contenido	La organización debe garantizar el control de las medidas de seguridad y su adecuación respecto de los objetivos de seguridad
ORG_23	
Contenido	La organización debe garantizar la conformidad de todos los locales con la política de seguridad (instalación de una sala técnica o informática, dispositivos de acceso al establecimiento, vigilancia de los locales, detección de incendios y

	protección contra incendios...)
ORG_24	
Contenido	La organización debe garantizar una reacción rápida y eficaz en caso de crisis, a fin de asegurar una reducción de los potenciales impactos y la continuidad de las actividades esenciales: fallos, siniestros, intrusión mayor, otros delitos informáticos
ORG_25	
Contenido	La organización debe asegurarse de que las intervenciones de personas ajenas al organismo (prestadores, suministros...) no sean fuente de riesgo para el sistema de información
ORG_26	
Contenido	La organización debe garantizar el respeto de la política de seguridad durante la aplicación de todo sistema delicado (hardware o software)
ORG_27	
Contenido	La organización debe garantizar el mantenimiento de todo hardware o software
ORG_28	
Contenido	La organización debe asegurarse la disponibilidad de la documentación técnica actualizada vinculada con todo el hardware, software e infraestructura
ORG_29	
Contenido	La organización debe adoptar una gestión de la calidad profesional conforme a las normas vigentes
ORG_30	
Contenido	La organización debe luchar contra el acceso a la información y los procesamientos de datos no autorizados
ORG_31	
Contenido	La organización de la seguridad del sistema de información debe considerar el contexto del entorno local (económico, social, político, legislativo)
ORG_32	
Contenido	La organización debe garantizar que se tengan en cuenta las necesidades de seguridad y las restricciones de uso antes y durante un desarrollo
ORG_33	
Contenido	La organización debe limitar la posibilidad de abuso de los derechos y privilegios sobre los sistemas
ORG_34	
Contenido	La organización debe asegurar al personal el acceso a las nuevas tecnologías (formación, partenariado, ..)
ORG_35	
Contenido	La organización debe asegurarse de la aplicación de una política de seguridad para la protección y del control de la información
ORG_36	
Contenido	La organización debe asegurarse de que los procedimientos utilizados sean suficientemente fluidos como para ser aplicados
ORG_37	
Contenido	La organización debe prever sanciones justas y adaptadas al contexto en caso de incumplimiento de la política de seguridad que comprometiera la seguridad del sistema de información
ORG_38	
Contenido	La organización debe asegurarse de que los subcontratistas/prestadores/proveedores/industriales/filiales/establecimientos

	respeten la política de seguridad durante sus intervenciones (trabajos, desarrollo, mantenimiento...)
ORG_39	
Contenido	La organización debe asegurarse de que las trazas y los elementos de pruebas sean gestionados y protegidos de acuerdo con la política de seguridad
ORG_40	
Contenido	La organización debe asegurarse de que el conjunto de leyes y reglamentos aplicables sean tomados en cuenta en la política de seguridad
ORG_41	
Contenido	La organización debe asegurarse de que el conjunto de normas y procedimientos aplicables esté actualizado y sea fácilmente accesible a las personas involucradas
ORG_42	
Contenido	La organización debe asegurarse de que la gestión del sistema de información sea lo más sencilla posible
ORG_43	
Contenido	Se debe verificar la ejecución de las operaciones delicadas (operaciones realizadas por más de una persona, validación, gestión sistemática de las trazas...)
ORG_44	
Contenido	Los riesgos residuales aceptados deben ser objeto de estudios específicos y, si fuera posible, debe elaborarse un plan de acción para el caso de una eventual materialización de cada riesgo residual identificado
ORG_45	
Contenido	La organización debe asegurarse de que las condiciones de trabajo sean satisfactorias

3 Requerimientos de seguridad funcionales genéricos

Los requerimientos de seguridad funcionales genéricos propuestos en esta parte han sido formulados según los siguientes referenciales:

- la [ISO 15408],
- la [ISO 17799],
- diversas fuentes (EBIOS v1, [PSSI], mejores prácticas…).

Estos requerimientos se presentan por "clase", "familia" y, eventualmente, "subfamilia", y se describen mediante un código y una denominación.
Aunque este conjunto de requerimientos no sea, evidentemente, exhaustivo, nos permitirá cubrir la mayor parte de los temas de SSI.
Estos requerimientos deberán ajustarse para adaptarlos al contexto particular del estudio EBIOS.

3.1 Requerimientos surgidos de la ISO 15408

3.1.1 FAU : Auditoría de seguridad

FAU_ARP: Respuesta automática de la auditoría de seguridad	
Alarmas de seguridad	Jerárquico de: ningún otro componente. FAU_ARP.1.1 La TSF (funciones de seguridad del TOE (objeto de evaluación)) debe iniciar [aplicación: lista de las acciones menos perturbadoras] en cuanto se detecta una potencial violación de la seguridad. Dependencias: FAU_SAA.1 Análisis de violación potencial Ejemplos: Deben iniciarse acciones para frenar dicha violación y limitar sus impactos en cuanto se detecta una potencial violación de la seguridad.
FAU_GEN: Generación de los datos de la auditoría de seguridad	
Generación de los datos de auditoría	Jerárquico de: ningún otro componente. FAU_GEN.1.1 La TSF debe poder generar un registro de auditoría de los siguientes acontecimientos auditables: a) inicio y finalización de las funciones de auditoría; b) todos los elementos auditables para el nivel de auditoría [selección: mínimo, básico, detallado, no especificado]; c) y [aplicación: otros hechos auditables específicamente definidos]. Dependencias: FPT_STM.1 Consignación fiable de fecha y hora Ejemplos: Deben poder generarse registros de auditoría para acontecimientos específicos.
Generación de los datos de auditoría	Jerárquico de: ningún otro componente. FAU_GEN.1.2 La TSF debe registrar en cada registro de auditoría, como mínimo, los siguientes datos: a) fecha y hora del acontecimiento, tipo de acontecimiento, identidad del sujeto, resultado (éxito o fracaso) del acontecimiento; b) y, por cada tipo de hecho de auditoría, sobre la base de las definiciones de hechos auditables contenidas en los componentes funcionales incluidos en el PP (perfil de protección) o el ST (objetivo de seguridad), [aplicación: otros datos de auditoría pertinentes] Dependencias: FPT_STM.1 Consignación fiable de fecha y hora

	Ejemplos: Los registros de auditoría deben incluir, como mínimo, la fecha, la hora, el tipo de hecho, la identidad del sujeto, el resultado (éxito o fracaso) del hecho, y cualquier otra información adicional necesaria previamente definida.
auditado con el usuario	Jerárquico de: ningún otro componente. FAU_GEN.2.1 La TSF debe poder asociar cada elemento auditable con la identidad del usuario que da origen al hecho. Dependencias: FAU_GEN.1 Generación de datos de auditoría FIA_UID.1 Programación de la identificación de los usuarios Ejemplos: Cada acontecimiento auditable debe poder asociarse de manera segura a la identidad del usuario que da origen al acontecimiento.
FAU_SAA: Análisis de la auditoría de seguridad	
Análisis de posible violación de la seguridad	Jerárquico de: ningún otro componente. FAU_SAA.1.1 La TSF debe poder aplicar un conjunto de normas supervisando los acontecimientos auditados e indicar, en función de dichas normas, una potencial violación de la TSP (política de seguridad del TOE). Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Deben existir normas que permitan analizar los acontecimientos auditados para detectar potenciales violaciones de la seguridad.
Análisis de posible violación de la seguridad	Jerárquico de: ningún otro componente. FAU_SAA.1.2 La TSF debe aplicar las siguientes normas para el control de los acontecimientos auditados: a) acumulación o combinación de [aplicación: subconjunto de acontecimientos auditables definidos] conocidos para indicar una potencial violación de la seguridad; b) [aplicación: todas las otras normas]. Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Los acontecimientos auditables que indican una potencial violación de la seguridad deben ser identificados como tales.
Detección de anomalía basada en un perfil	Jerárquico de: FAU_SAA.1 FAU_SAA.2.1 La TSF debe poder mantener perfiles de utilización del sistema, donde un perfil individual representa los modelos históricos de conducta de uno o varios miembros de [aplicación: el grupo en el que se centra el perfil]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Deben implementarse y mantenerse actualizados diversos perfiles de tipos de usos del sistema, que representen los modelos históricos de conducta de un grupo de usuarios.
Detección de anomalía basada	Jerárquico de: FAU_SAA.1

en un perfil	FAU_SAA.2.2 La TSF debe poder mantener un índice de representatividad asociado a cada usuario cuya actividad se registra en un perfil, donde el índice de representatividad indica el grado en que la actividad actual del usuario parece diferir de los modelos de uso establecidos representados en el perfil. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Un índice de representatividad actualizado debe asociarse a cada usuario de un perfil tipo de uso. Dicho índice debe indicar en qué grado la actividad actual del usuario difiere de los modelos de uso establecidos representados en el perfil.
Detección de anomalía basada en un perfil	Jerárquico de: FAU_SAA.1 FAU_SAA.2.3 La TSF debe ser capaz de indicar una violación inminente de la TSP cuando el índice de representatividad de un usuario supera las siguientes condiciones límite [aplicación: condiciones en las cuales una actividad anormal es identificada por la TSF]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Deben implementarse normas de análisis de los índices de representatividad a fin de detectar potenciales violaciones inminentes de la política de seguridad.
Heurísticas de ataques simples	Jerárquico de: FAU_SAA.1 FAU_SAA.3.1 La TSF debe poder mantener una representación interna de los siguientes acontecimientos característicos [aplicación: un subconjunto de acontecimientos del sistema] que pueden indicar una violación de la TSP. Dependencias: Ninguna dependencia. Ejemplos: Debe mantenerse una representación interna de acontecimientos característicos que pueden indicar una violación de la política de seguridad.
Heurísticas de ataques simples	Jerárquico de: FAU_SAA.1 FAU_SAA.3.2 La TSF debe poder comparar los acontecimientos característicos discernibles con el registro de la actividad del sistema mediante el examen de [aplicación: los datos que deben utilizarse para determinar la actividad del sistema]. Dependencias: Ninguna dependencia. Ejemplos: Es necesario identificar un conjunto de datos que hay que utilizar para determinar la actividad del sistema y compararlo con los acontecimientos característicos que pueden indicar una violación de la política de seguridad.
Heurísticas de ataques simples	Jerárquico de: FAU_SAA.1 FAU_SAA.3.3 La TSF debe ser capaz de indicar una violación inminente de la TSP cuando un acontecimiento del sistema parece corresponder a un acontecimiento característico que indica una potencial violación de la TSP. Dependencias: Ninguna dependencia. Ejemplos:

	Deben implementarse mecanismos de alarma para indicar una violación inminente de la política de seguridad cuando un acontecimiento del sistema parece corresponder a un acontecimiento característico que indica una potencial violación.
Heurística de los ataques complejos	Jerárquico de: FAU_SAA.3 FAU_SAA.4.1 La TSF debe poder mantener una representación interna de las cadenas de acontecimientos que forman parte de las siguientes situaciones de intrusión conocidas [aplicación: lista de cadenas de acontecimientos del sistema cuya frecuencia es representativa de las situaciones de intrusión conocidas] y los siguientes acontecimientos característicos [aplicación: un subconjunto de acontecimientos del sistema] que pueden indicar una potencial violación de la TSP. Dependencias: Ninguna dependencia. Ejemplos: Debe mantenerse una representación interna de cadenas de acontecimientos que forman parte de situaciones de intrusión conocidas y de acontecimientos característicos.
Heurística de los ataques complejos	Jerárquico de: FAU_SAA.3 FAU_SAA.4.2 La TSF debe poder comparar los acontecimientos característicos discernibles con el registro de la actividad del sistema mediante el examen de [aplicación: los datos que deben utilizarse para determinar la actividad del sistema]. Dependencias: Ninguna dependencia. Ejemplos: Los datos utilizados para determinar la actividad del sistema deben compararse con los acontecimientos característicos y con las cadenas de acontecimientos.
Heurística de los ataques complejos	Jerárquico de: FAU_SAA.3 FAU_SAA.4.3 La TSF debe ser capaz de indicar una violación inminente de la TSP cuando la actividad del sistema parece corresponder a un acontecimiento característico que indica una potencial violación de la TSP. Dependencias: Ninguna dependencia. Ejemplos: Deben implementarse mecanismos de alarma para indicar una violación inminente de la política de seguridad cuando varios acontecimientos del sistema parecen corresponder a una cadena de acontecimientos que indica una potencial violación.
FAU_SAR: Revisión de la auditoría de seguridad	
Revisión de auditoría	Este componente otorga a los usuarios autorizados la capacidad de obtener e interpretar los datos. Cuando se trate de usuarios humanos (personas), dichos datos deberán presentarse de tal modo que les resulten comprensibles. Cuando se trate de entidades de TI externas, los datos deberán presentarse, sin ambigüedad, en un formato electrónico. Jerárquico de: ningún otro componente. FAU_SAR.1.1 La TSF debe ofrecer a [aplicación: usuarios autorizados] la capacidad de leer [aplicación: lista de datos de auditoría] a partir de los registros de auditoría.

	Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Los usuarios autorizados deben tener la capacidad de consultar los datos de las auditorías a partir de los registros de auditoría.
Revisión de auditoría	Este componente otorga a los usuarios autorizados la capacidad de obtener e interpretar los datos. Cuando se trate de usuarios humanos (personas), dichos datos deberán presentarse de tal modo que les resulten comprensibles. Cuando se trate de entidades de TI externas, los datos deberán presentarse, sin ambigüedad, en un formato electrónico. Jerárquico de: ningún otro componente. FAU_SAR.1.2 La TSF debe presentar los registros de auditoría de tal modo que permita al usuario interpretarlos. Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Los registros de auditoría deben presentarse de tal modo que permita al usuario interpretarlos.
Revisión restringida de auditoría	Jerárquico de: ningún otro componente. FAU_SAR.2.1 La TSF debe impedir a todos los usuarios el derecho de acceso en modo lectura a los registros de auditoría, con excepción de aquellos a quienes se ha otorgado un derecho de lectura explícito. Dependencias: FAU_SAR.1 Revisión de auditoría. Ejemplos: El derecho de acceso en modo lectura a los registros de auditoría debe negarse a todos los usuarios, con excepción de aquellos a quienes se ha otorgado un derecho de lectura específico.
Revisión selectiva de auditoría	Jerárquico de: ningún otro componente. FAU_SAR.3.1 La TSF debe ofrecer la capacidad de efectuar [selección: búsquedas, clasificaciones, ordenamientos] de datos de autoría en función de [aplicación: criterios vinculados lógicamente]. Dependencias: FAU_SAR.1 Revisión de auditoría. Ejemplos: Deben definirse criterios vinculados lógicamente dentro de los datos de auditoría de tal modo que puedan efectuarse búsquedas, clasificaciones y ordenamientos de los datos de auditoría.
FAU_SEL: Selección de los acontecimiento de la auditoría de seguridad	
Auditoría selectiva	Jerárquico de: ningún otro componente. FAU_SEL.1.1 La TSF debe poder incluir o excluir acontecimientos auditables del conjunto de acontecimientos auditados, en función de los siguientes atributos: a) [selección: identidad del objeto, identidad del usuario, identidad del sujeto, identidad del servidor, tipo de acontecimiento] b) [aplicación: lista de los atributos adicionales en los cuales se basa la selectividad de la auditoría]. Dependencias: FAU_GEN.1 Generación de datos de auditoría FMT_MTD.1 Gestión de los datos de la TSF

	Ejemplos: Deben poder excluirse algunos acontecimientos auditables de los acontecimientos auditados, en función de la identidad del objeto, del usuario, del sujeto o del servidor, del tipo de acontecimiento o de otros atributos en los cuales se basa la selectividad de la auditoría.
FAU_STG: Almacenamiento de los acontecimientos de la auditoría de seguridad	
Almacenamiento protegido del registro de la auditoría	Jerárquico de: ningún otro componente. FAU_STG.1.1 La TSF debe proteger los registros de auditoría almacenados para que no sean eliminados sin autorización. Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Los registros de auditoría almacenados deben estar protegidos para que no sean suprimidos sin autorización.
Almacenamiento protegido del registro de la auditoría	Jerárquico de: ningún otro componente. FAU_STG.1.2 La TSF debe poder [selección: impedir, detectar] las modificaciones realizadas en los registros de auditoría. Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Las modificaciones efectuadas en los registros de auditoría deben poder detectarse y/o impedirse.
Garantías de disponibilidad de los datos de auditoría	Jerárquico de: FAU_STG.1 FAU_STG.2.1 La TSF debe proteger los registros de auditoría almacenados para que no sean eliminados sin autorización. FAU_STG.2.2 La TSF debe poder [selección: impedir, detectar] las modificaciones realizadas en los registros de auditoría. FAU_STG.2.3 La TSF debe garantizar que [aplicación: métrica para el respaldo de los registros de auditoría] de los registros de auditoría se mantendrá cuando se presenten las siguientes condiciones: [selección: superación de la capacidad de almacenamiento de datos de auditoría, falla, ataque]. Dependencias: FAU_GEN.1 Generación de datos de auditoría Ejemplos: Debe mantenerse un porcentaje (definir) de registros de auditoría, en caso de que se supere la capacidad de almacenamiento de los datos de auditoría, o en caso de falla o ataque.
Acción en caso de eventual pérdida de datos de auditoría	Jerárquico de: ningún otro componente. FAU_STG.3.1 La TSF debe iniciar [aplicación: acciones que debe iniciar en caso de posible falla en el almacenamiento de la auditoría] si el registro de auditoría supera [aplicación: límite predefinido]. Dependencias: FAU_STG.1 Almacenamiento protegido del registro de la auditoría. Ejemplos:

	Deben preverse las acciones que se implementarán si los registros de auditoría superan el tamaño límite predefinido (definir).
Prevención de las pérdidas de datos de auditoría	Jerárquico de: FAU_STG.3 FAU_STG.4.1 Si el registro de auditoría está completo, la TSF debe [selección: "ignorar los acontecimientos auditables", "impedir los acontecimientos auditables que no sean aquellos generados por el usuario autorizado que cuenta con derechos especiales", "sobreescribir los registros de auditoría más antiguos"] y [aplicación: otras acciones que deben iniciarse en caso de falla del almacenamiento de los datos de la auditoría]. Dependencias: FAU_STG.1 Almacenamiento protegido del registro de la auditoría. Ejemplos: Deben definirse las medidas que se implementarán si se alcanza el límite de capacidad de almacenamiento de los datos de auditoría (por ejemplo, ignorar los acontecimientos auditables o sobreescribir los registros de auditoría más antiguos).

3.1.2 FCO : Comunicación

FCO_NRO: No repudio del origen	
Prueba selectiva del origen	Jerárquico de: ningún otro componente. FCO_NRO.1.1 La TSF debe poder generar la prueba del origen de los [aplicación: lista de los tipos de datos] transmitidos a pedido del [selección: emisor, destinatario, [aplicación: lista de terceros]]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: La prueba del origen de los datos transmitidos debe poder generarse a pedido del emisor, del destinatario o de terceras personas (identificar).
Prueba selectiva del origen	Jerárquico de: ningún otro componente. FCO_NRO.1.2 La TSF debe poder establecer un vínculo entre los [aplicación: lista de los atributos] del emisor de los datos y los [aplicación: lista de los campos de información] de los datos a los cuales se aplica la prueba. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Debe poder establecerse un vínculo entre los atributos del emisor de los datos y los campos de información de los datos a los cuales se aplica la prueba.
Prueba selectiva del origen	Jerárquico de: ningún otro componente. FCO_NRO.1.3 La TSF debe ofrecer al [selección: emisor, destinatario, [aplicación: lista de terceros]] la capacidad de verificar la prueba del origen de los datos, considerando [aplicación: limitaciones referidas a la prueba del origen]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: El emisor, el destinatario o terceros (identificar) deben tener la posibilidad de verificar la prueba del origen de los datos, considerando las limitaciones referidas a dicha prueba del origen.

Prueba sistemática del origen	Jerárquico de: FCO_NRO.1 FCO_NRO.2.1 La TSF debe implementar la generación de la prueba del origen en cualquier momento para [aplicación: lista de los tipos de datos] transmitidos. FCO_NRO.2.2 La TSF debe poder establecer un vínculo entre los [aplicación: lista de los atributos] del emisor de los datos y los [aplicación: lista de los campos de información] de los datos a los cuales se aplica la prueba. FCO_NRO.2.3 La TSF debe ofrecer al [selección: emisor, destinatario, [aplicación: lista de terceros]] la capacidad de verificar la prueba del origen de los datos, considerando [aplicación: limitaciones referidas a la prueba del origen]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: La prueba del origen debe generarse en cualquier momento para ciertos tipos de datos transmitidos (definir).
FCO_NRR: No repudio de la recepción	
Prueba selectiva de la recepción	Jerárquico de: ningún otro componente. FCO_NRR.1.1 La TSF debe poder generar la prueba de la recepción de los [aplicación: lista de los tipos de datos] recibidos a pedido del [selección: emisor, destinatario, [aplicación: lista de terceros]]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: La prueba de la recepción de los datos transmitidos debe poder generarse a pedido del emisor, del destinatario o de terceras personas (identificar).
Prueba selectiva de la recepción	Jerárquico de: ningún otro componente. FCO_NRR.1.2 La TSF debe poder establecer un vínculo entre los [aplicación: lista de los atributos] del destinatario de los datos y los [aplicación: lista de los campos de información] de los datos a los cuales se aplica la prueba. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Debe poder establecerse un vínculo entre los atributos del destinatario de los datos y los campos de información de los datos a los cuales se aplica la prueba.
Prueba selectiva de la recepción	Jerárquico de: ningún otro componente. FCO_NRR.1.3 La TSF debe ofrecer al [selección: emisor, destinatario, [aplicación: lista de terceros]] la capacidad de verificar la prueba de la recepción de los datos, considerando [aplicación: limitaciones referidas a la prueba de la recepción]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: El emisor, el destinatario o terceros (identificar) deben tener la posibilidad de verificar la prueba de la recepción de los datos, considerando las limitaciones referidas a dicha prueba de la recepción.
Prueba sistemática de la	Jerárquico de: FCO_NRR.1

recepción	FCO_NRR.2.1 La TSF debe implementar la generación de la prueba de la recepción en cualquier momento para los [aplicación: lista de los tipos de datos] recibidos. FCO_NRR.2.2 La TSF debe poder establecer un vínculo entre los [aplicación: lista de los atributos] del destinatario de los datos y los [aplicación: lista de los campos de información] de los datos a los cuales se aplica la prueba. FCO_NRR.2.3 La TSF debe ofrecer al [selección: emisor, destinatario, [aplicación: lista de terceros]] la capacidad de verificar la prueba de la recepción de los datos, considerando [aplicación: limitaciones referidas a la prueba de la recepción]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: La prueba de la recepción debe generarse en cualquier momento para ciertos tipos de datos transmitidos (definir).

3.1.3 FCS : Soporte criptográfico

FCS_CKM: Gestión de claves criptográficas	
Génération de clés cryptographiques	Hiérarchique à : aucun autre composant. FCS_CKM.1.1 La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [affectation : algorithme de génération de clés cryptographiques] et à des tailles de clés cryptographiques spécifiées [affectation : tailles des clés cryptographiques] qui satisfont à ce qui suit : [affectation : liste des normes]. Dépendances : [FCS_CKM.2 Distribution de clés cryptographiques ou FCS_COP.1 Opération cryptographique] FCS_CKM.4 Destruction de clés cryptographiques FMT_MSA.2 Attributs de sécurité sûrs Exemples Les clés cryptographiques doivent être générées conformément un algorithme de génération de clés cryptographiques spécifiques (définir) et des tailles de clés cryptographiques spécifiées (à définir) qui satisfont des normes identifiées (à définir)
Distribution de clés cryptographiques	Hiérarchique à : aucun autre composant. FCS_CKM.2.1 La TSF doit distribuer les clés cryptographiques conformément à une méthode de distribution de clés cryptographiques spécifiée [affectation : méthode de distribution de clés cryptographiques] qui satisfait à ce qui suit : [affectation : liste des normes]. Dépendances : [FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité ou FCS_CKM.1 Génération de clés cryptographiques] FCS_CKM.4 Destruction de clés cryptographiques FMT_MSA.2 Attributs de sécurité sûrs Exemples Les clés cryptographiques doivent être distribuées conformément une méthode de distribution de clés cryptographiques spécifiée (définir) qui satisfait des normes identifiées (définir)
Accès aux clés cryptographiques	Hiérarchique à : aucun autre composant.

	FCS_CKM.3.1 La TSF doit réaliser [affectation : type d'accès aux clés cryptographiques] conformément à une méthode d'accès aux clés cryptographiques spécifiée [affectation : méthode d'accès aux clés cryptographiques] qui satisfait à ce qui suit : [affectation : liste des normes]. Dépendances : [FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité ou FCS_CKM.1 Génération de clés cryptographiques] FCS_CKM.4 Destruction de clés cryptographiques FMT_MSA.2 Attributs de sécurité sûrs Exemples Les types d'accès aux clés cryptographiques doivent être conformes une méthode d'accès aux lés cryptographiques spécifiée (définir) qui satisfait des normes identifiées (définir)
Destruction de clés cryptographiques	Hiérarchique à : aucun autre composant. FCS_CKM.4.1 La TSF doit détruire les clés cryptographiques conformément à une méthode de destruction de clés cryptographiques spécifiée [affectation : méthode de destruction de clés cryptographiques] qui satisfait à ce qui suit : [affectation : liste des normes]. Dépendances : [FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité ou FCS_CKM.1 Génération de clés cryptographiques] FMT_MSA.2 Attributs de sécurité sûrs Exemples Les clés cryptographiques doivent être détruites conformément une méthode de destruction de clés cryptographiques (à définir) qui satisfait des normes identifi es (d finir)
FCS_COP: Operación criptográfica	
Operación criptográfica	Jerárquico de: ningún otro componente. FCS_COP.1.1 La TSF debe ejecutar [aplicación: lista de operaciones criptográficas] conforme a un algoritmo criptográfico [aplicación: algoritmo criptográfico] y respetando tamaños específicos de claves criptográficas [aplicación: tamaños de las claves criptográficas] que cumplan con lo siguiente: [aplicación: lista de las normas]. Dependencias: [FDP_ITC.1 Importación de datos del usuario sin atributos de seguridad o FCS_CKM.1 Generación de claves criptográficas]FCS_CKM.4 Destrucción de claves criptográficasFMT_MSA.2 Atributos de seguridad protegidos Ejemplos: Las operaciones criptográficas deben ejecutarse conforme a un algoritmo criptográfico (definir) y respetando tamaños específicos de claves criptográficas (definir), que cumplan con normas identificadas (definir).

3.1.4 FDP : Protección de los datos del usuario

FDP_ACC: Política de control de acceso	
Control de acceso parcial	Jerárquico de: ningún otro componente. FDP_ACC.1.1 La TSF debe aplicar la [aplicación: SFP (política de seguridad) de control de acceso] a los [aplicación: lista de los sujetos, objetos y operaciones sobre los sujetos y objetos cubiertos por la SFP]. Dependencias: FDP_ACF.1 Control de acceso basado en los atributos de

	seguridad Ejemplos: Para un control de acceso parcial, debe aplicarse la política de seguridad para los controles de acceso a los sujetos, objetos y operaciones efectuadas sobre los sujetos y objetos identificados cubiertos por la política de seguridad (definir).
Control de acceso completo	Jerárquico de: FDP_ACC.1 FDP_ACC.2.1 La TSF debe aplicar la [aplicación: SFP de control de acceso] a los [aplicación: lista de los sujetos y objetos] y a todas las operaciones sobre los sujetos y objetos cubiertos por la SFP. Dependencias: FDP_ACF.1 Control de acceso basado en los atributos de seguridad Ejemplos: Para un control de acceso completo, debe aplicarse la política de seguridad para los controles de acceso a los sujetos, objetos (definir) y todas las operaciones efectuadas sobre los sujetos y objetos identificados cubiertos por la política de seguridad.
Control de acceso completo	Jerárquico de: FDP_ACC.1 FDP_ACC.2.2 La TSF debe garantizar que todas las operaciones entre cualquier sujeto del TSC (alcance del control de la TSF) y cualquier objeto del TSC están cubiertas por una SFP de control de acceso. Dependencias: FDP_ACF.1 Control de acceso basado en los atributos de seguridad Ejemplos: Para un control de acceso completo, todas las operaciones entre cualquier sujeto y cualquier objeto del objetivo están cubiertos por la política de seguridad para los controles de acceso.
FDP_ACF: Funciones de control de acceso	
Control de acceso basado en los atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ACF.1.1 La TSF debe aplicar la [aplicación: SFP de control de acceso] a los objetos basándose en [aplicación: atributos de seguridad, grupos de atributos de seguridad designados]. Dependencias: FDP_ACC.1 Control de acceso parcial FMT_MSA.3 Inicialización estática de atributos Ejemplos: Para un control de acceso basado en los atributos de seguridad, debe aplicarse la política de seguridad para los controles de acceso a los objetos, basándose en atributos de seguridad o grupos de atributos de seguridad (definir).
Control de acceso basado en los atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ACF.1.2 La TSF debe aplicar las siguientes normas para determinar si una operación entre sujetos controlados y objetos controlados está autorizada: [aplicación: normas que rigen los accesos a los sujetos controlados y a los objetos controlados utilizando operaciones controladas sobre objetos controlados]. Dependencias: FDP_ACC.1 Control de acceso parcial FMT_MSA.3 Inicialización estática de atributos

	Ejemplos: Para un control de acceso basado en los atributos de seguridad, deben aplicarse las normas que rigen los accesos a los sujetos controlados y a los objetos controlados que utilizan operaciones controladas sobre objetos controlados deben aplicarse siempre .
Control de acceso basado en los atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ACF.1.3 La TSF debe autorizar explícitamente el acceso de los sujetos a los objetos, en función de las siguientes normas complementarias: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente al acceso de los sujetos a los objetos]. Dependencias: FDP_ACC.1 Control de acceso parcial FMT_MSA.3 Inicialización estática de atributos Ejemplos: Para un control de acceso basado en los atributos de seguridad, el acceso de los sujetos a los objetos debe estar explícitamente autorizado, en función de normas complementarias que autoricen explícitamente estos accesos (definir).
Control de acceso basado en los atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ACF.1.4 La TSF debe negar explícitamente el acceso de los sujetos a los objetos, en función de [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente el acceso de determinados sujetos a determinados objetos]. Dependencias: FDP_ACC.1 Control de acceso parcial FMT_MSA.3 Inicialización estática de atributos Ejemplos: Para un control de acceso basado en los atributos de seguridad, el acceso de determinados sujetos a determinados objetos debe ser explícitamente rechazado, en función de normas complementarias que prohíban explícitamente dichos accesos (definir).
FDP_DAU: Autenticación de datos	
Autenticación básica de datos	Jerárquico de: ningún otro componente. FDP_DAU.1.1 La TSF debe ofrecer la capacidad de generar una prueba que pueda ser utilizada como garantía de validez de [aplicación: lista de los objetos o tipos de datos]. Dependencias: Ninguna dependencia. Ejemplos: Los sujetos identificados (definir) deben tener la posibilidad de verificar la prueba de validez de los datos indicados (definir).
Autenticación básica de datos	Jerárquico de: ningún otro componente. FDP_DAU.1.1 La TSF debe ofrecer la capacidad de generar una prueba que pueda ser utilizada como garantía de validez de [aplicación: lista de los objetos o tipos de datos]. Dependencias: Ninguna dependencia. Ejemplos:

	Debe ser posible generar una prueba que pueda utilizarse como garantía de la validez de objetos o de tipos de datos (definir).
Autenticación básica de datos **Autenticación de datos con identidad del garante**	Jerárquico de: FDP_DAU.1 FDP_DAU.2.2 La TSF debe ofrecer a las [aplicación: lista de los sujetos] la aptitud para verificar la prueba de validez de los datos indicados y la identidad del usuario que ha generado la prueba. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos: Para una autenticación con identidad del garante, los sujetos identificados (definir) deben tener la posibilidad de verificar la prueba de validez de los datos indicados (definir) y la identidad del usuario que ha generado la prueba.
FDP_ETC: Exportación hacia una zona fuera del control de la TSF	
Exportación de datos del usuario sin atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ETC.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la exportación de datos del usuario, controlados por la o las SFP, fuera del TSC. FDP_ETC.1.2 La TSF debe exportar los datos del usuario sin los atributos de seguridad asociados a dichos datos. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos: Para una exportación de datos sin atributos de seguridad, los datos del usuario deben exportarse sin los atributos de seguridad asociados a dichos datos.
Exportación de datos del usuario sin atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ETC.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la exportación de datos del usuario, controlados por la o las SFP, fuera del TSC. FDP_ETC.1.2 La TSF debe exportar los datos del usuario sin los atributos de seguridad asociados a dichos datos. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos: Las políticas de seguridad para los controles de acceso y para los controles de flujo de datos deben aplicarse durante la exportación de datos del usuario, controlados por la política de seguridad, fuera del área de seguridad.
Exportación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ETC.2.1 La TSF debe aplicar la o las SFP [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la exportación de datos del usuario, controlados por la o las SFP, fuera del TSC. FDP_ETC.2.2 La TSF debe exportar los datos del usuario con los atributos de seguridad asociados a dichos datos. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información]

	Ejemplos: Para una exportación de datos con atributos de seguridad, los datos del usuario deben exportarse con los atributos de seguridad asociados a dichos datos.
Exportación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ETC.2.3 La TSF debe garantizar que los atributos de seguridad, cuando son exportados fuera del TSC, están asociados sin ambigüedad a los datos del usuario exportados. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos: La asociación sin ambigüedad de los atributos de seguridad a los datos del usuario debe garantizarse cuando estos son exportados.
Exportación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ETC.2.4 La TSF debe aplicar las siguientes normas durante la exportación de datos del usuario provenientes del TSC: [aplicación: normas complementarias de control de exportación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos: Las normas complementarias de control de exportación (definir) deben aplicarse durante la exportación de los datos del usuario hacia fuera del área de seguridad.
FDP_IFC: Política de control de flujo de datos	
Control parcial del flujo de datos	Jerárquico de: ningún otro componente. FDP_IFC.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] a los [aplicación: lista de los sujetos, datos y operaciones cubiertos por la SFP que desencadenan la transferencia de datos controlados hacia o a partir de sujetos controlados]. Dependencias: FDP_IFF.1 Atributos de seguridad simples Ejemplos: Para realizar un control parcial del flujo de datos, la política de seguridad para el control de flujo de datos debe aplicarse a los sujetos, datos y operaciones que desencadenan la transferencia hacia y desde sujetos controlados.
Control completo del flujo de datos	Jerárquico de: FDP_IFC.1 FDP_IFC.2.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] a los [aplicación: lista de los sujetos y datos] y a todas las operaciones cubiertas por la SFP que desencadenan la transferencia de dichos datos hacia o a partir de sujetos. Dependencias: FDP_IFF.1 Atributos de seguridad simples Ejemplos: Para realizar un control completo del flujo de datos, la política de seguridad para el control del flujo de datos debe aplicarse a los sujetos, a los datos y a todas las operaciones que desencadenen la transferencia hacia y desde sujetos controlados.

Control completo del flujo de datos	Jerárquico de: FDP_IFC.1 FDP_IFC.2.2 La TSF debe garantizar que todas las operaciones que desencadenan la transferencia de un dato cualquiera del TSC hacia o a partir de cualquier sujeto del TSC están cubiertas por una SFP de control del flujo de información. Dependencias: FDP_IFF.1 Atributos de seguridad simples Ejemplos: Para realizar un control completo del flujo de datos, todas las operaciones que desencadenan una transferencia de datos hacia o desde cualquier sujeto del área de seguridad deben estar cubiertas por una política de seguridad para el control de los flujos.
FDP_IFF: Funciones de control del flujo de datos	
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: Para atributos de seguridad simples, un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada debe autorizarse en función de normas basadas en los atributos de seguridad (definir).
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas

	en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: La política de seguridad de control de flujo de datos debe aplicarse en función de una cantidad mínima de atributos de seguridad identificados (definir).
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: Deben aplicarse las normas complementarias de la política de seguridad para el control del flujo (definir).
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de

	sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: Debe proporcionarse una lista de las capacidades adicionales de la política de seguridad (definir).
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos:

	Un flujo de datos debe ser explícitamente autorizado en función de normas basadas en los atributos de seguridad que autoricen explícitamente los flujos de información (definir).
Atributos de seguridad simples	Jerárquico de: ningún otro componente. FDP_IFF.1.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] en función de los siguientes tipos de atributos de seguridad de sujetos y datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.1.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si se aplican las siguientes normas: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.1.3 La TSF debe aplicar las [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.1.4 La TSF debe ofrecer lo siguiente [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.1.5 La TSF debe autorizar explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.1.6 La TSF debe prohibir explícitamente un flujo de información en función de las siguientes normas: [aplicación: normas basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: Un flujo de datos debe ser explícitamente prohibido en función de normas basadas en los atributos de seguridad que prohíban explícitamente los flujos de información (definir).
Atributos de seguridad jerárquicos	Jerárquico de: FDP_IFF.1 FDP_IFF.2.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] sobre la base de los siguientes tipos de atributos de seguridad del sujeto y de los datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.2.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si las siguientes normas, basadas en las relaciones ordenadas entre los atributos de seguridad, se aplican: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.2.3 La TSF debe aplicar la [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.2.4 La TSF debe ofrecer las [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.2.5 La TSF debe autorizar explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información].

	FDP_IFF.2.6 La TSF debe prohibir explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. FDP_IFF.2.7 La TSF debe aplicar las siguientes relaciones para cada par válido de atributos de seguridad de control del flujo de información: a) existe una función de ordenación tal que, dados dos atributos de seguridad válidos, determina si los atributos de seguridad son idénticos, si uno de los atributos de seguridad es superior al otro o si los atributos de seguridad no son comparables; y b) existe un "límite superior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que es superior o igual a los dos atributos de seguridad válidos; y c) existe un "límite inferior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que no es superior a los dos atributos de seguridad válidos. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos: Para atributos de seguridad jerárquicos, un flujo de información entre un sujeto y datos controlados mediante una operación controlada debe autorizarse según normas basadas en las relaciones ordenadas entre atributos de seguridad (definir).
Atributos de seguridad jerárquicos	Jerárquico de: FDP_IFF.1 FDP_IFF.2.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] sobre la base de los siguientes tipos de atributos de seguridad del sujeto y de los datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.2.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si las siguientes normas, basadas en las relaciones ordenadas entre los atributos de seguridad, se aplican: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.2.3 La TSF debe aplicar la [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.2.4 La TSF debe ofrecer las [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.2.5 La TSF debe autorizar explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.2.6 La TSF debe prohibir explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. FDP_IFF.2.7 La TSF debe aplicar las siguientes relaciones para cada par válido de atributos de seguridad de control del flujo de información: a) existe una función de ordenación tal que, dados dos atributos de seguridad válidos, determina si los atributos de seguridad son idénticos, si uno de los atributos de seguridad es superior al otro o si los atributos de seguridad no son comparables; y b) existe un "límite superior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que es superior o igual a los dos atributos de seguridad válidos; y

	c) existe un "límite inferior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que no es superior a los dos atributos de seguridad válidos. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos Para atributos de seguridad jerárquicos, debe existir una función de ordenación que, dados dos atributos de seguridad válidos, determine si son idénticos, si uno es superior al otro o si no son comparables.
Atributos de seguridad jerárquicos	Jerárquico de: FDP_IFF.1 FDP_IFF.2.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] sobre la base de los siguientes tipos de atributos de seguridad del sujeto y de los datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.2.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si las siguientes normas, basadas en las relaciones ordenadas entre los atributos de seguridad, se aplican: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.2.3 La TSF debe aplicar la [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.2.4 La TSF debe ofrecer las [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.2.5 La TSF debe autorizar explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.2.6 La TSF debe prohibir explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. FDP_IFF.2.7 La TSF debe aplicar las siguientes relaciones para cada par válido de atributos de seguridad de control del flujo de información: a) existe una función de ordenación tal que, dados dos atributos de seguridad válidos, determina si los atributos de seguridad son idénticos, si uno de los atributos de seguridad es superior al otro o si los atributos de seguridad no son comparables; y b) existe un "límite superior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que es superior o igual a los dos atributos de seguridad válidos; y c) existe un "límite inferior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que no es superior a los dos atributos de seguridad válidos. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos Para atributos de seguridad jerárquicos, debe existir un "límite superior" tal que, dado cualquier par de atributos de seguridad válidos, exista un atributo que sea superior o igual a los dos atributos de seguridad válidos.
Atributos de	Jerárquico de: FDP_IFF.1

seguridad jerárquicos	FDP_IFF.2.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] sobre la base de los siguientes tipos de atributos de seguridad del sujeto y de los datos: [aplicación: la cantidad mínima y el tipo de atributos de seguridad]. FDP_IFF.2.2 La TSF debe autorizar un flujo de información entre un sujeto controlado y datos controlados mediante una operación controlada si las siguientes normas, basadas en las relaciones ordenadas entre los atributos de seguridad, se aplican: [aplicación: para cada operación, las relaciones basadas en los atributos de seguridad que deben existir entre los atributos de seguridad del sujeto y los atributos de seguridad de los datos]. FDP_IFF.2.3 La TSF debe aplicar la [aplicación: normas complementarias de la SFP sobre control del flujo de información]. FDP_IFF.2.4 La TSF debe ofrecer las [aplicación: lista de las capacidades adicionales de la SFP]. FDP_IFF.2.5 La TSF debe autorizar explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que autoricen explícitamente los flujos de información]. FDP_IFF.2.6 La TSF debe prohibir explícitamente un flujo de información sobre la base de las siguientes normas: [aplicación: normas, basadas en los atributos de seguridad, que prohíban explícitamente los flujos de información]. FDP_IFF.2.7 La TSF debe aplicar las siguientes relaciones para cada par válido de atributos de seguridad de control del flujo de información: a) existe una función de ordenación tal que, dados dos atributos de seguridad válidos, determina si los atributos de seguridad son idénticos, si uno de los atributos de seguridad es superior al otro o si los atributos de seguridad no son comparables; y b) existe un "límite superior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que es superior o igual a los dos atributos de seguridad válidos; y c) existe un "límite inferior", en el conjunto de atributos de seguridad, tal que, dado un par cualquiera de atributos de seguridad válidos, existe un atributo de seguridad que no es superior a los dos atributos de seguridad válidos. Dependencias: FDP_IFC.1 Control parcial del flujo de información FMT_MSA.3 Inicialización estática de atributos Ejemplos Para atributos de seguridad jerárquicos, debe existir un "límite inferior" tal que, dado cualquier par de atributos de seguridad válidos, exista un atributo que no sea superior a los dos atributos de seguridad.
Flujo ilícito de datos limitado	Jerárquico de: ningún otro componente. FDP_IFF.3.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] para limitar la capacidad de [aplicación: tipos de flujos ilícitos de información] a [aplicación: capacidad máxima]. Dependencias: AVA_CCA.1 Análisis de los canales ocultos FDP_IFC.1 Control parcial del flujo de información Ejemplos La aplicación de la política de seguridad para el control de flujos debe poder limitar el volumen de los flujos de datos ilícitos (definir) a una capacidad máxima (definir).

Supresión parcial de flujos ilícitos de datos	Jerárquico de: FDP_IFF.3 FDP_IFF.4.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] para limitar la capacidad de [aplicación: tipos de flujos ilícitos de información] a [aplicación: capacidad máxima]. FDP_IFF.4.2 La TSF debe impedir [aplicación: tipos de flujos ilícitos de información]. Dependencias: AVA_CCA.1 Análisis de los canales ocultos FDP_IFC.1 Control parcial del flujo de información Ejemplos Para una supresión parcial de flujos ilícitos de datos, la aplicación de la política de seguridad para el control de flujos debe impedir ciertos tipos de flujos ilícitos identificados (definir).
Ningún flujo ilícito de datos	Hiérarchique à : FDP_IFF.4 FDP_IFF.5.1 La TSF doit garantir qu'aucun flux d'information illicite n'existe pour contourner [affectation : nom de la SFP de contrôle de flux d'information]. Dépendances : AVA_CCA.3 Analyse exhaustive des canaux cachés FDP_IFC.1 Contrôle de flux d'information partiel Exemples Pour une élimination complète des flux d'information illicites, l'application de la politique de sécurité pour le contrôle de flux doit garantir qu'aucun flux illicite n'existe pour contourner les dispositions de contrôle de flux Jerárquico de: FDP_IFF.4 FDP_IFF.5.1 La TSF debe garantizar que no existe ningún flujo ilícito de información para evitar [aplicación: nombre de la SFP de control del flujo de información]. Dependencias: AVA_CCA.3 Análisis exhaustivo de los canales ocultos FDP_IFC.1 Control parcial del flujo de información Ejemplos Para una supresión total de los flujos ilícitos de datos, la aplicación de la política de seguridad para el control de flujos debe garantizar que no exista ningún flujo ilícito que permita evadir las disposiciones de control de flujos.
Control de los flujos ilícitos de datos	Jerárquico de: ningún otro componente. FDP_IFF.6.1 La TSF debe aplicar la [aplicación: SFP de control del flujo de información] para controlar [aplicación: tipos de flujos ilícitos de información] cuando superen [aplicación: capacidad máxima]. Dependencias: AVA_CCA.1 Análisis de los canales ocultos FDP_IFC.1 Control parcial del flujo de información Ejemplos La política de seguridad para el control de flujos debe permitir controlar determinados flujos ilícitos (definir) cuando superen una capacidad máxima (definir).
FDP_ITC: Importación desde una zona fuera del control de la TSF	
Importación de	Jerárquico de: ningún otro componente.

datos del usuario sin atributos de seguridad	FDP_ITC.1.1 La TSF debe aplicar la [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC. FDP_ITC.1.2 La TSF debe ignorar cualquier atributo de seguridad asociado a los datos del usuario cuando dichos datos sean importados desde fuera del TSC. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FMT_MSA.3 Inicialización estática de atributos Ejemplos Para una importación sin atributos de seguridad, cualquier atributo de seguridad asociado a los datos del usuario debe ser ignorado durante una importación desde fuera del TSC.
Importación de datos del usuario sin atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ITC.1.3 La TSF debe aplicar las siguientes normas durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC: [aplicación: normas complementarias de control de importación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FMT_MSA.3 Inicialización estática de atributos Ejemplos Deben aplicarse las normas complementarias de la política de seguridad sobre el control de importación (definir).
Importación de datos del usuario sin atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ITC.1.1 La TSF debe aplicar la [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC. FDP_ITC.1.2 La TSF debe ignorar cualquier atributo de seguridad asociado a los datos del usuario cuando dichos datos sean importados desde fuera del TSC. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FMT_MSA.3 Inicialización estática de atributos Ejemplos La política de seguridad para el control de acceso o para el control de flujos debe aplicarse durante la importación de datos provenientes del exterior del área de seguridad.
Importación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ITC.2.1 La TSF debe aplicar la [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC. FDP_ITC.2.2 La TSF debe utilizar los atributos de seguridad asociados a los datos de usuario importados. FDP_ITC.2.3 La TSF debe garantizar que el protocolo utilizado permite asociar de manera no ambigua los atributos de seguridad de los datos de usuario recibidos.

	FDP_ITC.2.4 La TSF debe garantizar que la interpretación de los atributos de seguridad de los datos de usuario importados es la prevista por el emisor de los datos del usuario. FDP_ITC.2.5 La TSF debe aplicar las siguientes normas durante la importación de datos del usuario provenientes de fuera del TSC, que son controlados por la SFP: [aplicación: normas complementarias de control de importación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] FPT_TDC.1 Coherencia básica de los datos de la TSF entre TSF Ejemplos Para una importación con atributos de seguridad, deben utilizarse los atributos de seguridad asociados a los datos de usuario importados.
Importación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ITC.2.1 La TSF debe aplicar la [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC. FDP_ITC.2.2 La TSF debe utilizar los atributos de seguridad asociados a los datos de usuario importados. FDP_ITC.2.3 La TSF debe garantizar que el protocolo utilizado permite asociar de manera no ambigua los atributos de seguridad de los datos de usuario recibidos. FDP_ITC.2.4 La TSF debe garantizar que la interpretación de los atributos de seguridad de los datos de usuario importados es la prevista por el emisor de los datos del usuario. FDP_ITC.2.5 La TSF debe aplicar las siguientes normas durante la importación de datos del usuario provenientes de fuera del TSC, que son controlados por la SFP: [aplicación: normas complementarias de control de importación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] FPT_TDC.1 Coherencia básica de los datos de la TSF entre TSF Ejemplos Para una importación con atributos de seguridad, el protocolo utilizado debe permitir asociar de manera no ambigua los atributos de seguridad a los datos de usuario recibidos.
Importación de datos del usuario con atributos de seguridad	Jerárquico de: ningún otro componente. FDP_ITC.2.1 La TSF debe aplicar la [aplicación: SFP de control de acceso o SFP de control del flujo de información] durante la importación de datos del usuario controlados por la SFP y provenientes de fuera del TSC. FDP_ITC.2.2 La TSF debe utilizar los atributos de seguridad asociados a los datos de usuario importados. FDP_ITC.2.3 La TSF debe garantizar que el protocolo utilizado permite asociar de manera no ambigua los atributos de seguridad de los datos de usuario recibidos.

	FDP_ITC.2.4 La TSF debe garantizar que la interpretación de los atributos de seguridad de los datos de usuario importados es la prevista por el emisor de los datos del usuario. FDP_ITC.2.5 La TSF debe aplicar las siguientes normas durante la importación de datos del usuario provenientes de fuera del TSC, que son controlados por la SFP: [aplicación: normas complementarias de control de importación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] FPT_TDC.1 Coherencia básica de los datos de la TSF entre TSF Ejemplos Para una importación con atributos de seguridad, la interpretación de los atributos de seguridad de los datos de usuario importados debe ser la prevista por el emisor de los datos del usuario.
FDP_ITT: Transferencia interna al TOE	
Protección básica de una transferencia interna	Jerárquico de: ningún otro componente. FDP_ITT.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para impedir la [selección: divulgación, modificación o pérdida de posibilidad de uso] de datos del usuario durante su transmisión entre partes del TOE físicamente separadas. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos La política de seguridad para el control de acceso o para el control de flujo debe impedir la divulgación, modificación o pérdida de posibilidad de uso de los datos durante su transmisión entre partes físicamente separadas del área de seguridad.
Separación de datos durante una transmisión en función de atributos	Jerárquico de: FDP_ITT.1 FDP_ITT.2.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para impedir la [selección: divulgación, modificación o pérdida de posibilidad de uso] de datos del usuario durante su transmisión entre partes del TOE físicamente separadas. FDP_ITT.2.2 La TSF debe separar los datos controlados por la o las SFP durante su transmisión entre partes del TOE físicamente separadas, en función del valor de lo siguiente: [aplicación: atributos de seguridad que requieren una separación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos Para una separación de datos transmitidos en función de atributos, los datos controlados transmitidos entre partes físicamente separadas del área de seguridad deben separarse en función de los atributos de seguridad que requieren una separación.
Control de la integridad	Jerárquico de: ningún otro componente. FDP_ITT.3.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para controlar los datos del usuario durante su transmisión entre partes del TOE físicamente separadas, para

	detectar los siguiente errores: [aplicación: errores de integridad]. FDP_ITT.3.2 En caso de detección de algún error de integridad de datos, la TSF debe [aplicación: especificar la acción que debe iniciarse en caso de error de integridad]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FDP_ITT.1 Protección básica de una transferencia interna Ejemplos Los errores de integridad deben detectarse durante la transmisión de los datos del usuario entre partes físicamente separadas del área de seguridad.
Control de la integridad	Jerárquico de: ningún otro componente. FDP_ITT.3.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para controlar los datos del usuario durante su transmisión entre partes del TOE físicamente separadas, para detectar los siguiente errores: [aplicación: errores de integridad]. FDP_ITT.3.2 En caso de detección de algún error de integridad de datos, la TSF debe [aplicación: especificar la acción que debe iniciarse en caso de error de integridad]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FDP_ITT.1 Protección básica de una transferencia interna Ejemplos En caso de detección de errores de integridad, deben iniciarse acciones específicas (definir).
Control de la integridad basado en los atributos	Jerárquico de: FDP_ITT.3 FDP_ITT.4.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para controlar los datos del usuario durante su transmisión entre partes del TOE físicamente separadas, para detectar los siguiente errores: [aplicación: errores de integridad], en función de los siguientes atributos: [aplicación: atributos de seguridad que requieren canales de transmisión separados]. FDP_ITT.4.2 En caso de detección de un error de integridad de datos, la TSF debe [aplicación: especificar la acción que debe iniciarse en caso de error de integridad]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FDP_ITT.2 Separación de datos durante una transmisión en función de atributos Ejemplos FDP_ITT.3.1: Control de integridad en función de los atributos de seguridad que requieren canales de transmisión separados.
FDP_RIP: Protección de los datos residuales	
Protección parcial de los datos residuales	Jerárquico de: ningún otro componente. FDP_RIP.1.1 La TSF debe garantizar que toda información contenida precedentemente en un recurso se transforme en no disponible durante [selección: la asignación del recurso a los, la anulación de asignación del recurso de los] siguientes objetos: [aplicación: lista de los objetos].

	Dependencias: Ninguna dependencia. Ejemplos Para una protección parcial de las informaciones residuales, cualquier información precedentemente contenida en un recurso debe ser transformada en no disponible durante la asignación o anulación de asignación del recurso de los objetos (definir).
Protección total de los datos residuales	FDP_RIP.2.1 La TSF debe garantizar que toda información contenida precedentemente en un recurso se transforme en no disponible durante [selección: la asignación del recurso a, la anulación de asignación del recurso de] todos los objetos. Dependencias: Ninguna dependencia. Ejemplos Para una protección total de los datos residuales, cualquier información anteriormente contenida en un recurso debe ser transformada en no disponible durante la asignación o anulación de asignación del recurso para todos los objetos.
FDP_ROL: Anulación	
Anulación básica	Jerárquico de: ningún otro componente. FDP_ROL.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para autorizar la anulación de las [aplicación: listas de las operaciones] sobre los [aplicación: listas de los objetos]. FDP_ROL.1.2 La TSF debe autorizar la anulación de las operaciones dentro de los [aplicación: límites dentro de los cuales puede efectuarse la anulación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos Para anulaciones básicas, debe autorizarse la anulación de operaciones (definir) sobre objetos identificados (definir).
Anulación básica	Jerárquico de: ningún otro componente. FDP_ROL.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para autorizar la anulación de las [aplicación: listas de las operaciones] sobre los [aplicación: listas de los objetos]. FDP_ROL.1.2 La TSF debe autorizar la anulación de las operaciones dentro de los [aplicación: límites dentro de los cuales puede efectuarse la anulación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos Para anulaciones básicas, debe autorizarse la anulación de operaciones dentro de los límites en que la anulación puede efectuarse (definir).
Anulación avanzada	Jerárquico de: FDP_ROL.1 FDP_ROL.2.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para autorizar la anulación de todas las operaciones sobre los [aplicación: listas de los objetos].

	FDP_ROL.2.2 La TSF debe autorizar la anulación para las operaciones dentro de los [aplicación: límites dentro de los cuales puede efectuarse la anulación]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos Para anulaciones avanzadas, deben poder anularse todas las operaciones sobre objetos identificados (definir).
FDP_SDI: Integridad de los datos almacenados	
Control de la integridad de los datos almacenados	Jerárquico de: ningún otro componente. FDP_SDI.1.1 La TSF debe controlar los datos del usuario almacenados dentro del TSC buscando [aplicación: errores de integridad] sobre todos los objetos, en función de los siguientes atributos: [aplicación: atributos de los datos del usuario]. Dependencias: Ninguna dependencia. Ejemplos Los datos del usuario almacenados deben controlarse mediante la búsqueda de errores de integridad sobre todos los objetos en función de los atributos de los datos del usuario (definir).
Control de la integridad de los datos almacenados y acciones que deben iniciarse	Jerárquico de: FDP_SDI.1 FDP_SDI.2.1 La TSF debe controlar los datos del usuario almacenados dentro del TSC buscando [aplicación: errores de integridad] sobre todos los objetos, en función de los siguientes atributos: [aplicación: atributos de los datos del usuario]. FDP_SDI.2.2 En caso de detección de un error de integridad, la TSF debe [aplicación: acción que hay que iniciar]. Dependencias: Ninguna dependencia. Ejemplos En caso de detección de un error de integridad, deben iniciarse acciones específicas (definir).
FDP_UCT: Protección de la confidencialidad de los datos del usuario durante una transferencia entre TSF	
Confidencialidad básica durante un intercambio de datos	Jerárquico de: ningún otro componente. FDP_UCT.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para poder [selección: transmitir, recibir] objetos de una manera que los proteja de cualquier divulgación no autorizada. Dependencias: [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] Ejemplos Los objetos deben ser transmitidos y recibidos de tal modo que se encuentren protegidos contra cualquier divulgación no autorizada.
FDP_UIT: Protección de la integridad de los datos del usuario durante una transferencia entre TSF	

Integridad durante un intercambio de datos	Jerárquico de: ningún otro componente. FDP_UIT.1.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para poder [selección: transmitir, recibir] datos del usuario de una manera que los proteja de errores de [selección: modificación, supresión, inserción, reinserción]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] Ejemplos Los datos del usuario deben ser transmitidos y recibidos de tal modo que se encuentren protegidos contra modificaciones, supresiones, inserciones o reinserciones.
Integridad durante un intercambio de datos	Jerárquico de: ningún otro componente. FDP_UIT.1.2 La TSF debe poder determinar, durante la recepción de los datos del usuario, si ha ocurrido [selección: una modificación, una supresión, una inserción, una reinserción]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] [FTP_ITC.1 Canal seguro entre TSF, o FTP_TRP.1 Ruta segura] Ejemplos Durante la recepción de los datos del usuario, debe ser posible determinar si ha ocurrido una modificación, una supresión, una inserción o una reinserción.
Reconstitución a partir del emisor durante un intercambio de datos	Jerárquico de: ningún otro componente. FDP_UIT.2.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para poder reconstituir los datos a partir de [aplicación: lista de los errores compatibles con una reconstitución] con la ayuda del producto TI de confianza que da origen a la emisión. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FDP_UIT.1 Integridad durante un intercambio de datos FTP_ITC.1 Canal seguro entre TSF Ejemplos Para realizar una reconstitución a partir del emisor, los datos deben poder reconstituirse a partir de errores compatibles con una reconstitución (definir) con ayuda del sistema de confianza que dio origen a la emisión.
Reconstitución a partir del destinatario durante un intercambio de datos	Jerárquico de: FDP_UIT.2 FDP_UIT.3.1 La TSF debe aplicar la o las [aplicación: SFP de control de acceso o SFP de control del flujo de información] para poder reconstituir los datos a partir de [aplicación: lista de los errores que permiten una reconstitución] sin ninguna ayuda del producto TI de confianza que da origen a la emisión. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FDP_UIT.1 Integridad durante un intercambio de datos FTP_ITC.1 Canal seguro entre TSF Ejemplos

	Para realizar una reconstitución a partir del destinatario, los datos deben poder reconstituirse a partir de errores que permitan una reconstitución (definir) sin ninguna ayuda del sistema de confianza que dio origen a la emisión.

3.1.5 FIA : Identificación y autenticación

FIA_AFL: Fallos de autenticación	
Gestión de un fallo de autenticación	Jerárquico de: ningún otro componente. FIA_AFL.1.1 La TSF debe detectar cuando han ocurrido [aplicación: cantidad] intentos de autenticación infructuosos relacionados con [aplicación: lista de acontecimientos vinculados con la autenticación]. Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos El sistema debe detectar cuando ha ocurrido una cantidad (definir) de intentos de autenticación infructuosos relacionados con acontecimientos vinculados con la autenticación (definir).
Gestión de un fallo de autenticación	Jerárquico de: ningún otro componente. FIA_AFL.1.2 Cuando se ha alcanzado o superado la cantidad especificada de intentos de autenticación, la TSF debe [aplicación: lista de acciones]. Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos Deben iniciarse acciones específicas (definir) cuando se ha alcanzado o superado la cantidad especificada de intentos de autenticación infructuosos.
FIA_ATD: Definición de los atributos del usuario	
Definición de los atributos de un usuario	Jerárquico de: ningún otro componente. FIA_ATD.1.1 La TSF debe mantener la siguiente lista de atributos de seguridad asignados a usuarios individuales: [aplicación: lista de atributos de seguridad]. Dependencias: Ninguna dependencia. Ejemplos Debe mantenerse una lista de atributos de seguridad asignados a usuarios individuales (definir).
FIA_SOS: Especificación de claves	
Verificación de claves	Jerárquico de: ningún otro componente. FIA_SOS.1.1 La TSF debe ofrecer un mecanismo para controlar las claves que responden a [aplicación: una métrica de calidad definida]. Dependencias: Ninguna dependencia. Ejemplos Un mecanismo debe controlar que las claves respondan a una métrica de calidad definida (definir).
Generación de claves por parte de la TSF	Jerárquico de: ningún otro componente. FIA_SOS.2.1 La TSF debe ofrecer un mecanismo para administrar las claves que responden a [aplicación: una métrica de calidad definida].

	Dependencias: Ninguna dependencia. Ejemplos Debe haber un mecanismo disponible para generar claves que respondan a una métrica de calidad definida (definir).
Generación de claves por parte de la TSF	Jerárquico de: ningún otro componente. FIA_SOS.2.2 La TSF debe ser capaz de imponer el uso obligatorio de las claves que ha generado para [aplicación: lista de funciones de la TSF]. Dependencias: Ninguna dependencia. Ejemplos Debe poder imponerse el uso obligatorio de las claves generadas en el marco de FIA_SOS.2.1, para funciones identificadas (definir).
FIA_UAU: Autenticación del usuario	
Secuencia de la autenticación	Jerárquico de: ningún otro componente. FIA_UAU.1.1 La TSF debe autorizar que [aplicación: lista de acciones generadas en la TSF] por cuenta del usuario se realicen antes de que éste se encuentre autenticado. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Ciertas acciones generadas en el sistema por cuenta del usuario (definir) deben autorizarse antes de que el usuario sea autenticado.
Secuencia de la autenticación	Jerárquico de: ningún otro componente. FIA_UAU.1.2 La TSF debe exigir que cada usuario sea autenticado con éxito antes de autorizar cualquier otra acción generada en la TSF por cuenta de dicho usuario. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Cada usuario debe ser autenticado con éxito antes de que se autorice cualquier acción generada en el sistema por cuenta del usuario, con excepción de las acciones definidas en el FIA_UAU.1.1.
Autenticación imposible de falsificar	Jerárquico de: ningún otro componente. FIA_UAU.3.1 La TSF debe [selección: detectar, impedir] la utilización de datos de autenticación que hayan sido falsificados por cualquier usuario de la TSF. Dependencias: Ninguna dependencia. Ejemplos Debe detectarse e impedirse el uso de datos de autenticación falsificados por cualquier usuario.
Autenticación imposible de falsificar	Jerárquico de: ningún otro componente. FIA_UAU.3.2 La TSF debe [selección: detectar, impedir] la utilización de datos de autenticación que hayan sido copiados por cualquier otro usuario de la TSF.

	Dependencias: Ninguna dependencia. Ejemplos Debe detectarse e impedirse el uso de datos de autenticación copiados por cualquier otro usuario que no sea el usuario titular de dichos datos.
Mecanismos de autenticación de uso único	Jerárquico de: ningún otro componente. FIA_UAU.4.1 La TSF debe impedir la reutilización de los datos de autenticación vinculados con [aplicación: mecanismo(s) de autenticación identificado(s)]. Dependencias: Ninguna dependencia. Ejemplos Debe impedirse, para una autenticación única, la reutilización de datos de autenticación vinculados con los mecanismos de autenticación identificados (definir).
Mecanismos de autenticación múltiple	Jerárquico de: ningún otro componente. FIA_UAU.5.1 La TSF debe ofrecer [aplicación: lista de mecanismos de autenticación múltiple] para contribuir a la autenticación del usuario. Dependencias: Ninguna dependencia. Ejemplos Para la implementación de mecanismos de autenticación múltiple, deben proporcionarse mecanismos de autenticación múltiples (definir) que contribuyan a la autenticación del usuario.
Mecanismos de autenticación múltiple	Jerárquico de: ningún otro componente. FIA_UAU.5.2 La TSF debe autenticar la identidad anunciada de cualquier usuario según [aplicación: normas que describen cómo los mecanismos de autenticación múltiple proporcionan la autenticación]. Dependencias: Ninguna dependencia. Ejemplos Para la implementación de mecanismos de autenticación múltiple, debe autorizarse la identidad anunciada de cualquier usuario según normas que describan cómo los mecanismos de autenticación múltiple proporcionan la autenticación (definir).
Nueva autenticación	Jerárquico de: ningún otro componente. FIA_UAU.6.1 La TSF debe autenticar nuevamente al usuario en las siguientes condiciones [aplicación: lista de las condiciones en las cuales se requiere una nueva autenticación]. Dependencias: Ninguna dependencia. Ejemplos El usuario debe ser nuevamente autenticado en las condiciones específicas para las cuales se exige una nueva autenticación (definir).
Autenticación con respuesta segura	Jerárquico de: ningún otro componente. FIA_UAU.7.1 La TSF solo debe proporcionar al usuario [aplicación: lista de las informaciones entregadas] durante la ejecución de la autenticación.

	Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos Sólo ciertos datos específicos (definir) pueden proporcionarse al usuario en el transcurso de la autenticación.
FIA_UID: Identificación de un usuario	
Secuencia de la identificación	Jerárquico de: ningún otro componente. FIA_UID.1.1 La TSF debe autorizar que [aplicación: lista de acciones generadas en la TSF] por cuenta del usuario se realicen antes de que éste se encuentre identificado. Dependencias: Ninguna dependencia. Ejemplos Ciertas acciones generadas en el sistema por cuenta del usuario (definir) deben autorizarse antes de que el usuario sea identificado.
Secuencia de la identificación	Jerárquico de: ningún otro componente. FIA_UID.1.2 La TSF debe exigir que cada usuario sea identificado con éxito antes de autorizar cualquier otra acción generada en la TSF por cuenta de dicho usuario. Dependencias: Ninguna dependencia. Ejemplos Cada usuario debe ser identificado con éxito antes de que se autorice cualquier acción generada en el sistema por cuenta del usuario, con excepción de las acciones definidas por el FIA_UID.1.1.
FIA_USB: Vínculo usuario-sujeto	
Vínculos usuario-sujeto	Jerárquico de: ningún otro componente. FIA_USB.1.1 La TSF debe vincular los atributos de seguridad propios del usuario con los sujetos que actúan por cuenta de dicho usuario. Dependencias: FIA_ATD.1 Definición de los atributos del usuario Ejemplos Los atributos de seguridad propios del usuario deben estar vinculados con los sujetos que actúan por cuenta de dicho usuario.

3.1.6 FMT : Gestión de la seguridad

FMT_MOF: Gestión de las funciones de la TSF	
Gestión del comportamiento de las funciones de seguridad	Jerárquico de: ningún otro componente. FMT_MOF.1.1 La TSF debe restringir la aptitud para [selección: determinar el comportamiento, desactivar, activar, modificar el comportamiento] de las funciones [aplicación: lista de las funciones] a los [aplicación: roles autorizados identificados]. Dependencias: FMT_SMR.1 Roles de seguridad Ejemplos La aptitud para determinar el comportamiento, desactivar, activar o modificar el

	comportamiento de funciones identificadas (definir) debe restringirse a los roles autorizados identificados (definir).
FMT_MSA: Gestión de los atributos de seguridad	
Gestión de los atributos de seguridad	Jerárquico de: ningún otro componente. FMT_MSA.1.1 La TSF debe implementar la o las [aplicación: SFP de control de acceso, SFP de control de flujo de datos] para restringir a los [aplicación: los roles autorizados identificados] la aptitud para [selección: cambiar el valor por defecto, consultar, modificar, suprimir, [aplicación: otras operaciones]] los atributos de seguridad [aplicación: lista de los atributos de seguridad]. Dependencias: [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FMT_SMR.1 Roles de seguridad Ejemplos La aptitud para cambiar el valor por defecto, consultar, modificar, suprimir o efectuar otras operaciones identificas (definir) sobre ciertos atributos de seguridad (definir) debe restringirse a los roles autorizados identificados (definir).
Atributos de seguridad protegidos	Jerárquico de: ningún otro componente. FMT_MSA.2.1 La TSF debe garantizar que sólo se acepten valores seguros para los atributos de seguridad. Dependencias: ADV_SPM.1 Modelo informal de política de seguridad del TOE [FDP_ACC.1 Control de acceso parcial, o FDP_IFC.1 Control parcial del flujo de información] FMT_MSA.1 Gestión de los atributos de seguridad FMT_SMR.1 Roles de seguridad Ejemplos Sólo deben aceptarse valores seguros para los atributos de seguridad.
Inicialización estática de atributos	Jerárquico de: ningún otro componente. FMT_MSA.3.1 La TSF debe implementar la o las [aplicación: SFP de control de acceso, SFP de control de flujo de datos] para proporcionar valores por defecto [selección: restrictivos, permisivos, otras propiedades] para los atributos de seguridad que se utilizan para aplicar la SFP. Dependencias: FMT_MSA.1 Gestión de los atributos de seguridad FMT_SMR.1 Roles de seguridad Ejemplos Deben proporcionarse los valores por defecto restrictivos, permisivos o referidos a otras propiedades (definir) para los atributos de seguridad que se utilizan para aplicar la política de seguridad.
Inicialización de atributo estático	Jerárquico de: ningún otro componente. FMT_MSA.3.2 La TSF debe permitir a los [aplicación: los roles autorizados identificados] especificar valores iniciales alternativos para reemplazar los valores por defecto cuando se crea un objeto o un dato. Dependencias: FMT_MSA.1 Gestión de los atributos de seguridad FMT_SMR.1 Roles de seguridad Ejemplos Los roles autorizados identificados (definir) deben poder especificar valores

	iniciales alternativos para reemplazar los valores por defecto cuando se crea un objeto o un dato.
FMT_MTD: Gestión de los datos de la TSF	
Gestión de los datos de la TSF	Jerárquico de: ningún otro componente. FMT_MTD.1.1 La TSF debe restringir la aptitud para [selección: cambiar un valor por defecto, consultar, modificar, suprimir, borrar [aplicación: otras operaciones]] las [aplicación: lista de los datos de la TSF] a los [aplicación: los roles autorizados identificados]. Dependencias: FMT_SMR.1 Roles de seguridad Ejemplos La aptitud para cambiar un valor por defecto, consultar, modificar, suprimir, borrar y efectuar otras operaciones identificadas (definir) debe restringirse a los roles autorizados (definir).
Gestión de los valores límite de los datos de la TSF	Jerárquico de: ningún otro componente. FMT_MTD.2.1 La TSF debe restringir la especificación de los valores límite de los [aplicación: lista de los datos de la TSF] a los [aplicación: los roles autorizados identificados]. Dependencias: FMT_MTD.1 Gestión de los datos de la TSF FMT_SMR.1 Roles de seguridad Ejemplos La especificación de los valores límite de ciertos datos (definir) debe restringirse a los roles autorizados definidos (definir).
Gestión de los valores límite de los datos de la TSF	Jerárquico de: ningún otro componente. FMT_MTD.2.2 La TSF debe iniciar las siguientes acciones cuando los datos de la TSF alcancen o superen los valores límite indicados: [aplicación: acciones que deben iniciarse]. Dependencias: FMT_MTD.1 Gestión de los datos de la TSF FMT_SMR.1 Roles de seguridad Ejemplos Deben iniciarse acciones específicas (definir) cuando los datos alcancen o superen los valores límite indicados en el FMT_MTD.2.2.
Datos seguros de la TSF	Jerárquico de: ningún otro componente. FMT_MTD.3.1 La TSF debe garantizar que sólo se aceptan valores seguros para los datos de la TSF. Dependencias: ADV_SPM.1 Modelo informal de política de seguridad del TOE FMT_MTD.1 Gestión de los datos de la TSF Ejemplos Deben aceptarse como datos del sistema sólo valores seguros.
FMT_REV: Revocación	
Revocación	Jerárquico de: ningún otro componente. FMT_REV.1.1 La TSF debe restringir a los [aplicación: los roles autorizados identificados] la aptitud para revocar los atributos de seguridad asociados a los [selección: usuarios, sujetos, objetos, otros recursos adicionales] dentro del TSC.

	Dependencias: FMT_SMR.1 Roles de seguridad Ejemplos Sólo los roles autorizados identificados (definir) deben tener la aptitud para revocar los atributos de seguridad asociados a los usuarios, sujetos, objetos y otros recursos adicionales (definir) dentro del sistema.
Revocación	Jerárquico de: ningún otro componente. FMT_REV.1.2 La TSF debe implementar las normas [aplicación: especificación de las normas de revocación]. Dependencias: FMT_SMR.1 Roles de seguridad Ejemplos Deben implementarse normas de revocación específicas (definir).
FMT_SAE: Caducidad de los atributos de seguridad	
Autorización con límite de tiempo	Jerárquico de: ningún otro componente. FMT_SAE.1.1 La TSF debe restringir a los [aplicación: los roles autorizados identificados] la capacidad de especificar una fecha de caducidad para [aplicación: lista de los atributos de seguridad a los cuales debe aplicarse una fecha de caducidad]. Dependencias: FMT_SMR.1 Roles de seguridad FPT_STM.1 Consignación fiable de fecha y hora Ejemplos Sólo los roles autorizados identificados (definir) deben tener la capacidad de especificar una fecha de caducidad para ciertos atributos de seguridad que requieren una fecha de caducidad (definir).
Autorización con límite de tiempo	Jerárquico de: ningún otro componente. FMT_SAE.1.2 Para cada uno de estos atributos de seguridad, la TSF debe ser capaz de [aplicación: lista de las acciones que hay que iniciar para cada atributo de seguridad] tras superar la fecha de caducidad del atributo de seguridad. Dependencias: FMT_SMR.1 Roles de seguridad FPT_STM.1 Consignación fiable de fecha y hora Ejemplos Ciertas acciones específicas (definir para cada atributo identificado en el FMT_SAE.1.1) deben poder iniciarse tras la fecha de caducidad del atributo de seguridad.
FMT_SMR: Roles para la gestión de la seguridad	
Roles de seguridad	Jerárquico de: ningún otro componente. FMT_SMR.1.1 La TSF debe mantener actualizados los roles [aplicación: los roles autorizados identificados]. FMT_SMR.1.2 La TSF debe ser capaz de vincular usuarios con roles. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos

	Deben mantenerse actualizados los roles autorizados identificados (definir).
Roles de seguridad	Jerárquico de: ningún otro componente. FMT_SMR.1.1 La TSF debe mantener actualizados los roles [aplicación: los roles autorizados identificados]. FMT_SMR.1.2 La TSF debe ser capaz de vincular usuarios con roles. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Debe ser posible vincular usuarios con roles.
Restricciones sobre los roles de seguridad	Jerárquico de: FMT_SMR.1 FMT_SMR.2.1 La TSF debe mantener actualizados los roles [aplicación: los roles autorizados identificados]. FMT_SMR.2.2 La TSF debe ser capaz de vincular usuarios con roles. FMT_SMR.2.3 La TSF debe garantizar que se cumplen las condiciones [aplicación: condiciones asociadas a los diferentes roles]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Para las restricciones sobre los roles de seguridad, deben cumplirse las condiciones asociadas a los diferentes roles (definir).
Adopción de los roles	Jerárquico de: ningún otro componente. FMT_SMR.3.1 La TSF debe exigir una petición explícita para hacerse cargo de los siguientes roles: [aplicación: los roles]. Dependencias: FMT_SMR.1 Roles de seguridad Ejemplos Debe realizarse una petición explícita para tomar a cargo ciertos roles identificados (definir).

3.1.7 FPR : Protección de la vida privada

FPR_ANO: Anonimato	
Anonimato	Jerárquico de: ningún otro componente. FPR_ANO.1.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. Dependencias: Ninguna dependencia. Ejemplos Ciertos grupos de usuarios o sujetos (definir) deben ser incapaces de determinar el verdadero nombre del usuario asociado a sujetos, operaciones u objetos identificados (definir).
Anonimato sin petición de datos	Jerárquico de: FPR_ANO.1 FPR_ANO.2.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o

	sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_ANO.2.2 La TSF debe proporcionar [aplicación: lista de servicios] a [aplicación: lista de sujetos] sin requerir referencia alguna al verdadero nombre del usuario. Dependencias: Ninguna dependencia. Ejemplos Para un anonimato sin petición de información, deben proporcionarse ciertos servicios a ciertos sujetos, sin requerir referencia alguna al verdadero nombre del usuario.
FPR_PSE: Posibilidad de actuar bajo un seudónimo	
Posibilidad de actuar bajo un seudónimo	Jerárquico de: ningún otro componente. FPR_PSE.1.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.1.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.1.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. Dependencias: Ninguna dependencia. Ejemplos Ciertos grupos de usuarios o sujetos (definir) deben ser incapaces de determinar el verdadero nombre del usuario asociado a sujetos, operaciones u objetos identificados (definir).
Posibilidad de actuar bajo un seudónimo	Jerárquico de: ningún otro componente. FPR_PSE.1.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.1.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.1.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. Dependencias: Ninguna dependencia. Ejemplos Debe ser posible proporcionar cierta cantidad de alias (definir) del verdadero nombre del usuario de los sujetos identificados (definir).
Posibilidad de actuar bajo un seudónimo	Jerárquico de: ningún otro componente. FPR_PSE.1.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.1.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de

	alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.1.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. Dependencias: Ninguna dependencia. Ejemplos El sistema debe determinar un alias para un usuario, aceptar el alias del usuario y controlar que el alias se haya establecido conforme a la métrica referida a los alias (definir).
Uso reversible de seudónimos	Jerárquico de: FPR_PSE.1 FPR_PSE.2.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.2.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.2.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. FPR_PSE.2.4 La TSF debe proporcionar a [selección: un usuario autorizado, [aplicación: lista de sujetos de confianza]] una capacidad para determinar la identidad del usuario a partir del alias proporcionado, únicamente en las siguientes condiciones [aplicación: lista de condiciones]. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Para un uso reversible de seudónimos, los usuarios autorizados y los sujetos de confianza (definir) deben poder determinar la identidad del usuario a partir del alias proporcionado, únicamente bajo ciertas condiciones (definir).
Posibilidad de actuar bajo un seudónimo utilizando un alias	Jerárquico de: FPR_PSE.1 FPR_PSE.3.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.3.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.3.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. FPR_PSE.3.4 La TSF debe proporcionar un alias para el verdadero nombre del usuario, que debe ser idéntico a un alias proporcionado anteriormente en las siguientes condiciones [aplicación: lista de condiciones]; en caso contrario, el alias proporcionado no debe guardar ninguna relación con los alias anteriormente proporcionados. Dependencias: Ninguna dependencia. Ejemplos Para tener la posibilidad de actuar bajo un seudónimo utilizando un alias, el alias

	proporcionado para el verdadero nombre del usuario debe ser, en lo posible, idéntico a un alias proporcionado anteriormente bajo ciertas condiciones (definir).
Posibilidad de actuar bajo un seudónimo utilizando un alias	Jerárquico de: FPR_PSE.1 FPR_PSE.3.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar el verdadero nombre del usuario asociado a [aplicación: lista de sujetos, operaciones u objetos]. FPR_PSE.3.2 La TSF debe ser capaz de proporcionar [aplicación: cantidad de alias] alias del verdadero nombre del usuario a [aplicación: lista de sujetos]. FPR_PSE.3.3 La TSF debe [selección: determinar un alias para un usuario, aceptar el alias del usuario] y controlar que se haya determinado conforme a la [aplicación: métrica referida a los alias]. FPR_PSE.3.4 La TSF debe proporcionar un alias para el verdadero nombre del usuario, que debe ser idéntico a un alias proporcionado anteriormente en las siguientes condiciones [aplicación: lista de condiciones]; en caso contrario, el alias proporcionado no debe guardar ninguna relación con los alias anteriormente proporcionados. Dependencias: Ninguna dependencia. Ejemplos Para la posibilidad de actuar bajo un seudónimo utilizando un alias, si no puede respetarse el FPR_PSE.3.4.1, el alias proporcionado no debe guardar ninguna relación con los alias anteriormente proporcionados.
FPR_UNL: Imposibilidad de establecer un vínculo	
Imposibilidad de establecer un vínculo	Jerárquico de: ningún otro componente. FPR_UNL.1.1 La TSF debe garantizar que [aplicación: conjunto de usuarios o sujetos] sean incapaces de determinar si [aplicación: lista de operaciones] [selección: han sido desencadenadas por el mismo usuario, están vinculadas de la siguiente forma [aplicación: lista de relaciones]]. Dependencias: Ninguna dependencia. Ejemplos Ciertos conjuntos de usuarios o sujetos (definir) deben ser incapaces de determinar si ciertas relaciones (definir) han sido desencadenadas por el mismo usuario o si están vinculadas mediante relaciones identificadas (definir).
FPR_UNO: Ocultamiento	
Ocultamiento	Jerárquico de: ningún otro componente. FPR_UNO.1.1 La TSF debe garantizar que [aplicación: lista de usuarios o sujetos] no puedan observar la ejecución de [aplicación: lista de las operaciones] en [aplicación: lista de los objetos] realizadas por [aplicación: lista de usuarios o sujetos protegidos]. Dependencias: Ninguna dependencia. Ejemplos Ciertos usuarios y sujetos identificados (definir) no deben poder observar la ejecución de ciertas operaciones (definir) sobre determinados objetos (definir) por parte de ciertos usuarios y sujetos protegidos (definir).
Asignación de los datos que tienen	Jerárquico de: FPR_UNO.1

un impacto sobre el ocultamiento	FPR_UNO.2.1 La TSF debe garantizar que [aplicación: lista de usuarios o sujetos] no puedan observar la ejecución de [aplicación: lista de operaciones] en [aplicación: lista de los objetos] realizadas por [aplicación: lista de usuarios o sujetos protegidos]. FPR_UNO.2.2 La TSF debe asignar los [aplicación: datos referidos al ocultamiento] a las diferentes partes del TOE de tal modo que las siguientes condiciones se cumplan durante la vida útil de los datos: [aplicación: lista de condiciones]. Dependencias: Ninguna dependencia. Ejemplos Para una asignación de los datos que tienen un impacto en el ocultamiento, los datos referidos al ocultamiento (definir) deben asignarse a diferentes partes del sistema a fin de respetar ciertas condiciones (definir).
Ocultamiento sin petición de información	Jerárquico de: ningún otro componente. FPR_UNO.3.1 La TSF debe proporcionar [aplicación: lista de servicios] a [aplicación: lista de sujetos] sin requerir ninguna referencia a [aplicación: datos referidos a la vida privada]. Dependencias: FPR_UNO.1 Ocultamiento Ejemplos Ciertos servicios (definir) deben proporcionarse a sujetos identificados (definir) sin requerir referencia alguna a datos de la vida privada (definir).
Observabilidad para un usuario autorizado	Jerárquico de: ningún otro componente. FPR_UNO.4.1 La TSF debe proporcionar a [aplicación: conjunto de usuarios autorizados] la capacidad de observar el uso de [aplicación: lista de recursos o servicios]. Dependencias: Ninguna dependencia. Ejemplos Ciertos usuarios autorizados (definir) deben tener la capacidad de observar el uso de recursos o servicios identificados (definir).

3.1.8 FPT : Protección de la TSF

FPT_AMT: Prueba de la máquina hipotética subyacente	
Prueba de la máquina hipotética	Jerárquico de: ningún otro componente. FPT_AMT.1.1 La TSF debe ejecutar una serie de pruebas [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a pedido de un usuario autorizado, en otras situaciones] para demostrar el correcto funcionamiento de las hipótesis de seguridad proporcionadas por la máquina hipotética subyacente en la TSF. Dependencias: Ninguna dependencia Ejemplos Deben poder realizarse pruebas durante la puesta en servicio inicial para demostrar el funcionamiento correcto de las hipótesis de seguridad proporcionadas por los sistemas a cargo de la seguridad.
Prueba de la	Jerárquico de: ningún otro componente.

máquina hipotética	FPT_AMT.1.1 La TSF debe ejecutar una serie de pruebas [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a pedido de un usuario autorizado, en otras situaciones] para demostrar el correcto funcionamiento de las hipótesis de seguridad proporcionadas por la máquina hipotética subyacente en la TSF. Dependencias: Ninguna dependencia. Ejemplos Deben poder realizarse pruebas durante el funcionamiento normal para demostrar el funcionamiento correcto de las hipótesis de seguridad proporcionadas por los sistemas a cargo de la seguridad.
Prueba de la máquina hipotética	Jerárquico de: ningún otro componente. FPT_AMT.1.1 La TSF debe ejecutar una serie de pruebas [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a pedido de un usuario autorizado, en otras situaciones] para demostrar el correcto funcionamiento de las hipótesis de seguridad proporcionadas por la máquina hipotética subyacente en la TSF. Dependencias: Ninguna dependencia. Ejemplos Deben poder realizarse pruebas a petición de un usuario autorizado para demostrar el funcionamiento correcto de las hipótesis de seguridad proporcionadas por los sistemas a cargo de la seguridad.
Prueba de la máquina hipotética	Jerárquico de: ningún otro componente. FPT_AMT.1.1 La TSF debe ejecutar una serie de pruebas [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a pedido de un usuario autorizado, en otras situaciones] para demostrar el correcto funcionamiento de las hipótesis de seguridad proporcionadas por la máquina hipotética subyacente en la TSF. Dependencias: Ninguna dependencia. Ejemplos Deben poder realizarse pruebas en ciertas situaciones adicionales (definir) para demostrar el funcionamiento correcto de las hipótesis de seguridad proporcionadas por los sistemas a cargo de la seguridad.
FPT_FLS: Modo seguro después de fallo	
Fallo con preservación de un estado seguro	Jerárquico de: ningún otro componente. FPT_FLS.1.1 La TSF debe preservar un estado seguro cuando se producen los siguientes tipos de fallos: [aplicación: lista de los tipos de fallos de la TSF]. Dependencias: ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Los sistemas a cargo de la seguridad deben preservar un estado seguro cuando se producen determinados tipos de fallos (definir).
FPT_ITA: Disponibilidad de datos exportados de la TSF	
Disponibilidad entre TSF en el marco de una	Jerárquico de: ningún otro componente. FPT_ITA.1.1 La TSF debe garantizar la disponibilidad [aplicación: lista de los

métrica de disponibilidad	tipos de datos de la TSF] proporcionada a un producto TI remoto de confianza en el marco de [aplicación: una métrica de disponibilidad definida], dadas las siguientes condiciones [aplicación: condiciones para garantizar la disponibilidad]. Dependencias: Ninguna dependencia. Ejemplos La disponibilidad de ciertos datos de seguridad en un sistema de confianza remoto.
FPT_ITC: Confidencialidad de los datos exportados de la TSF	
Confidencialidad entre TSF durante una transmisión	Jerárquico de: ningún otro componente. FPT_ITC.1.1 La TSF debe proteger todos los datos de la TSF transmitidos desde la TSF hacia un producto TI remoto de confianza para que no se produzca ninguna divulgación no autorizada durante su transmisión. Dependencias: Ninguna dependencia. Ejemplos Todos los datos de seguridad transmitidos desde un sistema a cargo de la seguridad hacia un sistema remoto de confianza deben protegerse contra una divulgación no autorizada durante su transmisión.
FPT_ITI: Integridad de los datos exportados de la TSF	
Detección de una modificación entre TSF	Jerárquico de: ningún otro componente. FPT_ITI.1.1 La TSF debe ofrecer la capacidad para detectar una modificación de todos los datos de la TSF durante su transmisión entre la TSF y un producto TI remoto de confianza dentro de los límites del siguiente sistema de medición: [aplicación: una métrica de modificación definida]. FPT_ITI.1.2 La TSF debe ofrecer la capacidad de controlar la integridad de todos los datos de la TSF transmitidos entre la TSF y un producto TI remoto de confianza y efectuar [aplicación: acción que hay que iniciar] si se detectan modificaciones. Dependencias: Ninguna dependencia. Ejemplos Cualquier modificación de datos de seguridad durante su transmisión entre un sistema a cargo de la seguridad y un sistema remoto de confianza debe detectarse dentro de los límites de una métrica de modificación específica (definir).
Detección de una modificación entre TSF	Jerárquico de: ningún otro componente. FPT_ITI.1.1 La TSF debe ofrecer la capacidad para detectar una modificación de todos los datos de la TSF durante su transmisión entre la TSF y un producto TI remoto de confianza dentro de los límites del siguiente sistema de medición: [aplicación: una métrica de modificación definida]. FPT_ITI.1.2 La TSF debe ofrecer la capacidad de controlar la integridad de todos los datos de la TSF transmitidos entre la TSF y un producto TI remoto de confianza y efectuar [aplicación: acción que hay que iniciar] si se detectan modificaciones. Dependencias: Ninguna dependencia. Ejemplos

	Debe controlarse la integridad de todos los datos de seguridad transmitidos entre un sistema a cargo de la seguridad y un sistema remoto de confianza y deben iniciarse acciones (definir) si se detectan modificaciones.
Detección y corrección de una modificación entre TSF	Jerárquico de: FPT_ITI.1 FPT_ITI.2.1 La TSF debe ofrecer la capacidad para detectar una modificación de todos los datos de la TSF durante su transmisión entre la TSF y un producto TI remoto de confianza dentro de los límites del siguiente sistema de medición: [aplicación: una métrica de modificación definida]. FPT_ITI.2.2 La TSF debe ofrecer la capacidad de controlar la integridad de todos los datos de la TSF transmitidos entre la TSF y un producto TI remoto de confianza y efectuar [aplicación: acción que hay que iniciar] si se detectan modificaciones. FPT_ITI.2.3 La TSF debe ofrecer la capacidad de corregir [aplicación: tipo de modificación] todos los datos de la TSF transmitidos entre la TSF y un producto TI remoto de confianza. Dependencias: Ninguna dependencia. Ejemplos Para una corrección de cualquier modificación entre sistemas, deben poder corregirse determinados tipos de modificaciones (definir) de cualquier dato de seguridad transmitido entre un sistema a cargo de la seguridad y un sistema remoto de confianza.
FPT_ITT: Transferencia de los datos de la TSF dentro del TOE	
Protección básica de la transferencia de datos dentro de la TSF	Jerárquico de: ningún otro componente. FPT_ITT.1.1 La TSF debe proteger los datos de la TSF contra la [selección: divulgación, modificación] cuando se transmiten entre partes separadas del TOE. Dependencias: Ninguna dependencia. Ejemplos Los datos de seguridad deben protegerse contra cualquier divulgación o modificación cuando se transmiten entre partes separadas del sistema.
Separación de los datos de la TSF durante una transferencia	Jerárquico de: FPT_ITT.1 FPT_ITT.2.1 La TSF debe proteger los datos de la TSF contra la [selección: divulgación, modificación] cuando se transmiten entre partes separadas del TOE. FPT_ITT.2.2 La TSF debe separar los datos del usuario de los datos de la TSF cuando tales datos se transmiten entre partes separadas del TOE. Dependencias: Ninguna dependencia. Ejemplos Los datos del usuario deben separarse de los datos de seguridad cuando tales datos se transmiten entre partes separadas del sistema.
Control de la integridad de los datos de la TSF	Jerárquico de: ningún otro componente. FPT_ITT.3.1 La TSF debe ser capaz de detectar [selección: la modificación de datos, la sustitución de datos, el reordenamiento de datos, la supresión de datos, [aplicación: otros errores de integridad]] para los datos de la TSF transmitidos entre partes separadas del TOE. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una

	transferencia interna Ejemplos Debe detectarse la modificación, sustitución, reordenamiento, supresión u otros errores de integridad (definir) que afecten a los datos de seguridad transmitidos entre partes separadas del sistema.
Control de la integridad de los datos de la TSF	Jerárquico de: ningún otro componente. FPT_ITT.3.2 En cuanto se detecta un error de integridad en los datos, la TSF debe iniciar las siguientes acciones: [aplicación: especificar la acción que debe iniciarse]. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una transferencia interna Ejemplos Deben iniciarse acciones específicas (definir) en cuanto se detecta un error de integridad en los datos.
FPT_PHP: Protección física de la TSF	
Detección pasiva de un ataque físico	Jerárquico de: ningún otro componente. FPT_PHP.1.1 La TSF debe detectar de manera no ambigua una intrusión física que pudiera comprometer a la TSF. FPT_PHP.1.2 La TSF debe ofrecer la capacidad de determinar si ha ocurrido una intrusión física en los dispositivos de la TSF o en los elementos de la TSF. Dependencias: FMT_MOF.1 Gestión del comportamiento de las funciones de seguridad Ejemplos Debe detectarse de manera no ambigua cualquier intrusión física susceptible de comprometer la seguridad del sistema.
Detección pasiva de un ataque físico	Jerárquico de: ningún otro componente. FPT_PHP.1.1 La TSF debe detectar de manera no ambigua una intrusión física que pudiera comprometer a la TSF. FPT_PHP.1.2 La TSF debe ofrecer la capacidad de determinar si ha ocurrido una intrusión física en los dispositivos de la TSF o en los elementos de la TSF. Dependencias: FMT_MOF.1 Gestión del comportamiento de las funciones de seguridad Ejemplos Debe ser posible determinar si ha ocurrido una intrusión física en los dispositivos de seguridad o en los elementos de seguridad.
Notificación de un ataque físico	Jerárquico de: FPT_PHP.1 FPT_PHP.2.1 La TSF debe detectar de manera no ambigua una intrusión física que pudiera comprometer a la TSF. FPT_PHP.2.2 La TSF debe ofrecer la capacidad de determinar si ha ocurrido una intrusión física en los dispositivos de la TSF o en los elementos de la TSF. FPT_PHP.2.3 Para [aplicación: lista de los dispositivos o elementos de la TSF para los cuales se requiere una detección activa], la TSF debe controlar los

	dispositivos y los elementos y notificar a [aplicación: un usuario o rol designado] cuando ha ocurrido una intrusión física en los dispositivos de la TSF o en los elementos de la TSF. Dependencias: FMT_MOF.1 Gestión del comportamiento de las funciones de seguridad Ejemplos Deben controlarse ciertos dispositivos y elementos de seguridad (definir). Cualquier intrusión física en estos dispositivos y elementos debe notificarse a un usuario específico o rol designado (definir).
Resistencia a un ataque físico	Jerárquico de: ningún otro componente. FPT_PHP.3.1 La TSF debe resistir a [aplicación: situaciones de intrusión física] en los [aplicación: lista de los dispositivos o elementos de la TSF], respondiendo automáticamente de tal modo que no se viole la TSP. Dependencias: Ninguna dependencia. Ejemplos El sistema debe resistir a situaciones de intrusión física (definir) en dispositivos o elementos de seguridad (definir), respondiendo automáticamente de tal modo que no se viole la política de seguridad.
FPT_RCV: Recuperación segura	
Recuperación manual	Jerárquico de: ningún otro componente. FPT_RCV.1.1 Luego de un fallo o una interrupción de servicio, la TSF debe pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del TOE. Dependencias: FPT_TST.1 Prueba de la TSF AGD_ADM.1 Manual de administración ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Luego de un fallo o una interrupción de servicio, los sistemas a cargo de la seguridad deben pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del sistema.
Recuperación automatizada	Jerárquico de: FPT_RCV.1 FPT_RCV.2.1 Cuando no sea posible una recuperación automatizada tras un fallo o una interrupción de servicio, la TSF debe pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del TOE. FPT_RCV.2.2 Para [aplicación: lista de fallos o interrupciones del servicio], la TSF debe garantizar que se restablezca el estado seguro del TOE utilizando procedimientos automatizados. Dependencias: FPT_TST.1 Prueba de la TSF AGD_ADM.1 Manual de administración ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Cuando no sea posible una recuperación automática tras un fallo o una interrupción de servicio, los sistemas a cargo de la seguridad deben pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado

	seguro del sistema.
Recuperación automatizada	Jerárquico de: FPT_RCV.1 FPT_RCV.2.1 Cuando no sea posible una recuperación automatizada tras un fallo o una interrupción de servicio, la TSF debe pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del TOE. FPT_RCV.2.2 Para [aplicación: lista de fallos o interrupciones del servicio], la TSF debe garantizar que se restablezca el estado seguro del TOE utilizando procedimientos automatizados. Dependencias: FPT_TST.1 Prueba de la TSF AGD_ADM.1 Manual de administración ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Para ciertos fallos o interrupciones del servicio (definir), el retorno del sistema a un estado seguro debe garantizarse utilizando procedimientos automatizados.
Recuperación automatizada sin pérdida excesiva de datos	Jerárquico de: FPT_RCV.2 FPT_RCV.3.1 Cuando no sea posible una recuperación automática tras un fallo o una interrupción de servicio, la TSF debe pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del TOE. FPT_RCV.3.2 Para [aplicación: lista de fallos o interrupciones del servicio], la TSF debe garantizar que se restablezca el estado seguro del TOE utilizando procedimientos automatizados. FPT_RCV.3.3 Las funciones proporcionadas por la TSF para la recuperación tras un fallo o una interrupción de servicio deben garantizar que se restablezca el estado inicial seguro sin superar [aplicación: cuantificación] de pérdida de datos de la TSF o de objetos en el TSC. FPT_RCV.3.4 La TSF debe ofrecer la capacidad de determinar los objetos que se ha podido o no recuperar. Dependencias: FPT_TST.1 Prueba de la TSF AGD_ADM.1 Manual de administración ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Para una recuperación automatizada sin pérdida excesiva de datos, las funciones para una recuperación luego de un fallo o de una interrupción de servicio deben garantizar que se restablezca el estado inicial seguro sin superar determinado volumen de pérdida de datos (definir).
Recuperación automatizada sin pérdida excesiva de datos	Jerárquico de: FPT_RCV.2 FPT_RCV.3.1 Cuando no sea posible una recuperación automatizada tras un fallo o una interrupción de servicio, la TSF debe pasar a un modo de mantenimiento que ofrezca la posibilidad de restablecer el estado seguro del TOE. FPT_RCV.3.2 Para [aplicación: lista de fallos o interrupciones del servicio], la TSF debe garantizar que se restablezca el estado seguro del TOE utilizando procedimientos automatizados. FPT_RCV.3.3 Las funciones proporcionadas por la TSF para la recuperación tras un fallo o una interrupción de servicio deben garantizar que se restablezca el

	estado inicial seguro sin superar [aplicación: cuantificación] de pérdida de datos de la TSF o de objetos en el TSC. FPT_RCV.3.4 La TSF debe ofrecer la capacidad de determinar los objetos que se ha podido o no recuperar. Dependencias: FPT_TST.1 Prueba de la TSF AGD_ADM.1 Manual de administración ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos Debe ser posible determinar que objetos han podido o no recuperarse.
Recuperación de función	Jerárquico de: ningún otro componente. FPT_RCV.4.1 La TSF debe garantizar que [aplicación: lista de las SF y de las situaciones de fallo] cuentan con la cualidad según la cual la SF cumple con éxito su tarea o bien retoma su funcionamiento en un estado coherente y seguro, para las situaciones de fallo indicadas. Dependencias: ADV_SPM.1 Modelo informal de política de seguridad del TOE Ejemplos En caso de situaciones de fallo identificadas (definir), las funciones de seguridad deben cumplir su tarea con éxito o bien retomar su funcionamiento en un estado coherente y seguro.
FPT_RPL: Detección de reinserción	
Detección de reinserción	Jerárquico de: ningún otro componente. FPT_RPL.1.1 La TSF debe detectar la reinserción para las siguientes entidades: [aplicación: lista de las entidades identificadas]. Dependencias: Ninguna dependencia. Ejemplos Debe detectarse la reinserción para ciertas entidades identificadas (definir).
Detección de reinserción	Jerárquico de: ningún otro componente. FPT_RPL.1.2 La TSF debe ejecutar [aplicación: lista de las acciones específicas] cuando se ha detectado la reinserción. Dependencias: Ninguna dependencia. Ejemplos Deben ejecutarse acciones específicas (definir) en cuanto se detecta la reinserción.
FPT_RVM: Paso obligatorio por un monitor de referencia	
Capacidad de la TSP para evitar ser puenteada	Jerárquico de: ningún otro componente. FPT_RVM.1.1 La TSF debe garantizar que las funciones que implementan la TSP son llamadas y se ejecutan con éxito antes de que cada función TSC sea autorizada a iniciarse. Dependencias: Ninguna dependencia. Ejemplos

	Las funciones que implementan la política de seguridad deben ser llamadas y ejecutarse con éxito antes de que cada función del sistema sea autorizada a iniciarse.
FPT_SEP: Separación de áreas	
Separación de áreas para la TSF	Jerárquico de: ningún otro componente. FPT_SEP.1.1 La TSF debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e intrusiones de sujetos no seguros. FPT_SEP.1.2 La TSF debe implementar una separación entre las áreas de seguridad de sujetos dentro del TSC. Dependencias: Ninguna dependencia. Ejemplos Los sistemas a cargo de la seguridad deben mantener un área de seguridad para su propia ejecución, que los proteja de interferencias e intrusiones de sujetos no seguros.
Separación de áreas para la TSF	Jerárquico de: ningún otro componente. FPT_SEP.1.1 La TSF debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e intrusiones de sujetos no seguros. FPT_SEP.1.2 La TSF debe implementar una separación entre las áreas de seguridad de sujetos dentro del TSC. Dependencias: Ninguna dependencia. Ejemplos Debe aplicarse en el sistema una separación entre las áreas de seguridad de los sujetos.
Separación de áreas para la SFP	Jerárquico de: FPT_SEP.1 FPT_SEP.2.1 La parte no aislada de la TSF debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e intrusiones de sujetos no seguros. FPT_SEP.2.2 La TSF debe implementar una separación entre las áreas de seguridad de sujetos dentro del TSC. FPT_SEP.2.3 La TSF debe mantener la parte de la TSF vinculada con [aplicación: lista de las SFP de control de acceso o de las SFP de control de flujo de datos] en un área de seguridad para su propia ejecución; área que la proteja de interferencias e intrusiones provenientes del resto de la TSF y de sujetos no seguros, en lo que respecta a dichas SFP. Dependencias: Ninguna dependencia. Ejemplos Los sistemas de seguridad a cargo del control de acceso o del control de flujo de datos deben mantenerse en un área de seguridad para su propia ejecución, que los proteja de las interferencias, de las intrusiones y de los sujetos no seguros.
Separación de áreas para la SFP	Jerárquico de: FPT_SEP.1 FPT_SEP.2.1 La parte no aislada de la TSF debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e

	intrusiones de sujetos no seguros. FPT_SEP.2.2 La TSF debe implementar una separación entre las áreas de seguridad de sujetos dentro del TSC. FPT_SEP.2.3 La TSF debe mantener la parte de la TSF vinculada con [aplicación: lista de las SFP de control de acceso o de las SFP de control de flujo de datos] en un área de seguridad para su propia ejecución; área que las proteja de interferencias e intrusiones provenientes del resto de la TSF y de sujetos no seguros, en lo que respecta a dichas SFP. Dependencias: Ninguna dependencia. Ejemplos La parte no aislada de un sistema a cargo de la seguridad debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e intrusiones de sujetos no seguros.
Monitor de referencia completo	Jerárquico de: FPT_SEP.2 FPT_SEP.3.1 La parte no aislada de la TSF debe mantener un área de seguridad para su propia ejecución; área que la protegerá de interferencias e intrusiones de sujetos no seguros. FPT_SEP.3.2 La TSF debe implementar una separación entre las áreas de seguridad de sujetos dentro del TSC. FPT_SEP.3.3 La TSF debe mantener la parte de la TSF que implementa las SFP de control de acceso o las SFP de control de flujo de datos en un área de seguridad para su propia ejecución; área que las proteja de interferencias e intrusiones provenientes del resto de la TSF y de sujetos no seguros, en lo que respecta a dicha TSP. Dependencias: Ninguna dependencia. Ejemplos Las partes de los sistemas de seguridad a cargo del control de acceso o del control de flujo de datos deben mantenerse en un área de seguridad para su propia ejecución, que las proteja de las interferencias, de las intrusiones y de los sujetos no seguros.
FPT_SSP: Protocolo de sincronización de estados	
Acuse de recibo de confianza simple	Jerárquico de: ningún otro componente. FPT_SSP.1.1 La TSF debe acusar recibo, cuando así lo requiera otra parte de la TSF, de una transmisión sin modificación de datos de la TSF. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una transferencia interna Ejemplos Un sistema a cargo de la seguridad debe acusar recibo de una transmisión sin modificación de datos de seguridad cuando se lo solicité otro sistema a cargo de la seguridad.
Acuse de recibo de confianza mutua	Jerárquico de: FPT_SSP.1 FPT_SSP.2.1 La TSF debe acusar recibo, cuando así lo requiera otra parte de la TSF, de una transmisión sin modificación de datos de la TSF. FPT_SSP.2.2 La TSF debe garantizar que las partes de la TSF involucradas

	conocen la situación exacta de los datos transmitidos entre sus diferentes partes, por medio de acuses de recibo. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una transferencia interna Ejemplos Para un acuse de recibo de confianza mutua, los sistemas a cargo de la seguridad involucrados deben conocer el estado exacto de los datos transmitidos entre sus diferentes partes mediante acuses de recibo.
FPT_STM: Consignación de la fecha y la hora	
Consignación fiable de la fecha y la hora	Jerárquico de: ningún otro componente. FPT_STM.1.1 La TSF debe ser capaz de proporcionar una consignación fiable de la fecha y la hora, para uso propio. Dependencias: Ninguna dependencia. Ejemplos Un sistema a cargo de la seguridad debe ser capaz de proporcionar una consignación fiable de la fecha y la hora, para uso propio.
FPT_TDC: Coherencia de los datos de la TSF entre TSF	
Coherencia básica de los datos de la TSF entre distintas TSF	Jerárquico de: ningún otro componente. FPT_TDC.1.1 La TSF debe ofrecer la capacidad de interpretar coherentemente [aplicación: lista de los tipos de datos de la TSF] cuando estos son compartidos por la TSF y otro producto TI de confianza. Dependencias: Ninguna dependencia. Ejemplos Ciertos tipos de datos de seguridad (definir) deben poder interpretarse de manera coherente cuando son compartidos por un sistema a cargo de la seguridad y un sistema de confianza.
Coherencia básica de los datos de la TSF entre distintas TSF	Jerárquico de: ningún otro componente. FPT_TDC.1.2 La TSF debe utilizar [aplicación: lista de las normas de interpretación que debe aplicar la TSF] para interpretar los datos de la TSF de otro producto TI de confianza. Dependencias: Ninguna dependencia. Ejemplos Los sistemas a cargo de la seguridad deben utilizar normas de interpretación (definir) para interpretar los datos de seguridad de otro sistema de confianza.
FPT_TRC: Coherencia de la reproducción de datos de la TSF dentro del TOE	
Coherencia interna de la TSF	Jerárquico de: ningún otro componente. FPT_TRC.1.1 La TSF debe garantizar que los datos de la TSF son coherentes cuando los mismos se reproducen entre diferentes partes del TOE. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una transferencia interna Ejemplos

	Los datos de seguridad deben ser coherentes cuando se reproducen entre diferentes partes del sistema.
Coherencia interna de la TSF	Jerárquico de: ningún otro componente. FPT_TRC.1.2 Cuando se desconecta alguna parte del TOE que contiene datos que han sido reproducidos de la TSF, la TSF debe garantizar la coherencia de dichos datos al momento de la reconexión, antes de procesar cualquier petición para [aplicación: lista de las SF que dependen de la coherencia de la reproducción de los datos de la TSF]. Dependencias: FPT_ITT.1 Protección básica de los datos de la TSF durante una transferencia interna Ejemplos Cuando se desconectan partes del sistema que contienen datos que han sido reproducidos, debe garantizarse la coherencia de dichos datos al momento de la reconexión, antes de ejecutar cualquier función de seguridad que requiera la utilización de dichos datos.
FPT_TST: Autotest de la TSF	
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.1 La TSF debe ejecutar una serie de autotests [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a petición del usuario autorizado, en determinadas condiciones [aplicación: condiciones en las que debería realizarse un autotest]] para demostrar el correcto funcionamiento de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Un sistema a cargo de la seguridad debe ejecutar una serie de autotests durante la puesta en servicio inicial para demostrar su correcto funcionamiento.
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.1 La TSF debe ejecutar una serie de autotests [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a petición del usuario autorizado, en determinadas condiciones [aplicación: condiciones en las que debería realizarse un autotest]] para demostrar el correcto funcionamiento de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Un sistema a cargo de la seguridad debe ejecutar una serie periódicamente durante el funcionamiento normal, para demostrar su correcto funcionamiento.
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.1 La TSF debe ejecutar una serie de autotests [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a petición del usuario autorizado, en las condiciones [aplicación: condiciones en las que debería realizarse un autotest]] para demostrar el correcto funcionamiento de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Un sistema a cargo de la seguridad debe ejecutar una serie de autotests a

	petición de un usuario autorizado, para demostrar su correcto funcionamiento.
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.1 La TSF debe ejecutar una serie de autotests [selección: durante la puesta en servicio inicial, periódicamente durante el funcionamiento normal, a petición del usuario autorizado, en determinadas condiciones [aplicación: condiciones en las que debería realizarse un autotest]] para demostrar el correcto funcionamiento de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Un sistema a cargo de la seguridad debe ejecutar una serie de autotests en determinadas condiciones (definir), para demostrar su correcto funcionamiento.
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.2 La TSF debe proporcionar a los usuarios autorizados la capacidad de controlar la integridad de datos de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Los usuarios autorizados deben tener la capacidad de controlar la integridad de los datos de seguridad.
Prueba de la TSF	Jerárquico de: ningún otro componente. FPT_TST.1.3 La TSF debe proporcionar a los usuarios autorizados la capacidad de controlar la integridad de datos de la TSF. Dependencias: FPT_AMT.1 Prueba de la máquina hipotética Ejemplos Los usuarios autorizados deben tener la capacidad de controlar la integridad del código ejecutable almacenado de un sistema a cargo de la seguridad.

3.1.9 FRU : Uso de los recursos

FRU_FLT: Tolerancia a fallos	
Tolerancia a fallos con modo funcionalidad reducida	Jerárquico de: ningún otro componente. FRU_FLT.1.1 La TSF debe garantizar el funcionamiento de [aplicación: lista de las capacidades del TOE] cuando aparecen los siguientes fallos: [aplicación: lista de los tipos de fallos]. Dependencias: FPT_FLS.1 Fallo con preservación de un estado seguro Ejemplos Para una tolerancia a fallos con modo funcionalidad reducida, deben garantizarse ciertas capacidades del sistema (definir) cuando ocurran ciertos fallos (definir).
Tolerancia a fallos limitada a ciertos casos	Jerárquico de: FRU_FLT.1 FRU_FLT.2.1 La TSF debe garantizar el funcionamiento de todas las capacidades del TOE cuando aparezcan los siguientes fallos: [aplicación: lista de los tipos de fallos].

	Dependencias: FPT_FLS.1 Fallo con preservación de un estado seguro Ejemplos Para una tolerancia a las averías limitada, todas las capacidades del sistema deben garantizarse cuando ocurran ciertos fallos (definir).
FRU_PRS: Prioridad de servicio	
Prioridad de servicio limitada	Jerárquico de: ningún otro componente. FRU_PRS.1.1 La TSF debe asignar una prioridad a cada sujeto de la TSF. FRU_PRS.1.2 La TSF debe garantizar que cada acceso a [aplicación: recursos controlados] debe otorgarse sobre la base de la prioridad asignada a los sujetos. Dependencias: Ninguna dependencia. Ejemplos Para una prioridad de servicio limitada, debe otorgarse cada acceso a recursos controlados (definir) sobre la base de la prioridad asignada a los sujetos.
Prioridad de servicio limitada	Jerárquico de: ningún otro componente. FRU_PRS.1.1 La TSF debe asignar una prioridad a cada sujeto de la TSF. FRU_PRS.1.2 La TSF debe garantizar que cada acceso a [aplicación: recursos controlados] debe otorgarse sobre la base de la prioridad asignada a los sujetos. Dependencias: Ninguna dependencia. Ejemplos Debe asignarse una prioridad a cada sujeto.
FRU_RSA: Asignación de los recursos	
Cuotas máximas	Jerárquico de: ningún otro componente. FRU_RSA.1.1 La TSF debe aplicar cuotas máximas para los siguientes recursos: [aplicación: recursos controlados] que [selección: un usuario individual, un grupo definido de usuarios, ciertos sujetos] pueden utilizar [selección: simultáneamente, durante un período de tiempo especificado]. Dependencias: Ninguna dependencia. Ejemplos Deben aplicarse cuotas máximas para los recursos controlados identificados (definir) que pueden utilizar, simultáneamente o durante un período de tiempo especificado, ciertos usuarios individuales, grupos de usuarios o sujetos (definir).
Cuotas mínimas y máximas	Jerárquico de: FRU_RSA.1 FRU_RSA.2.1 La TSF debe aplicar cuotas máximas para los siguientes recursos: [aplicación: recursos controlados] que [selección: un usuario individual, un grupo definido de usuarios] pueden utilizar [selección: simultáneamente, durante un período de tiempo especificado]. FRU_RSA.2.2 La TSF debe garantizar la provisión de una cantidad mínima de cada [aplicación: recurso controlado] que esté disponible para un uso [selección: simultáneo, durante un período de tiempo especificado] por parte de [selección: un usuario individual, un grupo definido de usuarios, ciertos sujetos]. Dependencias: Ninguna dependencia.

	Ejemplos Para cuotas mínimas, debe estar disponible una cantidad mínima identificada de cada recurso controlado (definir), para su uso simultáneo o durante un período de tiempo especificado, por parte de ciertos usuarios individuales, grupos de usuarios o sujetos (definir).

3.1.10 FTA : Acceso al TOE

FTA_LSA: Limitación del alcance de los atributos que pueden seleccionarse	
Limitación del área de los atributos que pueden seleccionarse	Jerárquico de: ningún otro componente. FTA_LSA.1.1 La TSF debe limitar el alcance de los atributos de seguridad de sesión [aplicación: atributos de seguridad de sesión] en función de [aplicación: atributos]. Dependencias: Ninguna dependencia. Ejemplos Debe delimitarse el alcance de los atributos de seguridad de sesión (definir) en función de ciertos atributos (definir).
FTA_MCS: Limitación de la cantidad de sesiones paralelas	
Limitación básica de la cantidad de sesiones paralelas	Jerárquico de: ningún otro componente. FTA_MCS.1.1 La TSF debe limitar la cantidad máxima de sesiones paralelas que pertenecen a un mismo usuario. FTA_MCS.1.2 La TSF debe aplicar, por defecto, un límite de [aplicación: cantidad por defecto] sesiones por usuario. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Debe delimitarse la cantidad máxima de sesiones paralelas pertenecientes al mismo usuario.
Limitación básica de la cantidad de sesiones paralelas	Jerárquico de: ningún otro componente. FTA_MCS.1.1 La TSF debe limitar la cantidad máxima de sesiones paralelas que pertenecen a un mismo usuario. FTA_MCS.1.2 La TSF debe aplicar, por defecto, un límite de [aplicación: cantidad por defecto] sesiones por usuario. Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Debe aplicarse por defecto un límite de la cantidad de sesiones por usuario (definir).
Limitación de la cantidad de sesiones paralelas mediante los atributos del usuario	Jerárquico de: FTA_MCS.1 FTA_MCS.2.1 La TSF debe limitar la cantidad máxima de sesiones paralelas que pertenecen a un mismo usuario, conforme a las normas [aplicación: normas referidas a la cantidad máxima de sesiones paralelas]. FTA_MCS.2.2 La TSF debe aplicar, por defecto, un límite de [aplicación: cantidad por defecto] sesiones por usuario.

	Dependencias: FIA_UID.1 Programación de la identificación Ejemplos Para limitar la cantidad de sesiones paralelas usando los atributos del usuario, debe limitarse la cantidad máxima de sesiones paralelas para un mismo usuario según las normas (definir), basándose en los atributos del usuario.
FTA_SSL: Bloqueo de sesión	
Bloqueo de una sesión iniciada por la TSF	Jerárquico de: ningún otro componente. FTA_SSL.1.1 La TSF debe bloquear una sesión interactiva luego de [aplicación: duración de la inactividad de un usuario]: a) borrando o sobrescribiendo el contenido de las pantallas de visualización, haciéndolas así ilegibles; b) desactivando cualquier medio de acceso a los datos del usuario o de visualización de los mismos, con excepción del desbloqueo de la sesión. FTA_SSL.1.2 La TSF debe requerir que los siguientes acontecimientos tengan lugar antes de desbloquear la sesión: [aplicación: acontecimientos que tienen que producirse]. Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos Debe bloquearse una sesión interactiva después de un período de inactividad del usuario (definir), haciendo ilegible el contenido de las pantallas de visualización y desactivando cualquier medio de acceso a los datos, excepto el desbloqueo de la sesión.
Bloqueo de una sesión iniciada por la TSF	Jerárquico de: ningún otro componente. FTA_SSL.1.1 La TSF debe bloquear una sesión interactiva luego de [aplicación: duración de la inactividad de un usuario]: a) borrando o sobrescribiendo el contenido de las pantallas de visualización, haciéndolas así ilegibles; b) desactivando cualquier medio de acceso a los datos del usuario o de visualización de los mismos, con excepción del desbloqueo de la sesión. FTA_SSL.1.2 La TSF debe requerir que los siguientes acontecimientos tengan lugar antes de desbloquear la sesión: [aplicación: acontecimientos que tienen que producirse]. Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos Ciertos acontecimientos (definir) deben ocurrir antes de desbloquear la sesión.
Bloqueo de una sesión iniciado por el usuario	Jerárquico de: ningún otro componente. FTA_SSL.2.1 La TSF debe autorizar al usuario a bloquear su propia sesión interactiva: a) borrando o sobrescribiendo el contenido de las pantallas de visualización, haciéndolas así ilegibles; b) desactivando cualquier medio de acceso a los datos del usuario o de visualización de los mismos, con excepción del desbloqueo de la sesión. FTA_SSL.2.2 La TSF debe requerir que los siguientes acontecimientos tengan lugar antes de desbloquear la sesión: [aplicación: acontecimientos que tienen que producirse].

	Dependencias: FIA_UAU.1 Programación de la autenticación Ejemplos El usuario debe poder bloquear su propia sesión interactiva haciendo ilegible el contenido de las pantallas de visualización y desactivando todo medio de acceso a los datos, excepto el desbloqueo de la sesión.
Cierre de una sesión iniciado por la TSF	Jerárquico de: ningún otro componente. FTA_SSL.3.1 La TSF debe terminar una sesión interactiva luego de [aplicación: período de inactividad de un usuario]: Dependencias: Ninguna dependencia. Ejemplos Debe cerrarse una sesión interactiva tras determinado período de inactividad de un usuario (definir).
FTA_TAB: Mensaje de acceso al TOE	
Mensaje por defecto de acceso al TOE	Jerárquico de: ningún otro componente. FTA_TAB.1.1 Antes de iniciar una sesión de usuario, la TSF debe mostrar en pantalla un mensaje de advertencia que informe sobre el uso no autorizado del TOE. Dependencias: Ninguna dependencia. Ejemplos Antes de iniciar una sesión de usuario, debe mostrarse en pantalla un mensaje de advertencia que informe sobre el uso no autorizado del sistema.
FTA_TAH: Registro histórico de los accesos al TOE	
Registro histórico de los accesos al TOE	Jerárquico de: ningún otro componente. FTA_TAH.1.1 En cuanto se inicia con éxito una sesión, la TSF debe mostrar en pantalla, para el usuario, [selección: la fecha, la hora, el método, el lugar] de la última sesión iniciada con éxito. Dependencias: Ninguna dependencia. Ejemplos En cuanto se inicia con éxito una sesión, deben mostrarse en pantalla, para el usuario, la fecha, la hora, el método y el lugar de la última sesión iniciada con éxito.
Registro histórico de los accesos al TOE	Jerárquico de: ningún otro componente. FTA_TAH.1.2 En cuanto se inicia con éxito una sesión, la TSF debe mostrar en pantalla [selección: la fecha, la hora, el método, el lugar] del último intento infructuoso de inicio de una sesión y la cantidad de intentos infructuosos desde la última sesión iniciada con éxito. Dependencias: Ninguna dependencia. Ejemplos En cuanto se inicia con éxito una sesión, deben mostrarse en pantalla la fecha, la hora, el método y el lugar del último intento infructuoso de inicio de una sesión y la cantidad de intentos infructuosos desde la última sesión iniciada con éxito.
Registro histórico	Jerárquico de: ningún otro componente.

de los accesos al TOE	FTA_TAH.1.3 La TSF no debe borrar los datos referidos al registro histórico de los accesos de la interfaz de usuario sin dar al usuario la posibilidad de revisar dichos datos. Dependencias: Ninguna dependencia. Ejemplos No deben borrarse de la interfaz de usuario los datos referidos al registro histórico de los accesos sin dar al usuario la posibilidad de revisar dichos datos.
FTA_TSE: Inicio de una sesión del TOE	
Inicio de una sesión del TOE	Jerárquico de: ningún otro componente. FTA_TSE.1.1 La TSF debe ser capaz de rechazar el inicio de una sesión en función de [aplicación: atributos]. Dependencias: Ninguna dependencia. Ejemplos Debe poder rechazarse, en función de ciertos atributos (definir), el inicio de una sesión.

3.1.11 FTP : Rutas y canales seguros

FTP_ITC: Ruta segura entre TSF	
Ruta segura entre TSF	Jerárquico de: ningún otro componente. FTP_ITC.1.1 La TSF debe proporcionar un canal de comunicación entre ella misma y un producto TI remoto de confianza que sea lógicamente diferente de los otros canales de comunicación y que garantice la identificación de sus extremos y la protección de los datos transmitidos por dicho canal para que no puedan ser modificados o divulgados. Dependencias: Ninguna dependencia. Ejemplos Debe proporcionarse con cada sistema de confianza un canal de comunicación lógicamente distinto de los otros canales y que garantice la identificación de sus extremos y la protección de los datos transmitidos contra toda modificación o divulgación.
Ruta segura entre TSF	Jerárquico de: ningún otro componente. FTP_ITC.1.2 La TSF debe permitir a [selección: la TSF, el producto TI remoto de confianza] iniciar la comunicación por medio del canal seguro. Dependencias: Ninguna dependencia. Ejemplos La comunicación por medio de un canal seguro debe poder ser iniciada por el sistema a cargo de la seguridad o por el sistema de confianza involucrado.
Ruta segura entre TSF	Jerárquico de: ningún otro componente. FTP_ITC.1.3 La TSF debe iniciar la comunicación por medio del canal seguro para [aplicación: lista de las funciones para las cuales se requiere un canal seguro].

	Dependencias: Ninguna dependencia. Ejemplos El sistema debe iniciar la comunicación por medio del canal seguro para las funciones para las cuales se requiere un canal seguro (definir).
FTP_TRP: Ruta segura	
Ruta segura	Jerárquico de: ningún otro componente. FTP_TRP.1.1 La TSF debe proporcionar una ruta de comunicación entre ella misma y los usuarios [selección: remotos, locales] que sea lógicamente diferente de las otras vías de comunicación y que garantice la identificación de sus extremos y la protección de los datos transmitidos contra cualquier modificación o divulgación. Dependencias: Ninguna dependencia. Ejemplos Debe proporcionarse una ruta de comunicación entre el sistema y los usuarios lógicamente distinta de las otras rutas y que garantice la identificación de sus extremos y la protección de los datos transmitidos contra cualquier modificación o divulgación.
Ruta segura	Jerárquico de: ningún otro componente. FTP_TRP.1.2 La TSF debe permitir a [selección: la TSF, usuarios locales, usuarios remotos] iniciar una comunicación utilizando la ruta segura. Dependencias: Ninguna dependencia. Ejemplos La comunicación por medio de una ruta segura debe poder ser iniciada por el sistema, por usuarios locales o por usuarios remotos.
Ruta segura	Jerárquico de: ningún otro componente. FTP_TRP.1.3 La TSF debe requerir la utilización de una ruta segura para [selección: autenticación inicial de un usuario, [aplicación: otros servicios para los cuales se requiere una ruta segura]]. Dependencias: Ninguna dependencia. Ejemplos Debe exigirse el uso de una ruta segura par la autenticación inicial de un usuario y para otros servicios (definir).

3.2 Requerimientos surgidos de la ISO 17799

3.2.1 BPS : Política de seguridad (capítulo 3)

BPS_PSI: Política de seguridad de la información (§3.1)	
BPS_PSI.1.1	Debe elaborarse la documentación de la política de seguridad, que deberá aprobar la dirección.
BPS_PSI.1.2	La política de seguridad debe ser comunicada a todos los colaboradores.
BPS_PSI.1.3	La política de seguridad debe incluir la definición de las responsabilidades generales y específicas.
BPS_PSI.1.4	La política de seguridad debe definir normas de seguridad claras y aplicables que cubran todos los aspectos de la seguridad.
BPS_PSI.1.5	La política de seguridad debe incluir normas sobre la clasificación de la información.
BPS_PSI.2.1.1	La política de seguridad debe ser revisada regularmente y cuando surjan cambios que la afecten, para lograr que siga siendo adecuada.
BPS_PSI.2.1.2	La actualización de la política de seguridad debe ser responsabilidad de un grupo o comité de revisión cuyos miembros estén claramente identificados.
BPS_PSI.2.1.3	El grupo o comité de revisión de la política de seguridad debe apoyarse en los trabajos del grupo de gestión de la seguridad (ver BOS_ISI.1.2).
BPS_PSI.2.2	La conformidad de los sistemas de información con la política de seguridad debe examinarse antes de que el SI comience a prestar cualquier nuevo servicio.
BPS_PSI.2.3	Debe existir un procedimiento de revisión de la política o de las normas de seguridad en función de los datos recogidos sobre los incidentes de seguridad identificados (tipo, frecuencia, costos generados...).
BPS_PSI.2.4	Debe verificarse regularmente la adecuación de la política de seguridad a los objetivos profesionales (por ejemplo, contemplándola dentro de una política de auditoría global).

3.2.2 BOS : Organización de la seguridad (capítulo 4)

BOS_ISI: Infraestructura de la seguridad de la información (§4.1)	
BOS_ISI.1.1	Debe formarse un grupo de gestión de la seguridad para brindar una orientación clara y proporcionar un apoyo visible de la dirección a las iniciativas de seguridad.
BOS_ISI.1.2	El grupo de gestión de la seguridad debe trabajar en base a informes periódicos del estado la seguridad de los sistemas de información (incidentes detectados, avance de los planes de acción, nuevos servicios...).
BOS_ISI.2.1	De ser posible, un grupo de gestión, cuyos miembros cumplan diversas funciones en las secciones del organismo involucradas, debe hacerse cargo de coordinar de la implementación de las medidas de control de seguridad de la información.
BOS_ISI.3.1	Deben definirse claramente las responsabilidades referidas a la protección del capital individual y de los datos, así como la ejecución de los procedimientos de seguridad específicos.
BOS_ISI.3.2	La política de seguridad debe proporcionar directrices generales para la asignación de las responsabilidades en materia de seguridad.
BOS_ISI.3.3	Las directrices de la política de seguridad para la asignación de las responsabilidades en materia de seguridad pueden completarse con documentos complementarios más detallados para los establecimientos, sistemas o servicios específicos.
BOS_ISI.4.1	Debe establecerse un procedimiento de autorización por parte de la dirección para las nuevas infraestructuras de tratamiento de la información.

BOS_ISI.5.1	El organismo debe disponer de un sistema de vigilancia tecnológica adaptado a sus entornos y desafíos (por ejemplo, seguimiento de las vulnerabilidades y parches disponibles)
BOS_ISI.5.2	Debe existir la posibilidad de solicitar asesoramiento a especialistas internos o externos (incluidos los organismos nacionales especializados en seguridad de los sistemas de información como la DCSSI o la CNIL) en materia de seguridad de la información.
BOS_ISI.5.3	El asesoramiento obtenido de los especialistas debe ser notificado a toda la organización.
BOS_ISI.6.1	Es necesario mantener contactos adecuados con las autoridades legales, los organismos de reglamentación, los prestadores de servicios informáticos y los prestadores de servicios de telecomunicación.
BOS_ISI.6.2	En caso de incidente de seguridad, debe ser posible utilizar los contactos indicados en el punto BOS_ISI.6.1 para asegurar una reacción rápida y adecuada (obtención de asesoramiento, acción de los asociados...).
BOS_ISI.6.3	La comunicación efectuada con los contactos indicados en el punto BOS_ISI.6.1 no debe poner en peligro la protección de las informaciones de seguridad.
BOS_ISI.7.1	La implementación de la política de seguridad de la información debe ser revisada en forma independiente (por ejemplo, por un organismo interno o externo que no tenga ninguna otra responsabilidad operativa en el área de la seguridad).
BOS_SAT: Seguridad de los accesos por parte de terceros (§4.2)	
BOS_SAT.1.1	Debe realizarse un inventario del tipo de accesos al sistema de información realizados por terceros (accesos lógicos y accesos físicos), además de un análisis de riesgo para cada uno de los accesos inventariados.
BOS_SAT.1.2	Deben implementarse medidas adecuadas para el control de la seguridad de los accesos al sistema de información por parte de terceros.
BOS_SAT.1.3	Cada vez que un tercero debe trabajar en el sistema de información, un responsable del organismo debe contar con todos los medios necesarios para controlar las operaciones realizadas.
BOS_SAT.1.4	El acceso al sistema de información por parte de terceros debe estar motivado por una necesidad funcional.
BOS_SAT.1.5	El acceso al sistema de información por parte de terceros que trabajan en el establecimiento no debe realizarse sin antes implementar mecanismos de control adecuados y firmar un contrato que defina las modalidades de acceso.
BOS_SAT.2.1	Las disposiciones que impliquen el acceso de terceros a las infraestructuras de tratamiento de la información del organismo deben basarse en un contrato realizado en buena y debida forma, que contenga los requerimientos de seguridad necesarios.
BOS_SOT: Subcontratación (§4.3)	
BOS_SOT.1.1	Los requerimientos de seguridad de un organismo que confía a terceros la gestión y el control de todo o parte de sus sistemas informáticos, sus redes y/o sus entornos de oficina deben ser especificados en un contrato acordado entre las partes.
BOS_SOT.1.2	Los contratos de servicios externalizados deben definir las responsabilidades de los contratantes y las posibles acciones en caso de incumplimiento de dicho acuerdo.

3.2.3 BCM : Clasificación y control de los activos (capítulo 5)

BCM_RLC: Responsabilidades vinculadas con los activos (§5.1)	
BCM_RLC.1.1	Debe realizarse un inventario global de los bienes y recursos (incluidas las licencias asociadas), que permita, como mínimo, identificar los elementos delicados y vitales.
BCM_CLI: Clasificación de la información (§5.2)	

BCM_CLI.1.1	Las clasificaciones de la información y las medidas de protección correspondientes deberán contemplar las necesidades de la empresa de compartir o restringir la información y los impactos profesionales asociados a dichas necesidades.
BCM_CLI.1.2	De ser posible, la responsabilidad de la asignación de una clasificación a una información y de la revisión periódica de dicha clasificación debe recaer en el emisor de la información o en su propietario.
BCM_CLI.2.1	Debe definirse un conjunto de procedimientos para el etiquetado y procesamiento de la información conforme al sistema de clasificación adoptado por el organismo.

3.2.4 BSP : Seguridad del personal (capítulo 6)

BSP_SPR: Seguridad en la definición de los puestos y de los recursos (§6.1)	
BSP_SPR.1.1	Los roles y las responsabilidades en materia de seguridad deben estar, en la medida de lo posible, documentados en las definiciones de los puestos, tal como han sido descritos en la política de seguridad del organismo.
BSP_SPR.2.1	Los controles de verificación sobre el personal permanente deben efectuarse al momento de la solicitud de empleo.
BSP_SPR.3.1	Los empleados deben firmar un acuerdo de confidencialidad como parte de sus condiciones iniciales de contratación.
BSP_SPR.4.1	Las condiciones de contratación deberán estipular las responsabilidades del empleado en materia de seguridad.
BSP_FOU: Formación de los usuarios (§6.2)	
BSP_FOU.1.1	Todos los empleados del organismo y, llegado el caso, también los usuarios ajenos al organismo, deben recibir una formación apropiada y actualizaciones regulares sobre la política de seguridad y los procedimientos del organismo.
BSP_FOU.2.1	Todos los empleados del organismo y, llegado el caso, también los usuarios ajenos al organismo, deben recibir una formación apropiada sobre la utilización de las herramientas (especialmente para la puesta en producción de nuevas herramientas).
BSP_RIS: Reacción ante los incidentes de seguridad y fallas de funcionamiento (§6.3)	
BSP_RIS.1.1	Los incidentes de seguridad deben ser informados por el intermediario de los equipos de gestión correspondientes en cuanto son descubiertos.
BSP_RIS.2.1	Los usuarios de servicios de información deben anotar e informar cualquier falla de seguridad observada o sospechada en los sistemas o servicios, o cualquier amenaza a la que pudieran estar expuestos estos últimos.
BSP_RIS.3.1	Deberán establecerse y respetarse diversos procedimientos para informar sobre cualquier mal funcionamiento del software.
BSP_RIS.4.1	Deberán implementarse mecanismos que permitan cuantificar y controlar los tipos, volúmenes y costos de los incidentes y fallas de funcionamiento.
BSP_RIS.5.1	La violación de la política de seguridad y de los procedimientos de seguridad del organismo por parte de los empleados deberá ser tratada siguiendo un procedimiento disciplinario.
BSP_RIS.5.2	Las medidas disciplinarias para la violación de la política de seguridad y de los procedimientos de seguridad deben informarse a todos los empleados.

3.2.5 BPE : Seguridad física y seguridad del entorno (capítulo 7)

BPE_ZOS: Zonas de seguridad (§7.1)	
BPE_ZOS.1.1	Los organismos deben utilizar perímetros de seguridad para proteger las zonas que contienen infraestructuras de tratamiento de la información.
BPE_ZOS.2.1	Las zonas de seguridad deben contar con entradas protegidas por medidas de control adecuadas de tal modo que sólo el personal autorizado pueda tener acceso a dichas zonas.

BPE_ZOS.3.1	Deben crearse zonas de seguridad para proteger las oficinas, salas e infraestructuras con requerimientos de seguridad especiales.
BPE_ZOS.4.1	Deben utilizarse medidas de control y directivas adicionales para trabajar en las zonas de seguridad, a fin de aumentar la seguridad proporcionada por las medidas de seguridad físicas que protegen las zonas de seguridad.
BPE_ZOS.5.1	Las zonas de entrega y de carga deben estar controladas y, en lo posible, aisladas de las infraestructuras de tratamiento de la información, a fin de evitar cualquier acceso no autorizado.
BPE_SEM: Seguridad del hardware (§7.2)	
BPE_SEM.1.1	El hardware debe estar situado y protegido de tal modo que se minimicen los riesgos que representan las amenazas y peligros asociados al entorno y las posibilidades de accesos no autorizados.
BPE_SEM.2.1	El hardware debe estar protegido para evitar que se vea afectado por los cortes de energía eléctrica u otras anomalías eléctricas.
BPE_SEM.3.1	El cableado eléctrico y de telecomunicación que transmite datos o soporta servicios de información debe estar protegido para no que no sea interceptado.
BPE_SEM.3.2	El cableado eléctrico y de telecomunicación que transmite datos o soporta servicios de información debe estar protegido para evitar que pueda ser dañado.
BPE_SEM.4.1	El hardware debe recibir mantenimiento conforme a las instrucciones del fabricante y/o a procedimientos documentados, a fin de garantizar su disponibilidad e integridad en forma continua.
BPE_SEM.5.1	Deben utilizarse procedimientos y medidas de control de seguridad a fin de proteger el hardware utilizado fuera de los locales del organismo.
BPE_SEM.6.1	Las informaciones contenidas en el hardware deben ser borradas antes de desecharlo o reutilizarlo.
BPE_MMG: Medidas de control generales (§7.3)	
BPE_MMG.1.1	Los organismos deben adoptar y aplicar una política de oficinas y pantallas despejadas, para reducir los riesgos de accesos no autorizado, de pérdida de datos o de daños a los datos.
BPE_MMG.2.1	No debe retirarse sin autorización ningún hardware, información ni software.

3.2.6 BGC : Gestión de las comunicaciones y de las operaciones (capítulo 8)

BGC_PRE: Procedimientos y responsabilidades operativas (§8.1)	
BGC_PRE.1.1	Los procedimientos operativos deben ser documentados y conservados.
BGC_PRE.2.1	Los responsables de las infraestructuras involucradas deben controlar las modificaciones realizadas en las infraestructuras de tratamiento de la información y sistemas informáticos.
BGC_PRE.2.2	Las modificaciones realizadas en las infraestructuras de tratamiento de la información y sistemas informáticos deben documentarse.
BGC_PRE.3.1	Deben establecerse responsabilidades y procedimientos de gestión de incidentes, de tal modo que se garantice una reacción rápida, eficaz y ordenada ante cualquier incidente de seguridad.
BGC_PRE.4.1	Las responsabilidades y zonas de responsabilidad deben dividirse de tal modo que se reduzcan las posibilidades de se lleven a cabo modificaciones no autorizadas o se permita abusar de la información o de los servicios.
BGC_PRE.5.1	Las infraestructuras de desarrollo y prueba deberán estar separadas de las infraestructuras operativas.
BGC_PRE.6.1	Antes de utilizar servicios externos para la gestión de las infraestructuras, deberán identificarse por anticipado los riesgos y deberán convenirse con el proveedor las medidas de control adecuadas, incluyéndose estas últimas en el contrato.
BGC_PRS: Planificación y recepción de los sistemas (§8.2)	

BGC_PRS.1.1	Debe vigilarse la demanda de capacidad y deben realizarse previsiones de las futuras necesidades de capacidad a fin de garantizar la disponibilidad de una capacidad adecuada de tratamiento y almacenamiento.
BGC_PRS.2.1	Deben establecerse los criterios de recepción para los nuevos sistemas de información, actualizaciones y nuevas versiones. Deben realizarse ensayos adecuados del sistema antes de su puesta en servicio.
BGC_PLM: Protección contra el software malicioso (§8.3)	
BGC_PLM.1.1	Deben implementarse medidas de control, detección y prevención para proporcionar protección contra el software malicioso, así como procedimientos adecuados de concienciación de los usuarios.
BGC_INT: Administración (§8.4)	
BGC_INT.1.1	Deben realizarse, a intervalos regulares, copias de seguridad de los datos profesionales y de los programas esenciales.
BGC_INT.2.1	El personal operativo debe llevar un registro de sus actividades.
BGC_INT.3.1	Deben informarse las fallas y deben implementarse las medidas correctoras correspondientes.
BGC_GER: Gestión de las redes (§8.5)	
BGC_GER.1.1	Debe implementarse un conjunto de medidas de control a fin de lograr y mantener la seguridad en las redes.
BGC_MSS: Manipulación y seguridad de los soportes de información (§8.6)	
BGC_MSS.1.1	Debe controlarse la gestión de los soportes de información extraíbles, como cintas magnéticas, discos, casetes e informes impresos.
BGC_MSS.2.1	Cuando han dejado de ser útiles, los soportes de información deben ser desechados de un modo seguro.
BGC_MSS.3.1	Deben establecerse procedimientos para la manipulación y almacenamiento de datos, a fin de proteger esta información de cualquier divulgación no autorizada o abuso.
BGC_MSS.4.1	La documentación de los sistemas debe estar protegida contra todo acceso no autorizado.
BGC_EIL: Intercambios de datos y de software (§8.7)	
BGC_EIL.1.1	Deben establecerse convenios, algunos de los cuales podrían ser oficiales, para los intercambios de datos y software entre organismos.
BGC_EIL.2.1	Los soportes de información en tránsito deben protegerse contra todo acceso no autorizado, abuso o alteración.
BGC_EIL.3.1	El comercio electrónico debe protegerse contra las actividades fraudulentas, los litigios contractuales y la divulgación o alteración de la información.
BGC_EIL.4.1	Debe elaborarse una política para el uso del correo electrónico y deben implementarse medidas de control a fin de reducir los riesgos en materia de seguridad generados por el correo electrónico.
BGC_EIL.5.1	Deben elaborarse e implementarse políticas e instrucciones para controlar los riesgos profesionales y los riesgos de seguridad asociados a los sistemas de oficina.
BGC_EIL.6.1	Debe existir un procedimiento de autorización oficial antes de que los datos sean puestos a disposición del público y la integridad de dichos datos debe protegerse de cualquier modificación no autorizada.
BGC_EIL.7.1	Deben implementarse procedimientos y medidas de control para proteger el intercambio de datos mediante comunicaciones de voz, fax y video.

3.2.7 BMA : Control de acceso (capítulo 9)

BMA_EMA: Requerimientos de la empresa respecto del control de acceso (§9.1)	
BMA_EMA.1.1	Deben definirse y documentarse los requerimientos profesionales de control de acceso y los accesos deben limitarse a lo que se ha definido en la política de

	control de acceso.
BMA_GAU: Gestión de los accesos de usuarios (§9.2)	
BMA_GAU.1.1	Debe existir un procedimiento oficial de creación y eliminación de usuarios para el otorgamiento del acceso a todos los sistemas y servicios informáticos destinados a múltiples usuarios.
BMA_GAU.2.1	La asignación y el uso de privilegios deben restringirse y controlarse.
BMA_GAU.3.1	La asignación de contraseñas debe controlarse mediante un procedimiento de gestión oficial.
BMA_GAU.4.1	Debe ejecutarse, a intervalos regulares, un procedimiento de revisión de los derechos de acceso de los usuarios.
BMA_REU: Responsabilidades de los usuarios (§9.3)	
BMA_REU.1.1	Los usuarios deben respetar las buenas prácticas en materia de seguridad para la elección y utilización de contraseñas.
BMA_REU.2.1	Los usuarios deben procurar que el hardware no vigilado cuente con una protección de seguridad adecuada.
BMA_MAR: Control de acceso a las redes (§9.4)	
BMA_MAR.1.1	Los usuarios no deben poder acceder directamente a los servicios específicos que están autorizados a utilizar.
BMA_MAR.2.1	La ruta entre las terminales de usuarios y el servicio informático debe ser controlada.
BMA_MAR.3.1	El acceso por parte de usuarios remotos debe ser autenticado.
BMA_MAR.4.1	Las conexiones a sistemas informáticos remotos deben autenticarse.
BMA_MAR.5.1	El acceso a los puertos de diagnóstico debe ser controlado de manera segura.
BMA_MAR.6.1	Deben introducirse medidas de control en las redes, a fin de aislar grupos de servicios de información, usuarios y sistemas de información.
BMA_MAR.7.1	En las redes compartidas, la capacidad de conexión de los usuarios debe restringirse, conforme a la política de control de acceso del punto BMA_EMA.1.1.
BMA_MAR.8.1	Las redes compartidas deben contar con medidas de control del encaminamiento de tal modo que las conexiones de ordenadores y el flujo de datos no infrinjan lo especificado en el punto BMA_EMA.1.1.
BMA_MAR.9.1	Debe proporcionarse una descripción clara de las características de seguridad de todos los servicios utilizados por el organismo.
BMA_MAS: Control de acceso a los sistemas de gestión (§9.5)	
BMA_MAS.1.1	Debe usarse una identificación automática de la terminal para autenticar las conexiones a establecimientos específicos y al hardware portátil.
BMA_MAS.2.1	El acceso a los servicios de información debe realizarse mediante un proceso de conexión segura.
BMA_MAS.3.1	Todos los usuarios deben tener una identificación única (código de identificación de usuario) para su uso personal exclusivo, de tal modo que las actividades pueden vincularse retrospectivamente con el individuo responsable.
BMA_MAS.4.1	Los sistemas de gestión de contraseñas deben ofrecer una función interactiva eficaz que garantice la calidad de las contraseñas (sin contraseñas demasiado cortas o demasiado simples, sin reutilización de contraseñas anteriores...).
BMA_MAS.5.1	El uso de programas utilitarios debe restringirse y controlarse estrictamente.
BMA_MAS.6.1	Debe proporcionarse una alarma individual a los usuarios que pudieran llegar a verse sometidos a algún tipo de coerción.
BMA_MAS.7.1	Las terminales no utilizadas situadas en las zonas de alto riesgo o comunicadas con sistemas de alto riesgo deben apagarse automáticamente luego de un período de inactividad determinado, a fin de impedir que personas no autorizadas puedan acceder a las mismas.
BMA_MAS.8.1	Debe usarse la limitación del tiempo de conexión para proporcionar un nivel de seguridad adicional para las aplicaciones de alto riesgo.

BMA_MAA: Control de acceso a las aplicaciones (§9.6)	
BMA_MAA.1.1	Los accesos a la información y a las funciones de los sistemas de aplicaciones deben limitarse conforme a la política de control de acceso especificada en el punto BMA_EMA.1.1.
BMA_MAA.2.1	Los sistemas críticos deben contar con un entorno informático dedicado (aislado).
BMA_SAS: Vigilancia de los accesos a los sistemas y de su utilización (§9.7)	
BMA_SAS.1.1	Deben elaborarse y mantenerse registros de auditoría donde se registrarán las excepciones y otros acontecimientos referidos a la seguridad, durante un período convenido, para facilitar las investigaciones futuras y el control de las medidas de supervisión de los accesos.
BMA_SAS.2.1	Deben establecerse procedimientos para la vigilancia del uso de las infraestructuras de tratamiento de la información y el resultado de estas actividades de vigilancia debe analizarse regularmente.
BMA_SAS.3.1	Los relojes de los ordenadores deben estar sincronizados a fin de obtener un registro exacto.
BMA_IMT: Informática móvil y teletrabajo (§9.8)	
BMA_IMT.1.1	Debe establecerse una política oficial y deben adoptarse medidas de control adecuadas para brindar protección contra los riesgos que representan el trabajo con unidades informáticas móviles.
BMA_IMT.2.1	Deben establecerse políticas y procedimientos para la autorización y control de las actividades de teletrabajo.

3.2.8 BDM : Desarrollo y mantenimiento de los sistemas (capítulo 10)

BDM_ESS: Requerimientos de seguridad de los sistemas (§10.1)	
BDM_ESS.1.1	Las especificaciones de la empresa para la adquisición de nuevos sistemas o la realización de mejoras en sistemas existentes deben especificar los requerimientos referidos a medidas de control.
BDM_SSA: Seguridad de los sistemas de aplicaciones (§10.2)	
BDM_SSA.1.1	Los datos de entrada de los sistemas de aplicaciones deben ser validados para garantizar que son correctos y adecuados.
BDM_SSA.2.1	Deben incorporarse a los sistemas verificaciones de validación que permitan detectar cualquier alteración de los datos procesados.
BDM_SSA.3.1	Debe utilizarse la autenticación de los mensajes para las aplicaciones que son objeto de un requerimiento de seguridad en cuanto a la protección del contenido de los mensajes.
BDM_SSA.4.1	Los datos de salida de un sistema de aplicaciones deben ser validados para garantizar que el procesamiento de los datos almacenados sea correcto y adecuado a las circunstancias.
BDM_COC: Medidas criptográficas (§10.3)	
BDM_COC.1.1	Debe elaborarse y respetarse una política de uso de comandos criptográficos para la protección de los datos.
BDM_COC.2.1	Debe utilizarse la encriptación para proteger las informaciones confidenciales o cruciales.
BDM_COC.3.1	Deben utilizarse firmas digitales para proteger la autenticidad y la integridad de la información electrónica.
BDM_COC.4.1	Deben utilizarse servicios de no repudio para solucionar cualquier discrepancia sobre la aparición o la no aparición de un acontecimiento o de una acción.
BDM_COC.5.1	Debe utilizarse un sistema de gestión basado en un conjunto convenido de normas, procedimientos y métodos, a fin de apoyar el uso, por parte del organismo, de los dos tipos de técnicas criptográficas.
BDM_SFS: Seguridad de los archivos (§10.4)	

BDM_SFS.1.1	Debe aplicarse un control para la instalación de software en los sistemas operativos.
BDM_SFS.2.1	Los datos de prueba deben protegerse y controlarse.
BDM_SFS.3.1	Debe realizarse constantemente un estricto control del acceso a las bibliotecas de los códigos fuente.
BDM_SED: Seguridad de los entornos de desarrollo y de asistencia técnica (§10.5)	
BDM_SED.1.1	La aplicación de las modificaciones deben controlarse de manera estricta utilizando procedimientos de control de las modificaciones tendientes a minimizar la alteración de los sistemas de información.
BDM_SED.2.1	Cuando se realizan modificaciones, debe realizarse también una revisión y una prueba de los sistemas de aplicaciones.
BDM_SED.3.1	Es necesario desalentar la realización de modificaciones en los paquetes de programas y las modificaciones esenciales deben controlarse estrictamente.
BDM_SED.4.1	La compra, uso y modificación de software debe ser vigilada y controlada a fin de protegerlo de cualquier posibilidad de introducción de puntos de acceso ocultos y troyanos.
BDM_SED.5.1	Deben aplicarse medidas de control para proteger el desarrollo subcontratado de software.

3.2.9 BCA : Gestión de la continuidad de las actividades del organismo (capítulo 11)

BCA_AGC: Aspectos de la gestión de la continuidad de las actividades del organismo (§11.1)	
BCA_AGC.1.1	Debe establecerse un procedimiento controlado en todo el organismo para el desarrollo y resguardo de la continuidad de las actividades profesionales.
BCA_AGC.2.1	Debe elaborarse un plan estratégico basado en una adecuada evaluación de los riesgos, a fin de determinar el enfoque global respecto de la continuidad de las actividades profesionales.
BCA_AGC.3.1	Deben elaborarse diversos planes para mantener o restablecer las actividades profesionales en los plazos requeridos, tras una interrupción o fallo de procesos profesionales cruciales.
BCA_AGC.4.1	Debe mantenerse un solo marco de planificación de continuidad de las actividades profesionales a fin de lograr una coherencia de todos los planes e identificar las prioridades en materia de pruebas y mantenimiento.
BCA_AGC.5.1	Deben realizarse ensayos y mantenimiento continuo, mediante revisiones regulares, de los planes de continuidad de las actividades profesionales, a fin de garantizar que estén actualizados y que sean eficaces.

3.2.10 BCO : Conformidad (capítulo 12)

BCO_CEL: Conformidad con los requisitos legales (§12.1)	
BCO_CEL.1.1	Todos los requisitos legales, reglamentarios y contractuales para cada sistema informático deben definirse explícitamente y documentarse.
BCO_CEL.2.1	Deben aplicarse procedimientos adecuados para garantizar que se actúe conforme a los requisitos legales en lo referido al uso de productos para los cuales podrían existir derechos de propiedad intelectual y al uso de software propietario.
BCO_CEL.3.1	Los registros importantes del organismo deben protegerse de cualquier daño, destrucción o falsificación.
BCO_CEL.4.1	Deben aplicarse medidas de control para proteger los datos personales conforme a la legislación pertinente.
BCO_CEL.5.1	La dirección debe autorizar el uso de las infraestructuras de tratamiento de la información y deben aplicarse medidas de control para impedir el uso abusivo de dichas infraestructuras.

BCO_CEL.6.1	Deben establecerse medidas de control para garantizar la conformidad con los convenios, leyes, reglamentos nacionales y demás instrumentos que tienen por objeto controlar el acceso a los comandos criptográficos o su utilización.
BCO_CEL.7.1	Cuando una acción contra una persona supone un acción legal civil o penal, las pruebas presentadas deben establecerse conforme a las normas prescritas para las pruebas en la ley pertinente o en la reglamentación de la jurisdicción específica involucrada.
BCO_CEL.7.2	Cuando una acción contra una persona supone un acción legal, civil o penal, las pruebas presentadas deben establecerse conforme a cualquier norma o código de buenas prácticas aplicable a la conformación de pruebas admisibles .
BCO_RPS: Controles de la política de seguridad y de la conformidad técnica (§12.2)	
BCO_RPS.1.1	Los responsables deben procurar que todos los procedimientos de seguridad de su sector de responsabilidad se cumplan correctamente.
BCO_RPS.1.2	Todos los sectores dentro del organismo deben someterse a revisiones regulares para garantizar su conformidad con las políticas y normas de seguridad.
BCO_RPS.2.1	Los sistemas informáticos debe verificarse regularmente para verificar su conformidad con las normas de implementación de la seguridad.
BCO_CAS: Consideraciones sobre las auditorías de los sistemas (§12.3)	
BCO_CAS.1.1	Las auditorías de los sistemas operativos deben planificarse y aprobarse de tal modo que se minimicen los riesgos de alteración de los procesos profesionales.
BCO_CAS.2.1	El acceso a las herramientas de auditoría de los sistemas debe protegerse a fin de impedir que se comprometa la seguridad de las mismas o que se abuse de ellas.

3.3 políticas de seguridad de los sistemas de información (PSSI)

3.3.1 PSI : Política de seguridad

PSI-01: Evolución de la PSSI

Un organismo puede cambiar en el transcurso del tiempo (organización, misiones, perímetro de acción, ejes estratégicos, valores). En consecuencia, su sistema de información sufrirá frecuentes modificaciones, al igual que las amenazas y vulnerabilidades que lo afectan. Es conveniente, por lo tanto, prever una revisión de la PSSI:

- cada vez que se produce un modificación importante del contexto o del SI;

- en caso de evolución de la amenaza;

- en caso de evolución de las necesidades de seguridad;

- tras una auditoría;

- luego de un incidente de seguridad;

- sistemáticamente, a intervalos definidos;

- a petición de una autoridad (responsable de la seguridad, dirección....), en el marco de un procedimiento que debe definirse en la PSSI.

PSI-02: Difusión de la PSSI

La PSSI, al igual que todas sus consecuencias operativas, debe estar perfectamente documentada y las versiones de referencia actualizadas deben ser perfectamente accesibles para todo el personal del organismo.

La PSSI debe ser conocida por todos los actores internos y, llegado el caso, por todas las personas que tengan acceso al sistema de información del organismo (subcontratados, prestadores, becarios...).

Sin embargo, debe tenerse en cuenta que la PSSI puede contener datos confidenciales y los miembros del personal del organismo pueden verse afectados de manera diferenciada en función del rol que cumplen. Por ello, se recomienda, si fuera necesario, elaborar y difundir síntesis que puedan incluir fragmentos más detallados para la información pertinente en función de los distintos tipos de lectores. El objetivo de estas síntesis es permitir a cada actor conocer los objetivos y las normas de seguridad, en función de sus necesidades.

PSI-02: Difusión de la PSSI

PSI-03: Control de la aplicación de la SSI

Es oportuno prever procedimientos y medios de control interno de la aplicación de la PSSI, complementándolos con procedimientos y medios de auditoría externos. Publicar normas sin hacerse de los medios para controlar su aplicación no es una situación aceptable, especialmente desde el punto de vista de la seguridad.

PSI-04: Protección de la información confiada al organismo

Este principio permite garantizar la exhaustividad de las referencias reglamentarias.

La información provisoriamente en poder del organismo y que contiene una clasificación o una indicación particular de protección establecida por su propietario, debería protegerse rigurosamente, utilizando las mismas medidas aplicadas por el organismo de origen. Estas medidas pueden derivarse de la aplicación de los textos legales (Ley Nº 78-17 del 6 de enero de 1978 referida a la informática, a los ficheros y las libertades...), de las instrucciones

	interministeriales como, por ejemplo, la que trata sobre el respeto de la clasificación de los datos vinculados con el secreto de defensa [IGI 900], de la protección de los datos que afectan al patrimonio nacional [II 486] o de lo establecido mediante un contrato de defensa [II 2000]. En caso de que estas normas no provengan de reglamentaciones comunes, es conveniente establecer por contrato el compromiso de las partes respecto de la información que intercambian entre sí.
PSI-05: Adopción de una escala de necesidades	La adopción de una escala de necesidades basada en diferentes criterios de seguridad (disponibilidad, integridad, confidencialidad...) permitirá facilitar la clasificación objetiva de los elementos esenciales del organismo (información y funciones). El procedimiento metodológico de la guía de PSSI propone un enfoque para elaborar una escala de necesidades. Especifica que deben determinarse una ponderación y valores de referencia para cada uno de los criterios de seguridad. Los valores de referencia deben ser objetivos, propios del organismo y deben estar vinculados con sus orientaciones estratégicas. Por otra parte, en el plan tipo propuesto en la guía de PSSI, se recomienda incluir esta escala en la PSSI.
PSI-06: Criterios para la determinación de las necesidades de seguridad	El procedimiento metodológico de la guía de PSSI propone un enfoque para determinar las necesidades de seguridad (en términos de disponibilidad, integridad, confidencialidad...) de los elementos esenciales (información y funciones) según la escala de necesidades adoptada. Se presentan dos casos para los elementos esenciales identificados: - se utilizará directamente esta escala de necesidades para aquellos elementos que no tienen clasificación; - se establecerá la correspondencia entre esta escala de necesidades y aquellos elementos que ya poseen una clasificación (por ejemplo, los datos protegidos por el secreto de defensa, datos delicados, vitales.....). Fuera de, principalmente, los datos afectados por el secreto de defensa y los datos personales para los cuales deben aplicarse los textos legales vigentes, las necesidades de seguridad se determinarán en función del control del origen de la información, la estimación de su interés y validez respecto de su ciclo de vida en el proceso operativo de producción: - El control del origen de los datos (de origen extranjero, de dominio público, provenientes de clientes o proveedores...) reviste una gran importancia para la seguridad. Pueden preverse criterios específicos en función del origen de los datos, para evaluar, antes de su recogida, si podría llegar a verse comprometida su exactitud, su validez o su correcta presentación para el sistema. - La estimación del interés y la validez de la información recogida se realiza mediante la aplicación de criterios claramente definidos por la dirección del organismo y que pueden estar centrados en un área particular (I+D, control de

calidad, vigilancia tecnológica...).

Observación sobre la información delicada:

La información delicada es aquella cuya divulgación o alteración puede atentar contra los intereses del Estado o contra los intereses del organismo al que el perjuicio financiero producido podría, por ejemplo, llevar a la quiebra. En consecuencia, es necesario garantizar principalmente la confidencialidad de dicha información y, bastante a menudo, responder a una necesidad importante de integridad.

Los datos clasificados en esta categoría son:

- Por una parte, los datos protegidos por el secreto de defensa tal como lo define el artículo 5 de la [IGI 900]. El organismo es responsable por el cumplimiento de las normas de clasificación especificadas en la reglamentación y tiene, además, la obligación de implementar los medios necesarios para actuar conforme a la reglamentación.

- Por otra parte, los datos delicados no clasificados de defensa tal como lo define el artículo 4 de la [REC 901], es decir, aquellos vinculados con la misión o el oficio del organismo (por ejemplo, con el know-how tecnológico o el secreto profesional), aquellos referidos a propuestas comerciales, o incluso a los datos sobre el estado de la seguridad (por ejemplo, los resultados de auditorías internas).

La clasificación adoptada apuntará, en primer lugar, a brindar al usuario una justa apreciación de la sensibilidad de la información con la que trabaja, y, en segundo lugar, a facilitar el control y, en consecuencia, a mejorar la protección de la información delicada. Para aquellos datos no considerados en la [IGI 900], la clasificación elegida debe ser aprobada por el organismo.

Observación sobre la información vital:

Los datos considerados "vitales" son aquellos cuya existencia es necesaria para el buen funcionamiento del organismo. En consecuencia, es necesario garantizar principalmente la disponibilidad de dicha información y, muy a menudo, satisfacer una necesidad importante de integridad.

Los datos que pueden considerarse vitales son:

- Por una parte, los datos protegidos por el secreto de defensa tal como lo define el artículo 6 de la [IGI 900].

- Por otra parte, los datos no protegidos por el secreto de defensa tal como lo define el artículo 5 de la [REC 901] pero que son necesarios para el funcionamiento del sistema, así como los datos derivados del ámbito de aplicación del artículo 5 (por ejemplo, las nomenclaturas de los artículos para una unidad de producción).

La clasificación seleccionada apunta, en primer lugar, a brindar al usuario una justa apreciación de la sensibilidad de la información con la que trabaja, y, en

segundo lugar, a facilitar el control y, en consecuencia, a mejorar la protección de la información vital. Para aquellos datos no considerados en la [IGI 900], la clasificación elegida deberá ser aprobada por el organismo.

Puede preverse la especificación de un umbral mínimo de disponibilidad de la información vital (procesada o necesaria para procesar), por debajo del cual el sistema de información se declarará inoperante.

Observación sobre la información estratégica:

La información estratégica está conformada por datos cuyo conocimiento es necesario para lograr los objetivos derivados de las orientaciones estratégicas del organismo. Dicha información puede estar protegida por la legislación, pero debe igualmente resguardarse mediante contratos, convenios o protocolos de acuerdo enmarcados en el Código Civil.

La clasificación adoptada apuntará, en primer lugar, a brindar al usuario una justa apreciación de la sensibilidad de la información con la que trabaja, en segundo lugar, a facilitar el control y, en consecuencia, a mejorar la protección de la información estratégica. Puede apoyarse en criterios propios del organismo como, por ejemplo, el sector particular (estudios, innovaciones, contratos...) al que pertenece dicha información, el valor que se le ha dado y su validez en el tiempo. Para aquellos datos no considerados en la [IGI 900], la clasificación elegida deberá ser aprobada por el organismo.

Observación sobre la información personal:

El artículo 4 de la Ley "Informática y libertades" define la noción de información personal: "Los datos personales son aquellos que permiten, de alguna forma, sea directa o no, la identificación de las personas físicas a las cuales se aplican, siendo el proceso realizado por una persona física o jurídica".

La clasificación adoptada apuntará, en primer lugar, a facilitar el control y, en consecuencia, a mejorar la protección de los datos personales conforme a la Ley. Dicha clasificación puede basarse en criterios propios del organismo como, por ejemplo, un área particular (área médica, contrataciones...), el tipo de sondeo o encuesta, el lugar de procesamiento o de almacenamiento.

Observación sobre la información costosa:

Los datos costosos son datos que forman parte del patrimonio del organismo y cuya recogida, procesamiento, almacenamiento o transmisión requieren una gran inversión de tiempo o un elevado costo de adquisición. Las disposiciones legales enumeradas para los datos estratégicos pueden aplicarse también a esta categoría.

La clasificación adoptada apuntará, en primer lugar, a brindar al usuario una justa apreciación de la sensibilidad de la información con la que trabaja, y, en

	segundo lugar, a facilitar el control y, en consecuencia, a mejorar la protección de la información costosa. Dicha clasificación puede basarse en criterios propios del organismo como, por ejemplo, un sector particular (estudios, innovaciones...), el origen de los datos y el nivel de costo.
PSI-07: "Liberación" de la información	La clasificación de una información se asigna, a veces, para determinado período de tiempo. Las normas aplicables deberán definir los períodos mínimos en función del tipo de datos.
PSI-08 : "Sobreclasificación" de los datos	El grado de protección debe ser proporcional a la clasificación de los datos y sistemas. Si bien el uso de una clasificación alta parece garantizar una mejor protección, el recurso sistemático a la "sobreclasificación" podría acarrear una pérdida de confianza en el método de clasificación. Para impedir esto, es conveniente: - evitar la sobreclasificación de la información; - revisar periódicamente la clasificación asignada.
PSI-09: Identificación y alcance de la clasificación de una información	La identificación de la clasificación debe ser clara, conocida por todos e inmediatamente reconocible. La clasificación de la información debe integrarse: al manual de identidad corporativa, para los documentos; a los procedimientos de gestión de los soportes de información, para los disquetes y demás soportes informáticos; a los procedimientos de organización de los recursos informáticos, para los ficheros. Deben identificarse también las máquinas que forman parte de una red que procesa o alberga datos confidenciales. Es importante que el personal sea conciente de que la clasificación de su organismo puede no ser equivalente a una clasificación indicada para datos provenientes de otros organismos. A la inversa, la clasificación definida para el organismo podría tener sentido sólo dentro del perímetro de la PSSI.
PSI-10: Definición y control de los permisos	El organismo propietario de la información debe ser capaz de asignar permisos para el uso de dicha información y debe definir las normas de gestión de los permisos y efectuar los controles correspondientes. El organismo puede, sin ser necesariamente el propietario de los datos en un momento dado, ser su depositario. En este caso, no dispone de poder de decisión respecto de la información procesada pero debe respetar las normas de gestión definidas por el propietario (clientes, subcontratistas...) en función de la clasificación atribuida a dicha información.
PSI-11: Criterios de difusión interna de la información	A fin de evitar las indiscreciones y las fugas de información, los datos y, en general, sus soportes, sólo deben poder utilizarse en un entorno que responsa a los requerimientos de seguridad definidos por el organismo. El control de la difusión interna de información tiene por objetivo asegurarse de que los datos se encuentran disponibles exclusivamente para las personas que tienen necesidad de conocerlos para desempeñar sus tareas. La implementación de controles permitirá también verificar que la copia de información se realice conforme a las prerrogativas previstas por la Ley (derechos de autor, copyright), a la reglamentación (secreto de defensa) y a

las restricciones específicas del organismo.

La necesidad de conocer la información (que tiene que ver con su confidencialidad) puede extenderse a las necesidades de modificarla (integridad), de utilizarla (disponibilidad)...

PSI-12: Criterios de difusión externa de la información

Poner a disposición sin ningún control datos que requieren protección puede perjudicar al organismo (por ejemplo, provocando una pérdida de credibilidad o de imagen de marca, permitiendo la apropiación del know-how...).

La implementación de determinados criterios permitirá asegurarse de que los datos transmitidos fuera del organismo, si son de tipo confidencial, suponen un control previo de autorización del receptor o un cláusula contractual que vincule a los organismos involucrados. Cuando se trate de datos personales, la comunicación deberá realizarse conforme a la Ley.

Por otra parte, puede preverse, siguiendo ese mismo principio, que sólo el personal autorizado pueda realizar la difusión de información fuera del organismo, cumpliendo con un procedimiento de autorización previa.

3.3.2 ORG : Organización de la seguridad

ORG-01: Responsabilidades generales en cuanto a la seguridad del sistema de información del organismo

El nombramiento de un responsable de la seguridad de los sistemas de información (RSSI o equivalente) es necesario para garantizar la responsabilidad global de la elaboración, implementación y funcionamiento de la gestión de la SSI en el organismo. Este RSSI (terminología habitual que se utilizará en este documento) estará a cargo del cumplimiento de la PSSI en todos los niveles y áreas del organismo.

Este responsable, subordinado a la dirección del organismo, debe poder hacer prevalecer la seguridad por sobre los intereses particulares e integrar la seguridad en todos los proyectos que afecten a los sistemas de información.

La implementación de esta función es una señal clara y necesaria de la importancia que el organismo atribuye a su PSSI.Dentro de las instituciones del estado, la estructura funcional de SSI cubre estas responsabilidades.

ORG-02: Las responsabilidades en cuanto a la elaboración e implementación de una PSSI

La PSSI involucra a todas las funciones vitales de un organismo. Ciertamente, el organismo no podría, por lo general, soportar un fallo prolongado de su o sus sistemas de información.

Por ello, la PSSI reviste un interés estratégico: debe existir una norma que defina las responsabilidades en cuanto a su elaboración y sus inevitables evoluciones, dentro, por ejemplo, de un comité coordinador.

Además, en la fase de implementación de la PSSI, esta norma establecerá las responsabilidades de las autoridades calificadas en la implementación y control de las instrucciones de seguridad para la instalación y gestión de los medios que conforman el sistema de información.

Dicha norma destaca, especialmente, la necesidad de una integración de la seguridad a partir del diseño y desarrollo de cualquier nuevo proyecto que afecte al sistema de información. La PSSI indica también que la seguridad del SI no se limita a los aspectos y evoluciones técnicas sino que engloba también cualquier evolución o modificación de la organización, de las misiones...

ORG-03 : Alcance de las responsabilidades

El principio general de concienciación de la OCDE enuncia lo siguiente: "Las atribuciones y responsabilidades de los propietarios, proveedores, usuarios del sistema de información y demás partes involucradas en la seguridad de los sistemas de información deben expresarse en forma explícita".

Es fundamental que todas las áreas involucradas en la seguridad (seguridad de las infraestructuras, seguridad dentro de los proyectos y familias de aplicación, seguridad de los locales, documentación de seguridad...) cuenten con un responsable designado a tal fin y que todas las tareas referidas a las seguridad hayan sido asignadas.

La organización de la seguridad en cada una de estas áreas debe incluir los niveles estratégico, de conducción y operativo.

Debe existir una identificación clara y única de la responsabilidad en materia de seguridad vinculada con las redes o sistemas transversales como, por ejemplo, la red ofimática de una empresa o el dispositivo de acceso a las redes externas.

ORG-04: Responsabilidades del nivel de toma de decisiones

Corresponde al nivel de la toma de decisiones adoptar cualquier disposición necesaria para diseñar e implementar una seguridad adaptada a las necesidades y objetivos del organismo y garantizar el cumplimiento de la PSSI.

(1) Para un organismo ministerial, este nivel corresponde al del alto funcionario de Defensa (AFD) a quien delega responsabilidades el ministro. Él es responsable por la aplicación de las disposiciones referidas a la seguridad de defensa, a la protección del secreto y a la seguridad de los sistemas de información.

Puede colaborar con él, en su misión, un funcionario de seguridad de los sistemas de información (FSSI) cuyas principales misiones son ([IGI 900], artículo 19 y [REC 901], artículo 18):

- especificar las modalidades de aplicación de las instrucciones interministeriales;

- elaborar y controlar la aplicación de las instrucciones particulares de su ministerio;

- organizar la concienciación de las autoridades;

- garantizar el vínculo con las comisiones interministeriales y ministeriales especializadas.

(2) Para un organismo público o privado, este nivel es aquel de un alto responsable de la seguridad a quien delega responsabilidades el comité de dirección. Un comité de seguridad puede asistirle en sus funciones.

El comité de dirección establece, a petición del alto responsable de la seguridad, las grandes orientaciones en materia de SSI, respetando los objetivos del organismo y las diferentes políticas implementadas (política de gestión del personal, presupuestaria, de producción...). Este comité puede ser, además, la instancia de validación de la PSSI.

El alto responsable de la seguridad vela por la aplicación de la PSSI. También participa de las deliberaciones del comité de dirección, del cual es asesor, vinculadas con todas las cuestiones referidas a la seguridad como, por ejemplo, la definición de los objetivos, la asignación de los recursos y del personal.

El comité de seguridad, presidido por el alto responsable de seguridad, reúne a los responsables de la seguridad de las diferentes áreas del organismo. Dicho comité velará por la coordinación de la implementación de la PSSI, verificando especialmente la coherencia de las normas de seguridad y resolviendo los eventuales conflictos con las demás normas y prácticas en uso en el organismo.

(3) Si las necesidades del organismo lo requieren, puede formarse un equipo de seguridad del sistema de información, a disposición del alto funcionario de Defensa (o del alto responsable de la seguridad). Dicho equipo reunirá a especialistas en informática y en redes de telecomunicación, pero también a responsables de los aspectos no tecnológicos de los sistemas de información, que habrán recibido formación en seguridad. Las principales misiones de este equipo serán:

- la preparación y coordinación de las actividades de seguridad;

- la evaluación periódica de las vulnerabilidades;

- la búsqueda de soluciones técnicas y la elaboración de procedimientos;

- la implementación de programas de concienciación y de formación;

- la realización de peritajes de seguridad a petición del comité de dirección.

El equipo de seguridad puede estar compuesto por miembros permanentes pero podrá también, en función de las necesidades (por ejemplo, de grandes proyectos de evolución importante del SI) incorporar temporalmente algunos especialistas o expertos de las áreas involucradas.

ORG-05: Responsabilidades del nivel de conducción

Si el tamaño del organismo lo justifica, podrán identificarse subconjuntos (establecimientos, partes del SI, divisiones...) y nombrarse responsables "locales", implementándose una delegación de responsabilidad claramente definida y una organización eficaz de la coordinación con la estructura central.

Para un organismo ministerial, este nivel corresponde al de las autoridades calificadas que son responsables de la seguridad del sistema de información que tienen a su cargo ([IGI 900], artículo 20 y [REC 901], artículo 19).

Para un organismo privado, este nivel es el de un interlocutor local en materia de seguridad, cuya función se centrará en la SSI y que formará parte del equipo dirigido por el RSSI.

Su misión es conducir la implementación de la PSSI en su nivel (dirección, departamento, establecimiento...) y, más precisamente:

- garantizar el cumplimiento de las disposiciones contractuales y reglamentarias;

- elaborar las instrucciones y directivas internas;

- garantizar que los controles internos de seguridad se realicen correctamente;

- organizar la concienciación del personal.

Estas autoridades pueden apoyarse en las competencias del equipo de seguridad.

Para cumplir con las misiones de conducción de la SSI, resulta a veces necesario conformar comités coordinadores dedicados:

- al seguimiento de la aplicación de la PSSI;

- al tratamiento de crisis vinculadas con la seguridad del sistema de información;

- a la vigilancia tecnológica, al seguimiento de las necesidades del organismo en materia de SSI y a la evolución de la PSSI.

ORG-06: Responsabilidades del nivel operativo

En todos los niveles, las autoridades jerárquicas son personalmente responsables por la aplicación de las medidas, definidas por las autoridades calificadas, destinadas a garantizar la seguridad de los sistemas de información ([IGI 900], artículo 20 y [REC 901], artículo 19).

Todo el personal que pertenece o trabaja en el organismo está involucrado en la SSI y tiene responsabilidades que deben formalizarse claramente y darse a conocer a cada uno.Las responsabilidades y compromisos del personal (ver los principios de seguridad referidos a las obligaciones contractuales) abarcan, especialmente:

- el cumplimiento de las leyes y reglamentos,

- el cumplimiento de la política y normas específicas (vinculadas con un proyecto, un establecimiento, una función particular),

- el acceso a una red o a locales en otro organismo.

Estas responsabilidades pueden ser reforzadas en función de las funciones y permisos del personal (ver los principios de seguridad referidos a los permisos). Los administradores de los sistemas de información, por ejemplo, que son poseedores de claves y gestionan funciones delicadas de los SI, tendrán responsabilidades especiales en el ámbito de la SSI.

Por otra parte, las responsabilidades de los miembros del personal del organismo deben abarcar también los casos en que estos trabajan en otro SI ajeno al organismo al que pertenecen (clientes, asociados...).

ORG-07: Otros responsables del organismo que desempeñan algún papel en la SSI

Existen otras funciones no dedicadas a la seguridad pero que desempañan, sin embargo, roles especiales, indispensables para el funcionamiento la SSI.

Estas funciones son:

- Los agentes o interlocutores en materia de seguridad.

Para permitir a cada establecimiento, departamento o unidad la implementación de las instrucciones y procedimientos, las autoridades jerárquicas recurren a la ayuda de uno o varios agentes de seguridad, encargados principalmente de la interfaz entre los usuarios del sistema de información y los responsables del seguimiento de la SSI.

El objetivo que se persigue es doble:

o facilitar la difusión de la información de seguridad y la aplicación de las normas de buen uso;

o garantizar el envío de información por parte de los usuarios al equipo que tiene a su cargo el seguimiento centralizado de la seguridad.

Este rol deben desempeñarlo personas "cercanas" a los usuarios desde el punto de vista geográfico y profesional.

Estos agentes serán los interlocutores privilegiados del equipo de seguridad.

Pueden también tener a su cargo los recursos comunes de varias unidades operativas. Su función será, entonces, la implementación de las medidas de protección compatibles con los objetivos de las unidades y la resolución local de los problemas de seguridad. La falta de tales medidas podría provocar un arbitraje difícil entre una tarea funcional y una acción de seguridad.

- Los responsables jurídicos del organismo.

Estos desempeñan un papel indispensable en el área de la SSI del organismo. Intervienen, por iniciativa del RSSI, en diversas áreas, entre las cuales se destacan:

o la redacción de cláusulas de confidencialidad y los compromisos de SSI en los contratos comerciales y en los contratos de contratación de personal;

o la presentación de denuncias y la instrucción de causas;

o la integración de las normas de SSI en los diversos reglamentos y cartas orgánicas;

o las relaciones con los subcontratistas,

o las responsabilidades de los auditores.

Además de las responsabilidades de control asignadas a las tareas operativas, los auditores tienen a su cargo las siguientes misiones:

o definir la estrategia de auditoría, abarcando especialmente la estrategia de las auditorías de SSI;

o realizar o hacer realizar, conjuntamente con el RSSI, auditorías de SSI, según su plan de auditorías o a petición de las diferentes direcciones;

o informar a la entidad contratante y a las entidades auditadas, según su necesidad de conocerlo, e informar al RSSI, sobre la identificación de eventuales incidentes o anomalías en la SSI;

o otras responsabilidades que puedan requerirse para efectuar las acciones específicas de seguridad definidas, por ejemplo, dentro de los planes de mejora de la seguridad, de migración de aplicaciones, etc.

ORG-08: Entidades específicas dedicadas a la gestión y coordinación de la seguridad

Pueden crearse otras entidades específicas. Entre estas entidades, podemos citar especialmente:

- Un comité de seguridad, responsable del mantenimiento de la PSSI y del seguimiento de la implementación del plan de acción prioritario. También tendrá a su cargo mantener informada a la Dirección General sobre la eficacia de la política implementada.

	- Una célula de crisis, encargada, llegado el caso, de la implementación de un procedimiento de emergencia para hacer frente a una crisis. - Un equipo de vigilancia tecnológica, encargado del seguimiento de las alertas de seguridad y de su tratamiento según la pertinencia de las mismas.- Un equipo de auditoría, encargado de la realización efectiva de las auditorías del sistema de información.
ORG-09: Aplicación de la noción de responsable-poseedor	La noción de responsable-poseedor se refiere al responsable jerárquico de una unidad orgánica (establecimiento, departamento, centro de responsabilidades o de beneficio) o a la autoridad calificada tal como se la define en el principio ORG-05, "Responsabilidades del nivel de conducción", y que dispone de sus propios recursos humanos y materiales para llevar a cabo su misión. El término "posesión" se aplica al patrimonio de información, al software y al hardware que conforma el sistema de información y supone la obligación de respetar las leyes, reglamentos y normas vigentes en el organismo. La información, el software y el hardware involucrados pueden pertenecer al organismo o haber sido confiados al organismo por terceros (clientes, asociados, prestadores...). El responsable-poseedor determina los niveles de riesgo aceptables y las condiciones de acceso a los ficheros, de actualización de los datos (en conformidad con las normas de clasificación vigentes en el organismo) o de modificaciones del software y del hardware del que dispone.
ORG-10: Aplicación de la noción de responsable-depositario	El responsable-depositario recibe delegación del responsable-poseedor para la aplicación de las leyes, reglamentos y normas de protección referidas a la información, el software y el hardware durante las fases de recogida de datos, procesamiento, difusión y almacenamiento. El responsable-depositario puede ser, por ejemplo, un especialista en informática del equipo de gestión, un documentalista, un secretario. Es el depositario de una parte del patrimonio del organismo y estará, por lo tanto, obligado a garantizar la aplicación de la ley en cuanto a la protección jurídica del software que le ha sido confiado (copias ilegales).
ORG-11: Gestión de las relaciones con terceros que trabajan en el SSI en el marco de la SSI	La PSSI debe formalizar los tipos de relaciones, las instrucciones, e identificar a las personas de contacto útiles en terceros organismos que desempeñan algún papel (o son susceptibles de desempañar un papel) dentro del seguimiento y mantenimiento de la SSI. Entre estos organismos, pueden estar: - En la categoría de las autoridades y asociados: o los organismos con los que hay que comunicarse en caso de detección de un delito informático dentro del SI; o los organismos de vigilancia y alerta; o los organismos de auditoría. - En la categoría de los prestadores: o los prestadores de servicios de telecomunicación; o los prestadores que trabajan en el organismo;

o los prestadores subcontratados y/o que tienen a su cargo una parte de la gestión del SI;

o los prestadores expertos en el área de seguridad;

o los organismos de auditorías externas.

Es fundamental controlar los accesos, tanto al sistema de información como a la información delicada referida al SI y a su seguridad. Puesto que terceras personas tienen, por la naturaleza del servicio que prestan al organismo, necesidad de contar con ese tipo de accesos, es conveniente garantizar que las mismas normas impuestas al personal interno (documentación y aspectos contractuales) sean aplicables y aplicadas por los actores involucrados.

ORG-12: Marco contractual para los intercambios de datos seguros

Las propuestas de acceso a servicios o aplicaciones telemáticas internos o externos al organismo plantean el problema de la cooperación entre los diferentes sistemas de información. Esta norma apunta a prevenir la pérdida, la alteración y el uso incorrecto de los datos.

Es importante, en consecuencia, prever las responsabilidades y obligaciones contractuales de los diversos participantes, tanto a nivel de las transmisiones como de las aplicaciones que los integran.

El intercambio seguro de datos se sitúa dentro de las transmisiones tal como se las define más arriba. El marco contractual definirá los acuerdos estipulados entre varias partes para los intercambios de datos que recurren o no a tecnologías de la información. Esta norma abarca el caso de los intercambios de datos informatizados (EDI).

Los convenios o contratos firmados por el organismo con todos los usuarios del sistema de información incluyen cláusulas de control que especifican, por ejemplo:

- la responsabilidad en cuanto a la gestión de los flujos de intercambios;

- los procedimientos de seguridad utilizados para los intercambios;

- los estándares de estructuración de los datos;

- las responsabilidades en caso de pérdida de datos;

- las medidas específicas para la protección de las claves de cifrado.

ORG-13: Modalidades de uso de las redes de telecomunicación externas al organismo

El uso de redes de telecomunicación externas al organismo establece canales de comunicación con usuarios que no tienen, a priori, los mismos requerimientos de seguridad y que, por otra parte, no son controlables.

Las modalidades de uso seguro de redes de telecomunicación externas al organismo se centran especialmente en el control de los medios que pueden escapar a la gestión centralizada del sistema de información como, por ejemplo, la instalación de módems o de terminales Minitel. El caso particular del correo electrónico debería llevar a adoptar medidas tendientes a controlar el envío de mensajes considerados como vulnerables a intercepciones y modificaciones no autorizadas y a las consideraciones legales vinculadas con el no repudio del mensaje emitido o recibido.

El personal del organismo que trabaja desde su domicilio (teletrabajo) se encuentra en un entorno privado sobre el cual el organismo no tiene ningún

	control. Por este motivo, deben implementarse normas técnicas especiales referidas a los derechos de acceso y también se deben concienciar especialmente al usuario informándole sobre sus responsabilidades respecto de los datos que la empresa le confía. Las categorías extraídas del diseño OSI se aplican a las redes externas al organismo.
ORG-14: Cláusulas específicas de protección de los datos	Cuando se prevén intercambios con terceros, pueden incluirse en los contratos cláusulas específicas destinadas a regular dichos intercambios. Estas cláusulas se centrarán en los medios por implementar, como, por ejemplo: - el control de ausencia de códigos maliciosos; - las normas de protección aplicadas internamente (definición de un cuadro de clasificación cruzada); - el soporte de intercambio y los medios de protección contra la divulgación, la integridad, el no repudio... Si el organismo se ha comprometido a respetar cláusulas de este tipo enunciadas por un tercero, deberá informar de ello al personal involucrado, o incluso incorporarlas a su PSSI.
ORG-15: Selección, coordinación y uso de medios criptográficos	Debido a los objetivos que están en juego, la elección de los medios (por ejemplo, software o hardware criptográfico utilizable) y, con mayor razón, de los servicios externos (por ejemplo: autoridad de certificación, prestador de servicio de confianza) deberá ser validada y aprobada por la estructura de seguridad del organismo cuando esta elección no la realice directamente dicha estructura. Uno de los elementos esenciales que deben tenerse en cuenta en lo que se refiere a la confidencialidad es el tratamiento de la necesidad (o no) de que el organismo cubra documentos cifrados por miembros de su personal. Las soluciones pueden implementarse a nivel de la gestión de las claves (por ejemplo, implementación de un depositario) o de las funciones y utilitarios (creación sistemática de campos de cobertura). Es conveniente que se elaboren normas que indiquen los requerimientos mínimos (tanto teóricos como operativos) para cada una de las funciones básicas (confidencialidad, autenticación, no repudio) que deben respetarse. La elección de los prestadores externos (autoridad de certificación o prestador de servicios de certificación, por ejemplo) es una decisión estructurante que requiere la aprobación de la estructura de seguridad y la validación por parte de la dirección general. Es conveniente procurar que se incluyan explícitamente las cláusulas de protección, seguridad y garantía adecuadas en cada uno de los contratos con estos prestadores.
ORG-16: Implementación de una organización de vigilancia y prevención	Es indispensable definir una organización que controle y mantenga actualizada la lista de riesgos mayores que pesan sobre el sistema de información (nuevas amenazas, nuevas necesidades de seguridad, evolución importante del sistema de información ...). Esta organización debe disponer de la capacidad profesional de expertos internos o externos y de suficientes medios para recopilar y calificar la información (contactos, suscripciones a organismos especializados, ver ORG-12, Gestión de las relaciones con terceros que trabajan en el sistema en el

	marco de la SSI). También debe disponer de medios controlados para la difusión de la información de seguridad pertinente, con fines preventivos. Esta vigilancia puede externalizarse o llevarse a cabo en forma coordinada con organismos como el CERTA, que publica regularmente avisos, alertas o recomendaciones para las instituciones estatales francesas. Sin embargo, la implementación de un sistema de vigilancia debe ir acompañada de un seguimiento de las recomendaciones: la vigilancia no es un fin en sí misma, es menester controlar la implementación de las recomendaciones derivadas de la vigilancia.
ORG-17: Organización de células de crisis	El principio consiste en definir previamente una organización (responsabilidades, funcionamiento y medios) capaz de dar respuesta a incidentes importantes que ocurran en el sistema de información. Para ello es conveniente prever procedimientos de escalamiento, probarlos y formar al personal en su ejecución. El punto principal consiste en identificar a los actores del nivel jerárquico adecuado para que sean capaces de tomar decisiones tan rápidamente como lo requiera la situación. Es conveniente definir también los medios y procedimientos necesarios para: - difundir la alerta; - recoger la información; - constituir una célula de crisis; - definir medidas preventivas; - elaborar un plan de acción que agrupe las medidas correctoras.

3.3.3 GER : Gestión de los riesgos SSI

GER-01: Definición del marco de gestión de los riesgos SSI	La gestión de los riesgos SSI constituye un proceso continuo. Es conveniente definir con precisión el marco de dicho proceso (recursos, medios, responsabilidades...) para cada uno de sus aspectos: - Apreciación del riesgo: Esta tarea consiste en analizar y evaluar el riesgo SSI comparando el nivel de riesgo con criterios de riesgos previamente definidos. - Tratamiento del riesgo: Esta tarea consiste en reducir, transferir o asumir el riesgo apreciado durante la tarea anterior. - Aceptación del riesgo: Esta tarea consiste en aceptar el riesgo tratado y, llegado el caso, en asumir el riesgo residual. - Comunicación referida al riesgo: Esta tarea consiste en intercambiar o compartir información referida al riesgo.
GER-02: Identificación de los objetivos de seguridad	La identificación de los objetivos de seguridad permite definir las necesidades reales del organismo en materia de SSI. Este pliego de condiciones de SSI puede formalizarse respetando las etapas descritas a continuación, que tienen en cuenta la misión o el oficio del organismo: - recopilación de los elementos estratégicos (restricciones, objetivos,

orientaciones estratégicas, referencial...),

- expresión de las necesidades de seguridad de los elementos esenciales (datos y funciones) en términos de disponibilidad, integridad, confidencialidad... y según una escala de necesidades objetiva,

- estudio de las amenazas que pesan sobre el organismo (caracterización de los elementos peligrosos, estudio de las vulnerabilidades...).

- identificación de los riesgos reales para el organismo.

Los objetivos de seguridad deben cubrir todos los riesgos identificados.

La definición de las necesidades de seguridad permite describir de manera no ambigua los niveles de sensibilidad (en términos de confidencialidad, integridad, disponibilidad...) que será conveniente garantizar para los componentes de un sistema de información.En las especificaciones debe precisarse qué seguridad se espera del sistema de información, porque ésta es una dimensión esencial de este sistema, al igual que su rendimiento o los servicios que debe prestar. Esta expresión de las necesidades de seguridad debería analizarse en profundidad, mediante un estudio que utilice un procedimiento metodológico y tenga un enfoque global. Abordar este análisis de manera metodológica permitirá conservar una visión de conjunto homogénea sobre la problemática de SSI, conformar un referencial de seguridad completo y tomar conciencia de la mayor parte de los riesgos a los que debe hacer frente el sistema.

Una apreciación de los riesgos debe permitir también, en esta fase, identificar las vulnerabilidades del sistema y las consecuencias de eventuales atentados contra su seguridad, de tal modo que permita justificar la implementación de ciertas respuestas de seguridad de las cuales se habrá evaluado la relación costo/eficacia. De este modo, por ejemplo, los resultados de una apreciación de los riesgos pueden llevar a recurrir a seguros para paliar una falta de capacidad profesional o de recursos presupuestarios.

Sólo sobre la base de estos análisis podrá tomarse la decisión de tener en cuenta o no determinados riesgos.

GER-03: Circunstancias que justifican una reevaluación de la seguridad del SI

El principio de reevaluación de las directrices de la OCDE que regulan la seguridad de los sistemas y redes de información estipula:

"Las partes involucradas deben examinar y reevaluar la seguridad de los sistemas y redes de información e introducir las modificaciones adecuadas en sus políticas, prácticas, medidas y procedimientos de seguridad. Constantemente se descubren vulnerabilidades y amenazas nuevas o en evolución. Para hacer frente a estos riesgos en constante evolución, todas las partes involucradas deben continuamente revisar, reevaluar y modificar todos los aspectos de la seguridad".

Es irrealista pensar que, una vez que se ha sometido un sistema a una evaluación, éste se encuentra protegido de errores o es imposible de modificar: ciertamente, el sistema deberá responder a nuevos requerimientos que se

traducirán en modificaciones del hardware, del software y de la documentación. Además, pueden aparecer nuevas necesidades de seguridad y generar nuevos riesgos que será conveniente evaluar y tratar.

Desde esta perspectiva, es evidente que ciertas modificaciones requieren una reevaluación. Es el caso, por ejemplo, de la reestructuración del núcleo de un sistema operativo, que puede basarse, en parte en los resultados de una evaluación anterior. Otras modificaciones, por el contrario, pueden no implicar ninguna nueva evaluación, si afectan a partes del sistema de información separadas de los componentes de seguridad y no influyen en estos últimos. Por lo general, toda evolución del sistema de información (evoluciones de los aspectos humanos, organizacionales, financieros, geográficos...) debe conducirnos a replantear la cuestión de la seguridad. Este replanteo puede llevar a una reevaluación del sistema o sólo a una modificación de ciertas normas.

GER-04: Estudio prospectivo sobre la evolución de la SSI

Un estudio prospectivo sobre la evolución de la SSI permite prever las necesidades del organismo a mediano plazo e integrar lo antes posible los nuevos objetivos, software, hardware o mecanismos necesarios para la seguridad. Este estudio prospectivo no puede desvincularse de las orientaciones estratégicas (o de un esquema director de los sistemas de información) en cuanto a las nuevas tecnologías de la información que el organismo podría adoptar.

Por otra parte, esta norma apunta a verificar que cualquier evolución del sistema de información sigue siendo conforme a los principios de seguridad vigentes en el organismo. Si no fuera así, el estudio prospectivo permitirá medir su impacto en la seguridad y proponer las adecuaciones de orden técnico u organizacional que pueden implicar una modificación de los principios y normas de la PSSI del organismo.

GER-05: Regulación y control de ciertos flujos específicos

Cuando las comunicaciones permiten intercambios entre el interior y el exterior del SI del organismo, así como internamente en el mismo SI, o incluso para comunicaciones entre perímetros aislados, podría resultar necesario implementar normas y medios de control específicos para esos flujos. Resultará oportuno llevar acabo un análisis de los riesgos siguiendo una metodología, porque esto permitirá identificar claramente todos los flujos intercambiados por el SI así como las amenazas que pesan sobre este último.

Será éste el caso, por ejemplo, de las comunicaciones con el exterior del organismo mediante el uso del correo electrónico, reguladas por normas y dispositivos que permitan su implementación, en cuanto al tamaño de los mensajes enviados o recibidos, el tipo de ficheros adjuntos (aceptación o no de contenidos activos), el control antivirus y el control destinado a evitar la introducción de códigos maliciosos. Estas diversas medidas deberán ser coherentes con la guía de seguridad y de buen uso de los recursos informáticos que deberá haber firmado todo usuario, ya que, más allá de su información, entran en juego aspectos reglamentarios (deber de información del personal, respeto de la vida privada).

Otro ejemplo es el del flujo saliente HTTP (consulta de servidores web externos desde puestos del SI) mediante diversos dispositivos, como podría ser, por ejemplo, la implementación de un proxy de salida, de una autenticación de salida, la conservación de las trazas de las conexiones...

No se trataría aquí de identificar todos los casos posibles, ni tampoco de brindar

	para cada uno de ellos las normas y medios adecuados, la norma que debemos respetar es que cada uno de estos flujos debe ser identificado y analizado desde el punto de vista de la seguridad y podrá/deberá dar lugar a la implementación de soluciones específicas para garantizar su seguridad.
GER-06: Identificación de los servicios y medios que justifican el uso de la criptografía	Teniendo en cuenta lo que esto implica tanto desde el punto de vista técnico como desde el punto de vista legal, es importante identificar las aplicaciones y servicios que requieren del uso de medios criptográficos. También deben identificarse las soluciones criptográficas para cada aplicación o servicio. La elección de las mismas se realizará en función del tipo de datos procesados y del marco reglamentario. Por ejemplo, para un SI que maneja datos clasificados, el empleo de medios criptográficos aprobados es obligatorio. Aquí también la apreciación de los riesgos proporciona información sobre las restricciones reglamentarias pertinentes y sobre las necesidades de los usuarios

3.3.4 CDV : Seguridad y ciclo de vida

CDV-01: Integración de la SSI en los proyectos	La PSSI debe prever una organización que garantice que se tengan en cuenta los aspectos de seguridad durante todo el ciclo de vida de los proyectos (estudio de oportunidad, estudio de factibilidad, diseño general, diseño detallado... supresión). Esta organización, aunque autónoma en cuanto a los proyectos, debe actuar en estrecha relación con los responsables de la conducción y coordinación de la SSI global del organismo. El organismo debe, en particular, identificar las áreas y proyectos en los cuales deben intervenir expertos reconocidos.
CDV-02: Condiciones para la puesta en servicio de cualquier nuevo componente del SI	Esta norma apunta a reducir los riesgos inherentes a la falta de compatibilidad con los otros componentes del entorno en el plano de la seguridad o a la falta de adaptación de las instrucciones técnicas y humanas vigentes que originar errores de uso. Un nuevo componente del sistema de información (software o hardware), aun cuando sea considerado eficaz y conforme a las especificaciones de fabricación, debe ser sometido a pruebas de integración en su nuevo entorno. Las condiciones recomendadas por esta norma pueden prever, por ejemplo, una instalación completa del componente para la identificación de las modificaciones técnicas y de procedimiento que deben efectuarse, así como la posibilidad, en caso de falla, de restablecer el estado anterior del entorno técnico.
CDV-03: Control del software antes de su puesta en servicio	Los controles del software y de los ficheros de datos antes de su puesta en servicio apuntan principalmente a combatir la amenaza de infección con virus u otros códigos maliciosos y el riesgo de no conformidad del software. Los virus u otros códigos maliciosos plantean un problema cada vez más grave para la seguridad de los sistemas de información. Su existencia afecta a todos los organismos e instituciones, cualquiera sea su nivel de vulnerabilidad: Los organismos más abiertos al público son los más expuestos a los piratas informáticos cuyas motivaciones son, muy frecuentemente, la proeza técnica y el impacto mediático. El riesgo de no conformidad del software afecta a los organismos delicados que, en el marco del recurso a prestadores de servicios para el desarrollo de software, deben verificar la exactitud y la conformidad de la programación del

código, a fin de verificar que el programa sólo hace aquello para lo cual fue diseñado y que no existen puntos de acceso ocultos que permitan posteriormente una modificación ilícita de estas funcionalidades.

Pueden tomarse algunas precauciones para prevenir y detectar la introducción de programas maliciosos (virus, gusanos, troyanos, bombas lógicas...). Todos los soportes informáticos provenientes del exterior del organismo y, especialmente, aquellos cuyo origen es incierto, deben someterse a un control. La implementación de hardware dedicado a una detección sistemática constituye una respuesta a esta amenaza.

CDV-04: Circunstancias elegidas para la implementación de los controles de seguridad

El responsable de la seguridad controla la coherencia y validez de los programas instalados en los equipos de su organismo respecto de las principales orientaciones de seguridad y las orientaciones estratégicas del organismo.

Por otra parte, el equipo de seguridad implementa controles, en el marco de las investigaciones realizadas a petición del responsable de la seguridad. Estos controles pueden caracterizarse por su alcance y amplitud:

- su alcance se refiere a la definición del nivel de detalle (es el componente vertical);

- su amplitud se refiere a los diversos elementos considerados en el control (es el componente horizontal).

Es esencial, para el clima de confianza del personal y el buen desarrollo de la misión del organismo, adecuar los controles de seguridad en función de circunstancias claramente definidas por el nivel de toma de decisiones. Fuera de un contexto judicial o de medidas disciplinarias, estos controles deberían ir acompañados de una acción informativa y de preparación del personal.

CDV-05: Modalidades de los controles de seguridad por parte del nivel de conducción

Para apreciar el nivel de seguridad del sistema de información, es necesario realizar una reevaluación periódica de las vulnerabilidades de las entidades (hardware, software, redes, locales, organizaciones, personal) en lo que se refiere a los elementos peligrosos (accidentales o deliberados, y naturales, humanos o del entorno) y sus métodos de ataque.

Las autoridades calificadas, asistidas por el equipo de seguridad del organismo, fijan las modalidades técnicas, los métodos y las herramientas necesarias para la seguridad, controlando su buen uso y eficacia en función de los criterios enunciados por el nivel de toma de decisiones.

Estos controles se integran dentro de las inspecciones y auditorías de seguridad planificadas, abarcando las diferentes entidades de la seguridad de los sistemas de información (hardware, software, redes, locales, organizaciones, personal).

Es necesario que el nivel de conducción realice una planificación de los controles que supongan recurrir a personal operativo y utilizar algunos recursos técnicos, para que dichos controles no se transformen en un obstáculo para el buen desempeño de la misión del organismo.

CDV-06: Continuidad del control de seguridad para el nivel operativo

Los agentes de seguridad realizan los controles que se les imparten mediante la aplicación de umbrales de tolerancia fijados por la autoridad calificada. El nivel de conducción podría modificar dichos umbrales de tolerancia si se observaran repetidas diferencias, vinculadas, por ejemplo, con las restricciones operativas, o si se produjera un cambio de estado del sistema de información.

Sus acciones de control están estrechamente vinculadas con la ejecución de las tareas operativas y afectan a ([IGI 900], artículo 20, [REC 901], artículo 19):

- la protección de las personas, incluyendo, por ejemplo, la actualización continua de la lista del personal empleado en forma permanente y, llegado el caso, del personal afectado al procesamiento de datos;

- la protección de los datos, que abarca, por ejemplo, el control de la destrucción de los datos clasificados que deben eliminarse del sistema;

- la protección de los sistemas y redes, que implica, por ejemplo, el control de la distribución a los usuarios de los elementos de autenticación para las aplicaciones clasificadas.

Estos controles son complementarios de aquellos confiados a los ingenieros que gestionan los registros de auditorías.

CDV-07: Control permanente en de los medios de protección

El control de la integridad y de la disponibilidad de los medios de protección es un aspecto fundamental de la seguridad. Esta norma afecta a los dispositivos de seguridad en los cuales se confía para garantizar la protección de los datos procesados: se trata de equipos, mecanismos (hardware y software) y de la documentación asociada a los mismos, denominados en el artículo 10 de la [IGI 900] como "Artículos controlados de seguridad de los sistemas de información" (ACSSI), o mencionados en el artículo 9 de la [REC 901].

Resguardar esta confianza justifica un control de la integridad y disponibilidad de estos medios que tienen un ciclo de vida: son diseñados, fabricados, utilizados, reparados y luego reformados o destruidos. Su integridad y disponibilidad, condiciones fundamentales para lograr una seguridad eficaz, se garantizan mediante la implementación de medidas de gestión específicas, entre las cuales se cuenta un programa de mantenimiento lo más proactivo posible.

CDV-08: Aplicación de control de código y de procedimiento de instalación

Pueden llevarse a cabo procedimientos de control de los desarrollos para combatir la introducción de funciones maliciosas (por ejemplo: control mutuo de códigos, sellado de código bajo la responsabilidad del desarrollador, control por muestreo...).

Todo desarrollo o modificación de código debe dar lugar, antes de su puesta en servicio, a la ejecución de procedimientos de instalaciones unitarias, de integración y de calificación.

Por lo tanto, deberá prestarse especial atención al control de los valores y a los límites.

CDV-09: Otros tipos de controles necesarios

Algunos ejemplos de los controles que deben implementarse:

- control de la aplicación en los proyectos de las normas enunciadas en la PSSI;

- control de la cobertura de la PSSI respecto de la evolución de los desafíos del SI;

- control de la correcta aplicación de las normas de gestión de los accesos y permisos;

- control del cumplimiento de las normas de seguridad por parte de terceros (externalización de servicios, gestión informática externalizada);

	- control de la base de incidentes y de la exhaustividad de los procesos;- control del cumplimiento de las normas de acceso físico; - control del análisis regular de las trazas de actividades, especialmente de aquellas cuentas que disponen de privilegios extendidos sobre el sistema o que tienen acceso a información o funciones delicadas/vitales; - control de la presencia de cláusulas contractuales de seguridad en todos los contratos de proveedores; - control de la eficacia de las medidas de protección de la red pública; - control de la aplicación de los procedimientos de instalación antes de la puesta en servicio de un nuevo sistema de información o de una modificación importante; - control del cumplimiento de las leyes, reglamentos y de los diferentes códigos profesionales; -...
CDV-10: Los procesos de control no deben perturbar el funcionamiento de los SI	Los procedimientos de control deben estar claramente definidos. Los accesos y privilegios necesarios para las pruebas y controles del sistema de información deben limitarse en el tiempo y en cuanto a su alcance. Debe prestarse especial atención a verificar que la ejecución de estos procedimientos no tenga un impacto significativo en el funcionamiento del sistema de información.
CDV-11: Realización de auditorías de seguridad	La eficacia de cualquier medio de seguridad sólo puede mantenerse en el tiempo si se la verifica regularmente utilizando elementos tangibles. Personal calificado y autorizado debe realizar auditorías de seguridad del sistema de información, siguiendo procedimientos que es conveniente definir y procedimientos precisos y validados que permitan garantizar la correcta aplicación de los procedimientos de seguridad, del funcionamiento operativo de estos procedimientos, de la coherencia de estos procedimientos, de los medios implementados y de la consideración efectiva por parte de estos medios de todos los procesos evaluados, incluidas las evoluciones. Los resultados de estas auditorías se comunican a la entidad contratante y a las personas que precisan conocerlos. La identificación de incidentes o fallos de seguridad del sistema de información debe, necesariamente, informarse al RSSI. Las auditorías externas de seguridad del sistema de información deben ser previamente autorizadas por el RSSI. Este tipo de auditoría debe realizarse en un marco estricto, en el cual las responsabilidades de cada uno de los actores estén claramente definidas (profundidad de la investigación, difusión de los resultados). Complementariamente a estas auditorías, pueden realizarse pruebas de intrusión. Estas pruebas deben definirse y encuadrarse (elección de un prestador, compromiso de confidencialidad, procedimientos de respaldo y plan de restablecimiento de servicio...).

3.3.5 ACR : Aseguramiento y certificación

ACR-01:	Estos requerimientos deben definirse claramente y se refieren principalmente a:

Requerimientos mínimos para las aplicaciones utilizadas en el SI

- La protección de los datos de configuración o parámetros, que se olvidan muy a menudo, aunque representan uno de los medios más fáciles y, a menudo, uno los más susceptibles de piratería de una aplicación.

- La validación y el eventual filtrado de los datos de entrada antes de su procesamiento: esta validación debe preverse y aplicarse sistemáticamente, afecta principalmente a los "datos ingresados" por los usuarios (riesgos de error o tentativa delictiva) y a los datos provenientes del exterior del organismo.

- La validación de los datos de salida: es la contrapartida del punto anterior y se refiere a:

- la protección de las entradas del procesamiento dentro de una cadena de aplicaciones,

- y/o la fiabilidad de los resultados al final de la cadena.

- Los riesgos de modificación o corrupción de los datos por parte de la misma aplicación: estos problemas provienen, la mayoría de las veces, de errores de diseño y, muchas más veces aun, de errores de implementación (bugs) que podrían ser aprovechados por usuarios mal intencionados.

- La presencia y pertinencia de los mecanismos de autocontrol presentes dentro de la misma aplicación y de su capacidad para generar informes de alerta en caso de comportamientos anormales o, simplemente, imprevistos.

- La presencia y pertinencia de mecanismos de rastreo (trazas) y de registro disponibles y configurables según las necesidades.

ACR-02: Elaboración de un objeto de seguridad

El objeto de seguridad constituye la especificación del sistema en materia de seguridad. Es una etapa muy importante que establece, al mismo tiempo, el objetivo que se pretende alcanzar y los medios para lograrlo.

En primer lugar, la reflexión profunda que ha permitido el estudio de las necesidades de seguridad y el análisis de riesgos debe permitir establecer aquello que se decide finalmente proteger, especificando por qué, de quién y de qué. La síntesis de esta reflexión conforma los objetivos de seguridad del sistema. Dichos objetivos se definen claramente desde la fase de especificación, para que sea posible alcanzarlos y para que pueda apreciarse si la seguridad del sistema es capaz de cumplirlos.

De estos objetivos de seguridad se derivan las medidas, técnicas o no técnicas, que deben implementarse.

Las medidas no técnicas son los procedimientos y normas de implementación, gestión y organización, los permisos otorgados a las personas, las medidas que contribuyen a proteger el entorno del sistema y todas las disposiciones de carácter reglamentario.Las medidas técnicas son las funciones de seguridad que hay que prever en el diseño del sistema de tal modo que puedan alcanzarse los objetivos. Estas funciones se concretan gracias a mecanismos de seguridad integrados al sistema.

Objetivos y funciones constituyen lo esencial del objeto de seguridad. Éste representa el fundamento de la seguridad en el diseño del sistema de información.

Sin embargo, para que uno pueda estar seguro de que se han alcanzado los objetivos, es necesario, por una parte, que estas funciones y mecanismos

	existan y, por otra parte, que uno pueda tenerles suficiente confianza.
ACR-03: Cumplimiento de los requerimientos de seguridad antes de la puesta en servicio	La verificación del cumplimiento de los requerimientos debe ser: - por una parte, implementada durante la elección (software comprado) o la especificación (software desarrollado) a fin de que las características intrínsecas del software sean suficientes para permitir una implementación aceptable desde el punto de vista de la seguridad; - por otra parte, efectuada como condición previa de la fase operativa, a fin de que se garantice el nivel de seguridad en las condiciones de uso efectivas (entorno, configuración...).
ACR-04: Verificación periódica del cumplimiento de los requerimientos de seguridad en las aplicaciones	Para evitar una deriva en el tiempo, es importante implementar procedimientos que lleven a un control periódico regular del cumplimiento de los requerimientos de seguridad sobre las características y el funcionamiento de las aplicaciones. Parte de este control puede realizarse internamente.
ACR-05: Evaluación del nivel de confianza atribuido al SI: evaluación y certificación	El diseño del sistema está guiado por un procedimiento coherente que conduce al logro de los objetivos de seguridad. Se eligen la funciones de seguridad necesarias para alcanzar dichos objetivos. Una vez que el sistema ha sido desarrollado y puesto en servicio, es importante saber qué nivel de confianza continua podemos tener en que el objeto de seguridad ha sido efectivamente alcanzado. Esta confianza dependerá, por una parte, de la elección de las funciones, de su eficacia y de la calidad de su desarrollo y, por otra parte, de la manera en que se ha instalado, puesto en servicio y utilizado el sistema. El estudio de cada uno de estos aspectos permitirá tener una confianza justificada en la realización del objeto de seguridad. Es el objeto de la evaluación. Un sistema desarrollado según los principios arriba expuestos podrá ser evaluado y tendremos, entonces, la confirmación de que podemos confiar en él en lo que respecta a la seguridad que dicho sistema garantiza para los datos que le son confiados y para los procesos que utilizan dichos datos. La evaluación contribuye de manera significativa a reducir los riesgos de un comportamiento no deseado de una aplicación. Esto consiste en evaluar las propiedades de un sistema o de un producto respecto de criterios de seguridad normalizados como, por ejemplo, los Criterios Comunes. Esta devaluación debe llevarse a cabo según un método aprobado que obedezca a normas definidas. Los resultados de la evaluación y el hecho de que los criterios de evaluación utilizados hayan sido correctamente aplicados se confirmarán mediante una declaración formal denominada certificado. Sin embargo, la certificación no tiene carácter obligatorio: es responsabilidad de la entidad contratante de la evaluación decidir si es necesaria la certificación.
ACR-06: Criterios de adquisición y condiciones de	Si bien los criterios de compra de paquetes de programas son esencialmente económicos y operativos (disponibilidad inmediata del producto, costo accesible, mantenimiento y asistencia técnica), no por ello dejan de ser un problema de

uso de paquetes de programas	seguridad en lo que respecta a la integridad del software entregado y de su uso dentro del organismo. Resulta, por lo tanto, fundamental contar con una norma que prevea criterios que permitan justificar la adquisición de paquetes y sus condiciones de uso, basándose, por ejemplo, en los siguientes aspectos: - la verificación del cumplimiento de los principios de seguridad vigentes en el organismo antes de decidir su adquisición; - las pruebas de conformidad e integridad antes de la puesta en servicio de los paquetes; - las restricciones de uso de dichos paquetes en función de la sensibilidad de los puestos de trabajo.
ACR-07: Adopción de métodos y herramientas de desarrollo	La adopción, desde el momento del diseño del sistema de información, de métodos y herramientas de desarrollo muestra la voluntad del organismo de controlar la seguridad. La aplicación de esta norma permite adquirir una confianza justificada en el diseño y realización del objeto de seguridad. Contribuye además a la implementación de protecciones homogéneas y coherentes que constituyen así una garantía de éxito para una eventual evaluación del sistema de información. Sin embargo, esta norma no supone el uso de un método único para el desarrollo del sistema de información, sino que induce a procurar la necesaria coherencia que debe existir entre los diferentes métodos utilizados por el organismo.
ACR-08: Adopción de un estándar de programación y codificación de los datos	La adopción de un estándar de programación debe aplicarse a todos los desarrollos de aplicaciones informáticas, incluso a las partes lógicas que puede contener el hardware o diversos dispositivos del sistema de información. La primera recomendación vinculada con la adopción de un estándar de programación es la de especificar las configuraciones de hardware y software utilizadas para el desarrollo. La segunda recomendación se refiere a la elección de una representación y una estructuración de los programas que permite contar con referencias uniformes y reconocidas por todos, facilitando así las operaciones de mantenimiento del software y el seguimiento de la documentación técnica. La codificación de los datos se refiere al formateado y representación de los campos de datos que, por razones similares a la estructuración de los programas, requieren la adopción de un estándar. Los diversos estados de salida de los datos obedecen también a estándares de presentación que contemplan las particularidades funcionales de los usuarios del organismo. El administrador de la base de datos es responsable por la correcta definición de los datos y la estructura de los ficheros y bases de datos.
ACR-09: Homologación del sistema de información	La homologación de seguridad es la declaración que realiza la autoridad de homologación (gubernamental o específica del organismo, según corresponda), tras evaluar la documentación de homologación, afirmando que el SI se considera apto para procesar datos de determinado nivel de sensibilidad y de clasificación conforme a los objetivos de seguridad establecidos, y que se han asumido y se encuentran bajo control los riesgos de seguridad residuales

	generados. Generalmente un comité coordinador se encarga del seguimiento del proyecto destinado a llevar a cabo una homologación. Dicho comité dirigirá la conformación de la documentación de homologación que la autoridad de homologación deberá aprobar. La homologación de seguridad es válida mientras el SI funcione en las condiciones aprobadas por la autoridad de homologación. La homologación muestra la aceptación de un nivel de riesgo residual caracterizado y cuantificado en términos de confidencialidad, integridad, disponibilidad, autenticidad y no repudio.
ACR-10: Aceptación del sistema de información	La evaluación y la certificación que confirma sus resultados permiten garantizar sólo que el objeto de seguridad se ha alcanzado. No es más que uno de los elementos para evaluar si el sistema o el producto instalado en su entorno real presenta efectivamente las medidas de seguridad no técnicas (especialmente, los procedimientos de gestión efectivamente implementados), las protecciones adecuadas para la sensibilidad de los recursos que le han sido confiados y la importancia de las amenazas que debe contrarrestar. Además, resulta conveniente contar con una opinión sobre la pertinencia del objeto de seguridad respecto del entorno real de utilización del sistema: este es el papel que desempeña la aceptación, que constituye el reconocimiento formal de que el producto o sistema evaluado puede proteger los datos hasta un nivel determinado, en condiciones de uso definidas.
ACR-11: Gestión de la documentación de seguridad	La gestión de la documentación de seguridad abarca la contabilidad, la actualización, la reproducción y la destrucción: - La gestión de la documentación de seguridad se sustenta en un contabilidad precisa y eficaz basada en mantener actualizado un registro de inventario. - La actualización periódica de la documentación de seguridad es necesaria debido a la evolución constante del sistema de información. - La reproducción y destrucción de la documentación se realizan por orden del responsable de seguridad, quien verifica que la operación se realice con todos los documentos designados y que no afecte a otros documentos.
ACR-12: Adopción de un estándar de elaboración de la documentación de seguridad	La diversidad de equipos, software y procedimientos supone la definición de un estándar para la elaboración de la documentación de seguridad. Este estándar se refiere, en primer lugar, al modelo de presentación y al contenido de la documentación: Todos los componentes de seguridad se describen usando las mismas nomenclaturas, lo que facilita las intervenciones del personal autorizado para su gestión y mantenimiento. En segundo lugar, el estándar se refiere a la manera de producir la documentación, es decir, la redacción, impresión y clasificación de los documentos. Además, todos los elementos que hayan sido utilizados para la elaboración de la documentación serán manipulados y protegidos del mismo modo y en las mismas condiciones que los documentos de seguridad que de ellos resultan.
ACR-13:	Toda documentación producida por el organismo debe elaborarse conforme al

Producción de documentos por parte del organismo

manual de identidad corporativa y a su política de aseguramiento de la calidad. Dichos documentos deben incluir, en particular, una referencia única, que permita identificar claramente a su autor, la fecha de creación, los elementos de gestión de la versión, así como una indicación de la clasificación del documento, que figure claramente en el mismo.

La seguridad de una información se asignará desde el mismo momento de la publicación de un documento. El creador del documento es, por defecto, su propietario. Él es también, por lo tanto, responsable de su clasificación. En función de la clasificación de los datos involucrados, deberán aplicarse las normas de protección adecuadas al soporte de información correspondiente.

Se aplicarán normas de seguridad específicas en función de la clasificación.

ACR-14: Mantenimiento de la documentación de seguridad

Deben definirse un procedimiento y normas destinadas a establecer que toda la documentación de seguridad sea actualizada cuando se concluya cualquier modificación (cf. gestión de la documentación) y que la antigua documentación sea archivada o eliminada.

3.3.6 ASH : Aspectos humanos

ASH-01: Noción de reconocimiento de responsabilidad

Para los puestos de trabajo donde se maneja información protegida por el secreto de defensa, la declaración de reconocimiento de responsabilidad es el compromiso que asume una persona de respetar las leyes, reglamentos y normas de seguridad del sistema de información.

Esto dará lugar a una declaración escrita y firmada conforme a la IGI 1300. En particular, el artículo 16 estipula lo siguiente: "...esta declaración significa que el titular de la declaración reconoce haber tomado conocimiento de las obligaciones particulares y sanciones impuestas por los artículos 70 a 85 y R. 24 del Código Penal para todo depositario o poseedor de datos de interés para la defensa nacional y la seguridad del Estado [...] Corresponde al director del organismo o a la autoridad jerárquica competente llamar la atención del interesado sobre el significado del alcance de esta declaración".

Para los puestos que no entran en esta categoría, pueden insertarse, de ser necesario, en el contrato de trabajo, cláusulas específicas de confidencialidad, de finalización del contrato de trabajo o de no competencia. La [REC 600] trata estas problemáticas para datos que no dependen de la [IGI 1300], especificando, en particular, que: "Todo el personal de cada categoría que deba tener acceso a los recursos informáticos de la empresa debe previamente firmar un documento de compromiso de responsabilidad (cf. sección 1). Este documento puede contener elementos específicos para cada una de las categorías de personal."

Al carácter esencialmente disuasivo de esta medida, puede sumarse la aplicación de sanciones. Las consecuencias en el plano disciplinario del incumplimiento de las normas internas de seguridad deben, en este caso, ser explicadas en cuanto el personal recientemente contratado se hace cargo de sus funciones.

ASH-02: Cláusulas de seguridad en los

Los contratos de trabajo del personal deben:

- incluir cláusulas explícitas de seguridad del sistema de información tales

contratos de trabajo	como: o prohibiciones, o deber de informar cualquier anomalía o falla de seguridad, o deber de reserva, o cláusulas de confidencialidad, o responsabilidad en cuanto al respeto de las normas de protección del patrimonio del organismo; - o bien hacer referencia explícita a los diversos reglamentos aplicables en esta área (cf. capítulo que trata sobre las obligaciones legislativas y normativas), tales como: o la PSSI, o códigos de deontología vinculados con el oficio, o reglamentos del organismo (cartas orgánicas, reglamento interno...). Estos elementos deben establecer las sanciones o medidas aplicables en caso de incumplimiento de dichos compromisos. Este principio debe igualmente extenderse a cualquier convenio de pasantía o contrato de interinidad. El personal que tenga responsabilidades o que tenga a su cargo tareas delicadas (gestión de seguridad, inspección...) debe firmar compromisos especiales vinculados con su futura función. Los diversos compromisos, aun cuando no estén directamente integrados al contrato de trabajo, deben ser revisados y validados por el departamento jurídico del organismo (cf. capítulo anterior sobre las responsabilidades). (cf. Principios de autorización y cf. Obligaciones legales y reglamentarias)
ASH-03: Adopción de criterios de selección del personal que trabaja en los SI delicados	Esta norma involucra a todas las categorías de personal que deben trabajar en sistemas de información delicados. La misma especifica, para los puestos que tienen que ver con el funcionamiento y la gestión del sistema, el modo de selección de personal que debe emplear el organismo y, especialmente, los criterios de seguridad requeridos para cada puesto de trabajo. Por ejemplo, podría contemplarse requerir la presentación de referencias durante los procesos de contratación de personal para puestos delicados. Esta norma supone la posibilidad de verificación de las referencias de trabajo de un candidato a un puesto así como las referencias de las personas afectadas temporalmente a una actividad que requiere el uso del sistema de información.
ASH-04: Principios generales de autorización	El SI solo debe ser accesible, físicamente y lógicamente, para las personas específicamente autorizadas. Por tal motivo, se definirán restricciones de acceso a los sistemas y a los datos en función de su sensibilidad (cf. clasificación) y de la criticidad de las acciones autorizadas para estos datos y recursos.

	Los permisos se asignan a una persona física y no pueden ser cedidos. La asignación de permisos para un sistema o una información debe ser decidida por sus propietarios. La definición de los permisos debe respetar el principio de la necesidad de conocer la información involucrada: todo actor tendrá acceso exclusivamente a los datos que requiere para el cumplimiento de su tarea. Se recomienda que el principio de menor acceso (permiso nulo por defecto) se aplique durante la apertura/implementación de cualquier nuevo sistema.
ASH-05: Categorías de permisos	Las diversas categorías de permisos deben contemplarse durante el proceso de contratación de personal o de selección de proveedores que utilizarán permisos. A los permisos deben corresponder los requerimientos referidos al personal: verificaciones y controles que deben realizarse (identidad, competencia), firma de un acta de compromiso específica...
ASH-06: Normas de asignación y compromiso (responsabilidades)	La asignación de los permisos se determina desde el mismo momento de la contratación del personal. Deben establecerse sus límites en el tiempo y el espacio. La persona a la cual se asigna el permiso debe certificar formalmente que conoce las responsabilidades que acarrea el permiso que se le ha asignado. Cualquier permiso otorgado para un área o proyecto del sistema de información debe ser formalmente autorizado por su propietario (responsable de la protección de los procesos y de los datos procesados por el SI).
ASH-07: Personal polivalente	Pueden tomarse medidas organizacionales para que no haya ningún puesto vital vacante, ni siquiera temporalmente (vacaciones...). El organismo deberá prever suficiente personal polivalente y experimentado para cubrir todos los puestos de trabajo vitales. Toda persona que ocupe un puesto vital debería disponer de un suplente que cuente con competencias equivalentes y con el mismo nivel de conocimiento de la temática vinculada con dicho puesto.
ASH-08: Procedimiento de autorización para los puestos de trabajo delicados	Debe entenderse por sensibilidad de un puesto de trabajo la necesidad de confidencialidad, disponibilidad e integridad asociada a los datos, el software y el hardware que maneja. Dicha sensibilidad se define según los criterios de clasificación (cf. capítulo que trata sobre la seguridad de los datos), pero puede también estar vinculada con: un puesto de responsable de recursos humanos en una región de alto riesgo social puede considerarse un puesto delicado. Para los puestos que implican la manipulación de información protegida por el secreto de defensa, los permisos del personal se definen en el artículo 3 de la [IGI 1300]: "El procedimiento de autorización consiste en verificar que una persona puede, sin riesgo para la defensa nacional, la seguridad del Estado o su propia seguridad, conocer datos clasificados de determinado nivel, dentro del ejercicio de sus misiones. Al concluir el procedimiento de autorización, la autoridad competente decidirá si se admite o no que la persona involucrada tome conocimiento de datos clasificados al nivel requerido". Para los puestos de trabajo delicados donde no se utilice información protegida por el secreto de defensa, puede emplearse un procedimiento de autorización siguiendo el modelo del aplicado en el marco de los contratos de defensa. En este caso, es posible remitirse a la [REC 600].

ASH-09: Aislamiento de los puestos de trabajo

El aislamiento de los puestos de trabajo delicados apunta a combatir la fuga de información que representa un problema serio para los intereses del Estado o del organismo.

Para preservar los intereses del Estado y, especialmente en el marco de la protección del secreto de defensa, las decisiones de permiso o autorización para datos clasificados de determinado nivel, tal como han sido definidas en los artículos 10 a 12 de la [IGI Nº 1300], no autorizan, sin embargo, al beneficiario a acceder a todos los datos que cuentan con ese nivel. La necesidad de conocer dichos datos seguirá dependiendo de la actividad de la persona o de los asuntos particulares que se le confían.

De idéntica manera, para la preservación de los intereses propios de un organismo cuyos datos no están protegidos por el secreto de defensa, el conocimiento de las necesidades de información para el cumplimiento de la misión o del oficio permitirá la implementación de un aislamiento eficaz de los puestos de trabajo.

ASH-10: Delegación

Los propietarios o poseedores de información pueden delegar la implementación de los medios de protección a personal del organismo. Sin embargo, seguirán siendo responsables por su seguridad. Por tal motivo, deben disponer de medios para controlar el cumplimiento de las normas de seguridad.

Los permisos se asignan a una persona física y no pueden ser cedidos.

3.3.7 PSS : Planificación de la continuidad de las actividades

PSS-01: Definición del perímetro de un plan de contingencia

Es conveniente definir con precisión el marco completo del plan de contingencia (recursos, responsabilidades, periodicidad de las pruebas...) para cada uno de los siguientes aspectos:

- las instalaciones, el hardware y las redes informáticas;

- los programas y datos informáticos;

- los usuarios del sistema de información.

Un análisis de los riesgos SSI aportará los elementos que permitirán decidir los planes necesarios para el organismo. Estos planes tiene, ciertamente, un costo importante que es conveniente justificar.

PSS-02: Consideración de los servicios externalizados

Debe profundizarse la gestión de planes de contingencia que impliquen a asociados ajenos al organismo, especialmente durante la elaboración del contrato que los vincula con el organismo. Dicho contrato debe incluir apartados referidos a ejercicios regulares tendientes a verificar el buen funcionamiento de los planes de contingencia.

PSS-03: Elaboración de un plan de recuperación

Es necesario contar con un plan de recuperación informática (o plan de recuperación de actividad) para proteger las tareas operativas críticas del sistema de información de fallos importantes, errores humanos, catástrofes naturales o ataques deliberados. Dicho plan tendrá por objetivo limitar los daños a la seguridad tras un incidente importante y restablecer las condiciones de funcionamiento iniciales del sistema de información.

El plan de recuperación de la actividad implica considerar todos los

requerimientos operativos del sistema de información para garantizar el restablecimiento de un funcionamiento normal. Los procedimientos que derivan de dicho plan proporcionarán una alternativa y medios provisorios de continuidad del servicio, en caso de daño o fallo de un equipo.

Sin embargo, debemos tener en cuanta que es fundamental para el inicio de un plan de recuperación de actividad realizar el estudio de disponibilidad del sistema de información, dado que la importancia de los daños sufridos depende generalmente de la duración de la falta de disponibilidad. Por esta razón, el estudio de la disponibilidad tendrá por objetivo definir franjas temporales en las cuales el perjuicio se considere en determinado nivel, en correspondencia con el nivel de procedimiento de emergencia del plan de recuperación de actividad.

PSS-04: Posicionamiento de las aplicaciones en el plan de contingencia

En función del análisis de riesgos del organismo, cada aplicación puede ser calificada en términos de prioridad de recuperación. Esta calificación corresponde a una medición del impacto que tendría, sobre la actividad del organismo, la falta de disponibilidad de dicha aplicación.

PSS-05: Implementación de los procedimientos de respaldo

Debe implementarse un plan de respaldo que contemple los requerimientos de plazo de reconstrucción de los datos por tipo de actividad y/o proceso. Se diferenciarán las copias de seguridad del sistema, de las aplicaciones y de los datos.

Para lograr un nivel de confianza elevado, el plan de respaldo debe ser regularmente sometido a pruebas. El procedimiento para realizar regularmente copias de seguridad de los datos vitales y del software es una medida fundamental. Por lo general, una cantidad mínima de copias de seguridad de datos se almacenará en un lugar apartado, a distancia suficiente para resistir ante un siniestro en el establecimiento principal. Las protecciones físicas de las copias de seguridad deberán estar al mismo nivel que los estándares aplicados en el establecimiento principal. Deberán implementarse y gestionarse los medios de control necesarios para garantizar la coherencia e integridad de los datos respaldados.

PSS-06: Pruebas regulares de los planes

Para lograr un nivel de confianza elevado, el plan de contingencia y los otros planes asociados deben ser regularmente sometidos a pruebas. Al finalizar cada uno de estos ejercicios, se conformará un grupo de "resultado de la experiencia", que actualizará los planes tras haber analizado los problemas de fallas de funcionamiento y lentitud.

3.3.8 INC : Gestión de los incidentes

INC-01: Definición de las situaciones anormales previsibles

Los tipos de situaciones anormales potenciales abarcan, entre otros:

- los fallos o funcionamientos anormales del hardware;

- los fallos o funcionamientos anormales del software y las aplicaciones;

- los problemas ocasionados por la falta de datos de entrada faltantes o por datos de entrada incompletos o dañados;

- la falta de producción de resultados o la producción de resultados incompletos o dañados;

	-... El análisis de riesgos proporcionará elementos que deberán considerarse para la elección de las alertas que deben informarse. Estas decisiones se vinculan particularmente con los objetivos de seguridad elegidos.
INC-02: Implementación de una red de detección y alerta de incidentes de seguridad	La finalidad de una red de alerta es la de provocar una intervención tan rápidamente como sea posible, en cuanto se detecta un incidente, limitando así las consecuencias de una eventual falta de servicio del sistema de información, o activar la implementación de los procedimientos tras la aparición de un incidente. Todos los usuarios, y especialmente aquellos que se desempeñan en puestos de trabajo delicados, constituyen eslabones de esta red de alerta. Se trata de enseñar a los usuarios a proteger su hardware y a identificar los indicios de manipulaciones fraudulentas o de actividades no habituales. La eficacia de una red de alerta se basa en la estructura de la organización implementada y, especialmente, en los agentes de seguridad. Depende del nivel técnico de los medios de detección y de la movilización de los usuarios del sistema de información: la intervención que se realiza a partir de dicha red es aun más eficaz debido a que implementa los medios adecuados en el momento oportuno. En caso de que se vean comprometidos datos protegidos por el secreto de defensa, el organismo debe buscar la rapidez en la reacción: "Si la seguridad de una información se ha visto comprometida o parece estar comprometida de cualquier modo, la rapidez y la discreción de la intervención son de particular importancia para limitar las consecuencias de esta situación. Un informe infundado y desmentido, luego, por los hechos es siempre preferible a un retraso en la intervención."
INC-03: Control de los incidentes de seguridad	El control de los incidentes de seguridad consiste en asegurarse de la continuidad de la seguridad mientras dure la intervención que se dispone tras una alerta: el recurso a especialistas ajenos a la empresa y la obligación de facilitarles el acceso al establecimiento y al sistema de información no debe dispensar al personal del organismo de aplicar las normas de seguridad. Este control se logra mediante el cumplimiento de los procedimientos preestablecidos. Dos casos de emergencia pueden requerir acciones diferentes: - Las emergencias que se derivan de accidentes físicos que afectan a la infraestructura de una zona delicada o al sistema de información que ésta contiene y que no acarrean acciones hostiles destinadas a recuperar componentes del sistema de información. La acción consiste, entonces, en supervisar el hardware, el software y los documentos durante la intervención como podría ser, por ejemplo, durante el transporte de equipos hacia instalaciones de respaldo o la puesta en modo funcionalidad reducida de mecanismos de seguridad hasta el regreso al normal funcionamiento del sistema de información. - Las emergencias que se derivan de acciones hostiles tendientes a recuperar componentes del sistema de información: la implementación de un plan de destrucción de emergencia simple y práctico puede ser, en ciertos casos, el único medio para evitar que se comprometa seriamente la seguridad del sistema.
INC-04: Control de	La falta de seguimiento de los incidentes de seguridad expone al organismo a

los incidentes de seguridad

desconocer las vulnerabilidades de su sistema de información y lo condena a ser incapaz de reaccionar eficazmente frente a repetidos siniestros del mismo tipo.

Por tal motivo, deben establecerse las responsabilidades en cuanto al seguimiento de los incidentes y de los procedimientos. Los procedimientos deberán abarcar, por lo tanto, todos los tipos de incidentes potenciales, incluidos los fallos del sistema o pérdidas de servicio, los errores que resulten de datos falsos o inadecuados, los fallos de la confidencialidad.

Para ello, el seguimiento de los incidentes se basará en los informes realizados para las intervenciones inmediatas, en los registros de fallas de funcionamiento para las acciones diferidas y, en ambos casos, en el análisis e identificación de las causas del siniestro y de las estadísticas que pueden establecerse sobre su frecuencia de aparición.

La adopción de un estándar de informe y de directivas para su gestión son medidas tendientes a uniformizar e imponer el cumplimiento obligatorio del procedimiento de alerta mencionado.

Los incidentes de cualquier tipo, identificados, por ejemplo, durante la gestión, deberán dar lugar, lo más rápidamente posible, a un informe elevado al responsable de seguridad.

Las fallas de funcionamiento y los puntos débiles del sistema de información deben identificarse y corregirse. Resulta necesario, en particular, analizar las fallas de funcionamiento para garantizar que las medidas correctoras han sido efectivamente implementadas y que corresponden a acciones autorizadas.

El análisis y la identificación de las causas del incidente suponen una planificación de la recopilación de informes de auditoría, de la implementación de medidas de protección y de la comunicación con los usuarios afectados.

INC-05: Medios de detección de intrusión o de uso fraudulento

Se recomienda disponer de diversos dispositivos y/o procedimientos que permitan detectar intentos de intrusión o de uso fraudulento, favoreciendo, de este modo, que se reaccione tomando las medidas necesarias para hacer fracasar dichos intentos.

Será conveniente, por lo tanto, determinar e implementar los medios específicos para cada componente o aplicación delicada del SI; medios que pueden ir desde un mecanismo de supervisión bien configurado hasta herramientas específicas como los sistemas de detección de intrusión.

INC-06: Implementación de un servicio de alerta eficaz

El principio en que se basa este punto consiste en determinar lo más rápidamente posible la aparición de un acontecimiento que constituye (o es susceptible de constituir) los inicios de un ataque o de un incidente importante, o que pueda dar origen a un delito informático.

El servicio de alerta debe organizar el envío de informes y la centralización de las detecciones de incidentes por medio de procesos de información simples (cf. funcionamiento de los roles) y debe concienciar a usuarios y operadores del sistema sobre su deber de informar cualquier tipo de anomalía. Es conveniente prever varios niveles de alerta. Estos diferentes niveles deben poder ser detectados por los usuarios, lo cual supone que cada uno debe conocer en qué nivel se encuentra el SI en determinado momento.

INC-07: Previsión

El principio en que se basa este punto consiste en seleccionar situaciones tipo

de las reacciones reflejas frente a situaciones de emergencia

de siniestro y formalizar las mejores reacciones en términos de medidas preventivas tendientes a limitar, o incluso evitar, la propagación de los impactos del incidente o ataque, en términos de poder de decisión e información interna y externa, llegado el caso. Esto permitirá evitar que los incidentes se transformen en siniestros de consecuencias desagradables o imposibles de sobrellevar para el organismo.

A cada nivel de alerta corresponde un procedimiento claro de las acciones que deben llevarse a cabo. Este tipo de procedimiento se apoya en el principio de defensa en profundidad que permite establecer barreras de protección independientes y en función de la alerta.

3.3.9 FOR : Concienciación y formación

FOR-01: Documentación de las responsabilidades

Es fundamental que todas las responsabilidades del SSI se redacten sin ambigüedad y sean conocidas por las personas están a cargo de las mismas. La descripción de dichas responsabilidades debe incluir sus limitaciones en el espacio y en el tiempo.

Es igualmente indispensable que todos los actores involucrados se comprometan formalmente a informarse de estas responsabilidades y a aceptarlas.

FOR-02: Concienciación general sobre la seguridad

La concienciación busca hacer tomar conciencia a cada usuario de que tiene una gran parte de responsabilidad en la lucha contra el delito informático.

La definición de los objetivos de esta concienciación está estrechamente vinculada con la misión u oficio del organismo, con la sensibilidad del patrimonio de datos y bienes físicos, así como con las amenazas conocidas. Dichos objetivos pueden ser, por ejemplo, la búsqueda de la implicación del personal en la protección del patrimonio del organismo o incluso el establecimiento y la eficacia de una red de alerta que involucre a todos los usuarios del sistema de información.

Una acción de concienciación que no responda a objetivos claramente expresados no aportará más que una ilusión de confianza en la capacidad del personal para reaccionar eficazmente ante un atentado contra el sistema de información.

El RSSI debe prever y conducir un programa de concienciación que implementará con regularidad. Este programa tendrá por objetivo recordar los principales mensajes de la PSSI del organismo y, especialmente, informar a cada persona sobre:

- los objetivos de la seguridad;
- las principales amenazas;
- las leyes, reglamentos, cartas orgánicas;
- la organización de la seguridad;
- los principios y normas de seguridad del organismo;
- las conductas que deben adoptarse;
- las normas específicas (puestos nómades, teleactividades...).

FOR-03: Información sobre la SSI

La información referida a la organización y a los requerimientos generales de la SSI debe ser difundida lo más ampliamente posible dentro del organismo.Por lo tanto, debe definirse un medio de difusión y darlo a conocer a todos; un medio que permitirá encontrar cualquier información vinculada con la SSI dentro del organismo (procedimiento, contacto...). Uno de los medios utilizados puede ser, por ejemplo, la implementación de un área dedicada a la seguridad en la intranet del organismo.

La PSSI global deberá ser conocida por todo el personal del organismo, las PSSI específicas deberán ser dadas a conocer al personal que deba utilizar estos sistemas particulares. La difusión de una parte o de la totalidad de las PSSI a personas ajenas al organismo, que deban trabajar en el sistema de información, deberá depender de su necesidad de conocer dicha información y, en todos los casos, deberá ser validada por la organización a cargo de la SSI (Cf. ORG).

Debe conformarse una documentación "de entrada" que se entregará a toda nueva persona que trabaje en el SI, para garantizar que esté informada sobre la organización, las normas de seguridad y sus deberes. Análogamente, se conformará una documentación "de salida" para informar al personal que se retira del organismo sobre los procedimientos y normas que deben respetarse.

FOR-04: Aplicación para la protección jurídica de la información del organismo

Esta norma busca concienciar al personal sobre el deber jurídico de protección de los datos que utiliza o que le son confiados, a fin de disminuir el riesgo de robo o apropiación por parte de terceros.

Las directivas de aplicación se refieren, en parte, al principio de responsabilidad del personal y, especialmente, a la norma referida a la noción de responsable-poseedor (cf. capítulo responsabilidades ORG).

FOR-05: Adaptación de la concienciación a las diferentes clases de usuarios

En materia de seguridad, los niveles de preocupación difieren considerablemente según se trate del personal de dirección u operativo. La concienciación se adaptará, por lo tanto, a los niveles de responsabilidad y a la especificidad de los puestos de trabajo.

El personal involucrado pertenece a tres grandes categorías:

- la categoría vinculada con las actividades de dirección, del personal ejecutivo, de gestión, de relaciones públicas...;

- la categoría vinculada con los puestos del sistema de información (ingenieros y técnicos, usuarios de sistemas de oficina...);

- la categoría vinculada con la seguridad de los sistemas de información (ingenieros y técnicos del equipo de seguridad, agentes de seguridad...) que requieren una formación especializada.

Una concienciación que no tenga en cuenta las particularidades operativas de cada clase de usuarios y los requerimientos más o menos importantes vinculados con las responsabilidades o con los puestos de trabajo no logrará los objetivos establecidos y hará ver la seguridad como una restricción adicional sin valor agregado respecto de la productividad del puesto de trabajo.

FOR-06: Concienciación regular del personal sobre la

La información permanente de las personas apunta a lograr un nivel de vigilancia constante. Esta información se refiere, en particular, a las evoluciones de la PSSI y de las amenazas. Este proceso permite actualizar la información, comunicar nueva información, y, también, hacer un llamado de atención sobre las normas o instrucciones que no se aplican correctamente. También debe difundirse

SSI	cualquier evolución referida a la organización y a los requerimientos generales de la SSI.
FOR-07: Concienciación sobre el tratamiento de los incidentes	Más allá de la formación para el uso del sistema, el personal involucrado debe ser concienciado y formado, al nivel que convenga, en los aspectos de seguridad de las operaciones que tienen a su cargo. Uno de los puntos esenciales de las obligaciones de seguridad en las tareas de gestión se refiere al cumplimiento de los requerimientos de: - informar inmediatamente de cualquier incidente, - notificar/alertar a quien corresponda (cf. continuación).
FOR-08: Preparación y entrenamiento para la gestión de las situaciones de crisis	Además de prever las posibilidades y el tratamiento (procedimientos) de las situaciones anormales y de los incidentes (FOR-07), es esencial preparar y entrenar al personal involucrado, lo que supone, especialmente: - la presentación de los planes específicos (plan de emergencia, plan de contingencia, plan de recuperación...), - el entrenamiento del personal por medio de simulaciones (ejercicios comparables a los simulacros de incendio). (Cf. Gestión de crisis) Debe existir un programa de formación específico para cada perfil de agente, que apunte a garantizar reacciones reflejas adecuadas en caso de incidente o alerta de seguridad.
FOR-09: Concienciación del personal sobre el uso de las TIC	Deben emprenderse acciones de concienciación del personal para prevenir riesgos de divulgación externa (voluntaria o no), vinculados con el uso de los medios de comunicación que ponen a nuestra disposición las tecnologías de la información y la comunicación (TIC), tales como las comunicaciones por video, teléfono, fax, voz... Esta concienciación debe hacer hincapié especialmente en lo referido al control del destinatario de las comunicaciones, las escuchas clandestinas, las personas que se encuentran cerca.
FOR-10: Formación del personal en el uso de las TIC	Esta formación estará destinada a presentar la responsabilidad de cada uno en el área de la informática y las comunicaciones (TIC: tecnologías de la información y la comunicación) y a formar a cada usuario en el uso de los medios informáticos y de comunicación, así como en los medios de protección que tiene a su disposición.
FOR-11: Concienciación de los usuarios sobre los medios de control	El empleo de medios técnicos para detectar delitos informáticos o para el mantenimiento de los sistemas obliga al organismo a: - controlar los flujos de información, - acceder a los recursos "personales", - reglamentar las comunicaciones y transferencias (red, correo electrónico, Internet), - conservar los elementos de prueba. Para lograr un equilibrio entre control y respeto de la vida privada del individuo, evitando afrontar litigios o, inclusive, atentar contra la imagen de marca del organismo, deben incorporarse acciones destinadas a brindar información a los

actores del sistema de información.

Por tal motivo, se recomienda redactar un manual que reglamente y explique el objetivo de los medios de vigilancia y recopilación de pruebas informáticas.

3.3.10 EXP : Operatividad

EXP-01: Documentación de los procedimientos y normas de uso

Deben identificarse todas las actividades operativas, agrupándolas eventualmente en familias. Cada una de estas actividades deberá contar con una documentación precisa sobre los procedimientos y normas de uso. Esto podrá generar, según las necesidades, varios documentos; cada uno de ellos destinado a una categoría de actores involucrados en función de su rol, de sus responsabilidades y de su necesidad de conocer la información. Dicha documentación deberá mantenerse actualizada.

EXP-02: Integración de la SSI en los procedimientos y normas de uso

La documentación de procedimientos y normas de uso debe contar en todos los casos con un apartado dedicado a la seguridad, validado por la estructura de seguridad implementada en el organismo.

EXP-03: Separación del desarrollo y de las operaciones de producción

La separación de las tareas y entornos de desarrollo, de instalación y de las otras actividades vinculadas con el funcionamiento del sistema de información (utilización, gestión del sistema y de la red, carga de datos, mantenimiento, auditoría de seguridad...) reduce el riesgo de uso incorrecto deliberado o accidental de los recursos del sistema.

Esta norma influye en el nivel de seguridad y en la eficiencia de la división de tareas y responsabilidades, permitiendo:

- incrementar la seguridad, reduciendo el riesgo de modificaciones delictivas o accidentales de programas, gracias a la separación de las tareas que caracterizan al funcionamiento operativo del sistema de información, que requieren recursos diferentes y privilegios de acceso a máquinas críticas desde el punto de vista de la seguridad;

- mejorar la eficiencia de la SSI, dado que la acumulación de funciones técnicas puede incitar a un especialista en informática de un equipo de gestión a "parchar" un software, ignorando voluntariamente las normas de programación mencionadas en la norma anterior (por ejemplo, la ausencia de comentarios en las líneas de código modificadas).

Esta división de las funciones contribuye además a una mejor delimitación de las responsabilidades en caso de incidente.

EXP-04: Condiciones de uso de la externalización informática

Distinguimos diversos tipos de gestión externalizada de la informática: la externalización completa, los teleservicios (entre los cuales se cuenta el mantenimiento remoto), la gestión informática realizada por terceros dentro del establecimiento...Las condiciones de uso de servicios externalizados para la informática deben definirse rigurosamente y, en la medida de lo posible, sobre la base de un análisis específico de los riesgos.

La generalización de los servicios de mantenimiento remoto, por ejemplo, permite optimizar costos gracias a la reducción de los desplazamientos de

	personal. Sin embargo, la instalación de una línea de comunicación entre el sistema de información y el organismo de mantenimiento, y la necesidad de otorgar derechos de acceso de alto nivel incrementan los riesgos de ataques al sistema de información. (Cf. operaciones de teleacción)
EXP-05: Condiciones de seguridad para el mantenimiento de los componentes del SI	El incumplimiento de las instrucciones para la preparación de un componente antes de que sea enviado a mantenimiento puede exponer al organismo a que su sistema de información se vea comprometido o sea atacado. Dicho acondicionamiento consiste en preparar el componente para su reparación verificando los siguientes puntos: - retirar el soporte de la memoria no volátil que haya contenido datos clasificados o confidenciales;, - sobreescribir la memoria restante, de tal modo que se impida cualquier posibilidad de interpretación de los registros anteriores; - verificar que las instalaciones de mantenimiento externas respondan a las mismas normas de seguridad física y de personal aplicadas en las zonas de utilización de los componentes enviados a reparación. Si, por razones técnicas, no fuera posible retirar el soporte de la memoria no volátil, puede resultar necesario exigir que el mantenimiento de un componente se realice dentro del organismo, por personal autorizado. También es fundamental considerar el mantenimiento de los componentes de seguridad.
EXP-06: Condiciones de seguridad para la recuperación tras el mantenimiento	Las condiciones de seguridad para volver a poner en funcionamiento los componentes, tras su reparación, buscan desenmascarar cualquier eventual alteración de programas o falla de funcionamiento. Por lo tanto, pueden establecerse condiciones para la puesta en servicio de dichos componentes como, por ejemplo: - que el componente sea sometido a mediciones de detección cuando sea reintegrado a su zona de seguridad, en función de las condiciones locales, de la evaluación de la amenaza y, en el caso de los ordenadores, de la sensibilidad los datos guardados en la memoria; - para el caso particular del hardware que responde a la norma TEMPEST, que cualquier modificación implique una nueva verificación de su capacidad para evitar emisiones electromagnéticas.
EXP-07: Seguimiento de las operaciones de mantenimiento de los componentes del SI	Esta norma, que se aplica a todos los componentes del sistema de información (hardware y software), adquiere mayor importancia para los componentes que cumplen funciones de seguridad. La falta de seguimiento de las operaciones de mantenimiento tendría como consecuencia el desconocimiento del grado de aptitud de los componentes para cumplir nuevamente con sus funciones; lo que podría llevar a tener una confianza injustificada en el plan de seguridad. El seguimiento de las operaciones de mantenimiento requiere la apertura de un registro completo y detallado de las intervenciones realizadas en los componentes, para que el personal conozca las nuevas configuraciones y

	aplique los procedimientos adecuados. Por otra parte, cuando el organismo dispone de un centro de informática cuya misión principal es la asistencia a los usuarios, es necesario procurar que dicho centro aplique estas mismas normas para las intervenciones que realiza, especialmente cuando entre sus atribuciones se cuenta la instalación de paquetes o tarjetas solicitados por los usuarios en las máquinas del organismo.
EXP-08: Gestión de las prestaciones de servicios externas	El hecho de recurrir a prestadores de servicios externos (debidamente autorizados para contratos de Defensa) para el desarrollo del sistema de información, supone la aplicación estricta de las normas antes mencionadas y un control reforzado de los recursos puestos a su disposición (aplicaciones y ficheros delicados, compiladores, editores, documentación técnica...). La decisión de poner a su disposición recursos delicados debe tomarse teniendo en cuenta los requerimientos operativos de disponibilidad del sistema de información. Deben establecerse claramente, entre el organismo y los prestadores, las responsabilidades y los procedimientos, para la imputabilidad de eventuales incidentes. El recurso a prestaciones de servicio no debe nunca derivar en una subcontratación de la gestión informática (traducción del término anglosajón "facility management"), puesto que la seguridad de un sistema de información constituye un objetivo primordial para los intereses del Estado o del organismo. (Cf. externalización de servicios)
EXP-09: Integración de la SSI en los contratos de gestión informática externalizada	Los contratos de gestión informática externalizada y sus anexos deberán incluir un apartado dedicado a la SSI que especifique claramente los compromisos del prestador y de cada miembro involucrado de su personal. Deberán especificarse, en particular, y de manera muy precisa: - los requerimientos de seguridad a los que se compromete el prestador (que no podrán ser inferiores a los que estarían vigentes internamente); - los procedimientos de control del cumplimiento de dichos requerimientos; - la atribución de responsabilidades específicas para una coordinación eficaz en caso de incidentes o anomalías; - la posibilidad de evolución de los requerimientos y procedimientos, conforme a una evolución de la PSSI o de sus consecuencias operativas, y la obligación, para el prestador, de adecuarse a estas evoluciones.
EXP-10: Seguridad en los servicios externalizados	La decisión de optar por servicios externalizados y el proceso de contratación de dichos servicios deben estar precedidos por un análisis de riesgos y beneficios para el organismo. También deberán considerarse los siguientes aspectos problemáticos: - La responsabilidad del organismo y de los prestadores de los servicios de gestión informática externalizados debe definirse claramente y explicitarse en el contrato. - La unificación de los recursos provistos por los prestadores para responder a las necesidades de varios clientes podría no corresponderse con los objetivos de seguridad.

- Los medios implementados en los sistemas de información del prestador, utilizados para conectarse al sistema de información del organismo podrían no ser necesariamente adecuados, coherentes, incluso compatibles, con los medios de seguridad implementados.

- Las posibilidades y modalidades de control y auditoría por parte del contratante se encuentran a menudo limitadas, especialmente teniendo en cuenta las disposiciones contractuales establecidas o las modalidades prácticas de intervención del contratante en el lugar donde se lleva a cabo la gestión informática externalizada.

- Las personas que utilizan y manipulan el sistema de información no siempre son conocidas por el organismo, o estas personas se encuentran, por otra parte, simultáneamente en contacto con datos de empresas que podrían ser de la competencia, o con responsables de empresas de la competencia.

- Desde el punto de vista técnico, los privilegios otorgados al prestador para realizar su trabajo son, por lo general, particularmente amplios en términos de seguridad (cf. protección de los accesos de mantenimiento) y pueden ser utilizados para introducirse en el sistema de información.

Por todo esto, debería llevarse a cabo un análisis de los riesgos vinculados con estos aspectos problemáticos, a fin de determinar objetivos y medidas de seguridad que cubran los riesgos identificados, especialmente desde el punto de vista de las cláusulas contractuales, la trazabilidad y el seguimiento de las operaciones realizadas.

EXP-11: Control antivirus de los programas y datos antes de ponerlos nuevamente en servicio

Los controles del software y de los ficheros de datos antes de su puesta en servicio apuntan a luchar, en particular, contra la amenaza de contaminación por virus.

Pueden tomarse algunas precauciones para prevenir y detectar la introducción de programas maliciosos (virus, gusanos, troyanos, bombas lógicas...). Todos los soportes de información provenientes del exterior del organismo y, en especial, aquellos cuyo origen sea incierto, deberán ser sometidos a un control. La implementación de medios dedicados a una detección sistemática constituye una respuesta a esta amenaza. Estos medios deben implementarse de tal modo que se garantice que todos los puntos de entrada del sistema informático están controlados (Internet, red, servidores, estaciones de trabajo).

También es necesario identificar y proteger a aquellos elementos del sistema que tienen importantes necesidades de seguridad y a sus posibles vías de contaminación. Hay que contemplar los numerosos medios que pueden llegar a utilizarse para recuperar ficheros (disquetes, discos compactos, ficheros cifrados adjuntados a los mensajes de correo electrónico...).

Por otra parte, deben transmitirse a los usuarios instrucciones claras para que no instalen ningún programa en su estación de trabajo.

EXP-12: Controles de seguridad en fase de uso del sistema de información

El control de seguridad en fase de uso permite reducir los riesgos de atentados contra la disponibilidad e integridad de la información y los datos. Estos controles se traducen, por ejemplo, en verificaciones del uso de los recursos autorizados para el tratamiento de la información.

El primer aspecto de estos controles apunta a los usuarios del sistema de información. La responsabilidad de estos controles recaerá en los ingenieros del

	sistema y de la red que realizan la vigilancia directa utilizando medios de visualización: análisis de las transacciones en curso, ficheros en línea, intentos de conexiones... El segundo aspecto de estos controles apunta a la verificación del buen cumplimiento de los procedimientos de seguridad por parte de los especialistas en informática. Esto abarca, por ejemplo: - el respeto de la secuencia de operaciones planificadas, - el correcto manejo de ficheros, - el uso de las macros autorizadas, - el cumplimiento de las instrucciones para las recuperaciones de errores o para los acontecimientos excepcionales.
EXP-13: Reducción de las vulnerabilidades	Día a día se ofrece mayor cantidad de servicios a través de las redes de oficina; servicios que transmiten todo tipo de datos y cuyas necesidades de seguridad son muy heterogéneas.Debe establecerse una política de vigilancia de la evolución de la seguridad que permita seguir las últimas novedades en esta área y reaccionar adecuadamente cuando aparezcan vulnerabilidades significativas en los sistemas y aplicaciones estándar del sistema de información. La vigilancia deberá centrarse en los métodos de ataque, vulnerabilidades y soluciones de seguridad.
EXP-14: Procedimientos de gestión segura de la información y los datos	Los datos y sus soportes deberían heredar el mismo nivel de protección que la información que les han dado origen. La información y los datos deben ser gestionados de una manera específica, en función de su clasificación. Por esta razón, la gestión de datos vitales o delicados puede requerir la implementación de medidas técnicas particulares (por ejemplo, el uso de sistemas que soporten cortes de energía eléctrica o el uso de RAID 1) u organizacionales (por ejemplo, la norma de aislamiento de los puestos de trabajo delicados), a fin de evitar incidentes durante la fase de procesamiento de la información. Asimismo, los datos personales deben recibir la protección requerida por la Ley. La presente norma, centrada en los procedimientos de uso seguro, se justifica por la vulnerabilidad de los datos, vulnerabilidad existente en razón del paso de la información por diferentes fases (procesamientos, copias de seguridad y transporte en soportes de información, almacenamiento, destrucción...). Por esta razón, los procedimientos y controles de seguridad apuntan a garantizar la continuidad de la protección en estas diferentes etapas de uso. Entre los procedimientos que deben implementarse, los referidos al respaldo de los datos y a la destrucción de sus soportes de información clasificados son de importancia primordial para la seguridad. - El respaldo de los datos apunta a resguardar su integridad y disponibilidad: las copias de seguridad deben realizarse con regularidad y los soportes informáticos resultantes deben almacenarse en lugares alejados de la zona de procesamiento de dicha información, lugares que ofrezcan el mismo nivel de protección. La realización de pruebas de integridad de las copias de seguridad aportará la garantía de la continuidad de servicio. - La destrucción de los soportes de datos clasificados supone que los datos

	registrados se borren o sobrescriban antes de que se destruya su suporte magnético (cintas magnéticas, disquetes, discos extraíbles y fijos, memoria almacenada en discos...). - Puede preverse, para los datos que están protegidos por el secreto de defensa, en conformidad con la reglamentación vigente, un cifrado de datos que permita el almacenamiento intermedio de sus soportes durante procesos discontinuos.
EXP-15: Implementación de una organización para la lucha contra el código malicioso	La implementación de una organización y de una PSSI contra la amenaza de virus permite disminuir los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información. Esta organización debe disponer de las siguientes entidades: - un equipo antivirus (gestión, procesamiento, actualización...); - un equipo de asistencia técnica - un equipo de gestión de crisis; - una estructura de vigilancia. En la lucha contra los códigos maliciosos, es primordial definir correctamente las relaciones entre los diferentes participantes, en particular en lo que se refiere a la vigilancia, a quienes deben intervenir en caso de crisis y a la actualización de las herramientas y procedimientos. La definición de una organización de seguridad contra el código malicioso deberá definir, especialmente, la organización que hay que implementar y los roles y responsabilidades de cada actor. Será igualmente necesario implementar una arquitectura técnica de protección contra los virus para todos los componentes del sistema informático (estaciones de trabajo, servidores de correo electrónico, servidores Internet, servidores de copias de seguridad, de datos...).
EXP-16: Instrucciones de seguridad referidas a la teleacción	La teleacción agrupa a todas las acciones de uso de la red y de las estaciones de trabajo que se realicen en forma remota: copias de seguridad o uso remoto, instalación remota de aplicaciones, tratamiento remoto de anomalías, mantenimiento remoto... Los accesos para teleactividades son especiales cuando deben aplicarse a estaciones de trabajo que han sido asignadas a usuarios. Efectivamente, es necesario garantizar al usuario que conserva el control de su entorno y que nadie puede intervenir en sus archivos o en su sesión de trabajo sin tener su autorización previa. Esto debe contribuir a garantizar una relación de confianza mutua entre los administradores de la red y los usuarios.
EXP-17: Protección y uso del correo electrónico	Deben establecerse normas claras y simples para garantizar la confianza en el uso del correo electrónico. Será conveniente, por lo tanto, establecer una lista de medidas técnicas y no técnicas para luchar contra: - la propagación y ejecución de códigos maliciosos; - la intercepción de datos delicados transmitidos sin cifrar por medio del correo electrónico; - la desinformación o el spam;

	- la publicación de datos ilegales, difamatorios o de acosos; Será además conveniente definir las normas referidas a: - la conservación de pruebas de los intercambios electrónicos; - el uso de medios de seguridad (autenticación, cifrado de firma); - el uso del correo desde fuera del organismo (cf. acceso remoto); - la sobrecarga del sistema de correo electrónico.
EXP-18: Normas específicas de filtrado de accesos	Podrán implementarse normas técnicas de filtrado en los enrutadores, los cortafuegos y los servidores de correo electrónico, para autorizar el acceso sólo a algunos servidores identificados. Ciertamente, todo lo que no está explícitamente autorizado debería impedirse mediante el filtrado de los accesos. Este principio también es válido internamente.
EXP-19: Normas de conservación y de destrucción de los datos que requieren protección	Ciertas categorías de datos requieren condiciones de conservación y de destrucción especiales. En lo que se refiere a los datos protegidos por el secreto de defensa, la reglamentación especificará las medidas que deben tomarse en cuenta según el nivel de clasificación de dicha información. Para las otras categorías, las medidas se adecuarán al entorno propio del organismo y deberán ser coherentes entre sí. El control previo de las buenas condiciones de almacenamiento es un aspecto fundamental, puesto que la información se confía por contrato a un organismo. La destrucción de emergencia puede ser, para algunos organismos, un recurso primordial en situaciones excepcionales (disturbios, guerras civiles...), pero, en la mayor parte de los casos, pueden adoptarse normas precisas para eliminar la información caduca que conserva un carácter residual de confidencialidad. Por otra parte, el archivado de documentos en soporte magnético responde a obligaciones jurídicas en cuanto a período de conservación y de protección de los soportes de información, en función del tipo de datos involucrados (información contable o fiscal, información referida al personal...).
EXP-20: Control de los soportes extraíbles antes de su puesta en servicio	Esta norma, centrada en el control de los soportes extraíbles, apunta principalmente a preservar la confidencialidad de la información e involucra a los organismos que procesan datos delicados protegidos por el secreto de defensa o información considerada estratégica para sus actividades. Una medida fundamental anterior al control de los soportes extraíbles, antes de su reutilización en otra instalación protegida, consiste en borrar los datos en ellos registrados recubriéndolos completamente mediante caracteres numéricos o alfanuméricos. Para la información protegida por el secreto de defensa, los soportes de memoria conservan la categoría más alta de clasificación de los datos utilizada para esa información a partir de su origen (salvo en caso de liberación de la información). Este principio puede aplicarse a los datos no clasificados muy delicados.
EXP-21: Los soportes de información,	Por lo general, los organismos son concientes de la importancia de la seguridad de los sistemas. Sin embargo, la protección de los soportes extraíbles (disquete, cinta de respaldo, listado impreso, informe...) se descuida muy a menudo, aun

fuentes de infección y de riesgo de divulgación	cuando dichos soportes contienen información del organismo. Denominamos soportes de información a todos los medios que contienen datos: principalmente, los soportes informáticos, los soportes papel (listado impreso, documentación, impresión de informes...). Los soportes de información deben estar protegidos conforme a las normas referidas a la clasificación de los datos que albergan. Deben existir, por lo tanto, y en función de la clasificación, normas de seguridad referidas a la gestión, el control, el almacenamiento (contra robo y destrucción), el transporte y la eliminación de los soportes de información. Aunque hoy la amenaza de virus (códigos maliciosos) proviene principalmente de las redes públicas, la introducción de virus mediante los soportes informáticos sigue constituyendo una problemática importante (cf. lucha antivirus). Existen normas específicas referidas al ingreso/salida de soportes informáticos en zonas clasificadas (gestión de un registro de soportes informáticos, de su contenido...); (cf. continuidad en la protección de los datos).
EXP-22: Eliminación de los soportes de información o salida de hardware	El hardware contiene soportes de información del organismo. Debe controlarse el ingreso y, sobre todo, la salida de dichos soportes del organismo. Los datos que contienen dichos soportes de información, del mismo modo que los datos contenidos en cualquier otro soporte de información del organismo, deben destruirse cuando son donados o desechados sus soportes, ya sea mediante la destrucción física de los mismos, o bien mediante un borrado lógico seguro (múltiples sobrescritos). El organismo debe, por lo tanto, definir las normas para la destrucción de los datos en función del tipo de soporte de información, y, llegado el caso, en función de su nivel de clasificación. En el caso del soporte papel, el organismo puede instalar destructoras de papel o bien centralizar los soportes de información que deben destruirse y confiar esta tarea a organismos especializados (previa firma de un compromiso de destrucción). En ambos casos, debe prestarse mucha atención a la protección del almacenamiento de los soportes de información antes de su destrucción.
EXP-23: Fotocopiado de documentos	Deben enunciarse directivas de seguridad que regulen el fotocopiado en función de la clasificación del documento. Estas directivas deberán contemplar las obligaciones vinculadas con la "fotocopia ilegal", que cuentan con una legislación específica.
EXP-24: Almacenamiento de la información por parte del organismo	Deben definirse normas de seguridad para el almacenamiento de los datos, normas que deberán ser aplicadas por todo el personal, en función de la clasificación de la información involucrada. Estas normas deben apuntar principalmente a garantizar la protección de los datos contra cualquier robo, divulgación o alteración por parte de personas no autorizadas.
EXP-25: Conexión de los puestos móviles y PDA	Deben redactarse normas de seguridad que regulen los tipos de datos que pueden almacenarse en estas unidades. Deben implementarse medios de protección y/o de control para garantizar el cumplimiento de dichas normas. La conexión de estas unidades al sistema de información del organismo debe autorizarse y debe respetar la PSSI del organismo.

Debe prestarse también mucha atención para evitar que estos equipos puedan servir de pasarela entre el sistema de información y una red pública.

3.3.11 ENV : Aspectos físicos y entorno

ENV-01: Continuidad en la gestión de los bienes físicos

La gestión de los bienes físicos se realiza a lo largo de todo su ciclo de vida: fases de asignación, instalación, funcionamiento, mantenimiento, eliminación y destrucción. Podría ser necesario que estos bienes cambien de propietario o de responsable, de entorno o de uso (préstamo de hardware para una exposición, reasignación de un hardware en el marco de un nuevo proyecto).

La norma prevé que las medidas seleccionadas ofrezcan una protección continua, cualesquiera sean las evoluciones o cambios de uso de los bienes físicos.

Esta continuidad de gestión se basa en la adopción de una clasificación (que incluirá, llegado el caso, la clasificación de defensa tal como la define la [IGI 900]) sobre el seguimiento de los bienes físicos desde su puesta en servicio y su evolución hasta su reemplazo. Las principales medidas que se desprenden de esta norma afectan al inventario y marcado de bienes y a las medidas específicas de protección física correspondiente a su estado (préstamo, mantenimiento...) o a su clasificación:

- El inventario de los bienes físicos permite identificar aquellos bienes que requieren protección.

- La operación de marcado es la materialización concreta del reconocimiento de que un elemento pertenece a determinada clase.

- Las medidas específicas de protección física determinan las acciones que deben realizarse en función de la clasificación adoptada. Por ejemplo, una calculadora marcada como "confidencial" deberá ubicarse en un entorno físico adecuado a este nivel de protección, como es, por ejemplo, el de una "zona reservada".

ENV-02: Consideración de las restricciones operativas del organismo

Una implementación de medios y procedimientos de seguridad física que no tuviera en cuenta las restricciones del organismo podría constituir un obstáculo para el buen desempeño de las tareas operativas y generar un rechazo hacia el tema seguridad por parte del personal.

Es necesario, por tanto, contemplar las restricciones operativas del organismo en la implementación de los medios y procedimientos de seguridad física.

ENV-03: Exhaustividad de las medidas de seguridad física

Deberían tenerse en cuenta los tipos de medidas que se detallan en este punto.

Las medidas de protección de los bienes físicos tienen por objetivo reducir la importancia de los perjuicios, principalmente en cuanto a disponibilidad, integridad y confidencialidad.

La falta de soluciones universales capaces de responder a todas las formas de amenazas obliga al organismo a implementar un conjunto de medidas susceptibles de contrarrestar el alcance de un ataque y reparar los daños causados: se trata de las medidas de prevención, detección, reacción y recuperación.

Las medidas de prevención apuntan a disminuir la probabilidad de aparición de un siniestro. Consisten, por ejemplo, en prestar atención a la ubicación de ciertos locales (como los archivos de cintas magnéticas, las salas de archivos, las canalizaciones, las salas donde se guardan productos peligrosos), teniendo en cuenta los riesgos de incendio o de inundación, y en controlar el uso apropiado del hardware.

Las medidas de detección apuntan a alertar cuando ocurre un intento de intrusión o cuando se desencadena un siniestro en el perímetro del sistema de información. Deben permitir también localizar dicha alerta. Estas medidas se traducen en la implementación, en los lugares críticos, de medios de detección y alerta como, por ejemplo, sensores de calor o cámaras de vigilancia.

Las medidas de reacción apuntan a combatir un siniestro declarado a fin de reducir su impacto. Estas medidas se traducen en el desencadenamiento de medios de intervención previstos por el organismo como, por ejemplo, un servicio de lucha contra incendios.

Las medidas de recuperación apuntan a limitar las consecuencias de un siniestro y a facilitar el restablecimiento del funcionamiento normal del sistema de información. Pueden traducirse en la activación de medios de emergencia o en la desactivación de funciones de seguridad como, por ejemplo, la supresión temporal del control de acceso físico en el marco de un funcionamiento de la seguridad en modo de funcionalidad reducida.

Para todos los siniestros previstos por el organismo, las medidas elegidas deben ser graduales, a fin de ofrecer un nivel de resistencia suficiente para contrarrestar o atenuar el ataque.

ENV-04: Aislamiento de los sistemas delicados o vitales

Aislar los sistemas delicados o vitales permite minimizar la exposición de los bienes a las amenazas. Así se reducen los riesgos. Esto ofrece, además, la posibilidad de lograr que las medidas de seguridad sean más proporcionales a los riesgos, reduciendo los costos de una protección total.

ENV-05: Adecuación de las medidas de seguridad física a los tipos de bienes

Las medidas de seguridad física deben aplicarse a todos los locales. Estas medidas apuntan, en primer lugar, a proteger al personal y, en segundo lugar, a reducir los riesgos de destrucción o divulgación que podrían atentar directa o indirectamente contra los intereses vitales de la empresa u organismo.

Esta norma indica que las medidas mencionadas en la norma anterior pueden presentarse en tres categorías de bienes físicos, a saber: la infraestructura, el hardware y los equipos de emergencia.

ENV-06: Protecciones contra los accidentes y fallos

En los locales que albergan equipos vitales para el sistema de información (sin olvidar los componentes de la infraestructura de red), considerando las amenazas el entorno cercano, será necesario prever medidas destinadas a:

- impedir daños ocasionados por el agua: detección y reacción (lo mejor es evitar ubicar equipos en locales de riesgo como salas en las cuales existen conductos

	de agua o situadas en zonas anegadizas); - la detección y extinción de incendios; - el control de la energía eléctrica y suministro de emergencia (los elementos de protección deben garantizar, como mínimo, el tiempo de alimentación mínimo requerido para realizar todas las operaciones de respaldo necesarias); - la implementación de redes de emergencia para las telecomunicaciones (prestar mucha atención a los procedimientos de transferencia hacia líneas de emergencia en caso de corte de línea); - la climatización y acondicionamiento de los ambientes (tener en cuenta el abastecimiento de los insumos como el agua, el gas y los filtros, así como las medidas para combatir la presencia de polvo); - la implementación de procedimientos formalizados de reacción en caso de siniestros o fallos (inclusive fuera del horario habitual de trabajo); - la implementación de procedimientos de emergencia. El control del entorno debe tener en cuenta la temperatura, la humedad, el polvo y las vibraciones.Es necesario prever también un plan de situación de emergencia por si se producen siniestros no controlables. (Cf. gestión de crisis) Todos los equipos de protección instalados deben controlarse regularmente. Existen requisitos legales referidos a los controles (especialmente en lo referido a las medidas para combatir los incendios). Se recomienda seriamente aplicar estos controles inclusive a los equipos para los cuales dichos controles no son obligatorios (por ejemplo, la detección de presencia de agua).
ENV-07: Protección física del cableado y de las redes de telecomunicación	El cableado de telecomunicaciones e informático debe, en la medida de lo posible, estar protegido contra cualquier acceso malicioso que pudiera dar lugar a escuchas (utilizando, por ejemplo, líneas bajo tierra, cables ocultos...). Es indispensable garantizar la protección de los accesos a las terminales y los equipos de encaminamiento. La protección de los accesos a los cableados y a los otros componentes de la red (autorizados o no) consiste no sólo en impedir la escucha pasiva (y, a veces, activa), sino también en evitar que, por accidente, estos medios sean dañados.
ENV-08: Subdivisión de la infraestructura en zonas de seguridad	Los establecimientos, los edificios y los locales que contienen bienes materiales o inmateriales (los datos y sus soportes, el hardware que conforma el sistema de información) o que albergan actividades críticas desde el punto de vista de la seguridad, deben ser controlados, especialmente a nivel de sus accesos. Debe establecerse una zona de seguridad y una zona en la cual se tomen disposiciones permanentes para controlar los movimientos del personal y del hardware, así como para detectar e impedir cualquier escucha. Una subdivisión de la infraestructura en zonas de seguridad facilitará la implementación de dispositivos adaptados, especialmente para el control de la circulación del personal mediante la asignación de derechos de acceso específicos para cada zona. Estos derechos podrán estar asociados a los

	puestos de trabajo y a los niveles de responsabilidad.
ENV-09: Aplicación de las modalidades de recepción y circulación de visitantes	Generalmente, el servicio de seguridad general fija las modalidades de recepción y circulación de los visitantes. Pero, sin interferir en ello, es deber de cada usuario del sistema de información hacerse cargo de la aplicación de esta norma en su propia zona de trabajo o cerca de su puesto de trabajo. El responsable-depositario de la información es, efectivamente, quien está en mejores condiciones de verificar que no se atente contra el patrimonio informacional que le ha sido confiado. Esta norma debe conciliarse con la que recomienda subdividir la infraestructura en zonas de seguridad, que aporta una gran facilidad para el control de los visitantes.
ENV-10: Gestión específica de los bienes físicos que requieren protección	La gestión de los bienes físicos que requieren protección abarca la adopción de una clasificación o de una tipología, las medidas de gestión de dichos bienes y las medidas de protección a lo largo de su vida útil. Debe respetarse el principio de adaptar estos medios de protección física, como cualquier medida de seguridad, al valor de los bienes que deben protegerse, pero armonizando también estas medidas con el resto de las medidas de seguridad aplicadas. El artículo 10 de la [IGI 900] nos brinda la siguiente definición: "Todo documento, software o hardware que, por su integridad o confidencialidad, contribuya a la seguridad del sistema de información, recibirá la denominación ACSSI que recuerda que su gestión y protección deben garantizarse conforme a lo indicado en la instrucción ministerial referida a los Artículos Controlados de la Seguridad de los Sistemas de Información". La adopción de una tipología para los bienes físicos no clasificados de defensa permite agruparlos en función de su naturaleza y destino. Se establecen clases de protección en función del nivel de requerimiento de seguridad, es decir, de los criterios de confidencialidad, integridad y disponibilidad vinculados con dichos bienes, a fin garantizar una vigilancia continua. La tipología adoptada es específica para la misión u oficio, la cultura y las restricciones propias del organismo.
ENV-11: Procedimientos de gestión segura de los medios descentralizados	Los medios descentralizados, dedicados o retirados de su zona de seguridad (microordenadores, hardware portátil, impresoras remotas, fotocopiadoras, fax...) se caracterizan a menudo por ser equipos de uso reducido, o incluso asignados a usuarios aislados. Sin asistencia inmediata y sin recurrir a las protecciones físicas de una zona de seguridad, la probabilidad de incidente o de delitos contra la seguridad de dichos bienes sigue siendo alta: la indiscreción o el delito informático representan una amenaza importante dado que las instrucciones de verificación son más difíciles de implementar. Por esta razón, la gestión de dichos medios requiere medidas específicas adaptadas a su entorno. En la medida de lo posible, los equipos periféricos deben estar situados en una zona vigilada. El caso del hardware portátil merece un análisis especial. Ciertamente, a partir del incremento de la capacidad de memoria y de la potencia de los procesadores, las máquinas portátiles se utilizan cada vez más. Pero están expuestas a amenazas más variadas que el hardware fijo y el uso

	que se les da dificulta aún más el control necesario para resguardar la información. El hecho de que sean portátiles y su tamaño reducido incrementa bastante la probabilidad de pérdida o robo. En la medida de lo posible, los datos que requieren protección sólo deberían poder procesarse en microordenadores portátiles dentro de lugares específicamente designados en función del nivel de clasificación de dichos datos. Cuando se retira este hardware del organismo, debe aplicarse el mismo procedimiento que se utiliza para la salida de documentación clasificada.
ENV-12: Protección de la documentación de seguridad	La documentación de seguridad debe estar protegida contra todo acceso no autorizado. Su protección debe estar al mismo nivel que los componentes a los cuales se refiere. Podemos sugerir las siguientes medidas: - Todo responsable-poseedor de documentos de seguridad deberá conocer el valor de los documentos que le han sido confiados y controlar su uso. - Sólo el personal autorizado deberá poder manipular dichos documentos. - Los documentos deberán guardarse en lugares seguros. - La difusión de los mismos, que realizará el responsable de seguridad, podrá restringirse a un mínimo de personas.
ENV-13: Protección contra robos de los equipos	El agente a quien se el asigne el equipo, aun si dicha asignación es temporal, será responsable, desde el momento de la asignación, de protegerlo utilizando medios coherentes y adecuados. En la medida de lo posible, cuando un poseedor de un bien deba sacar el equipo del establecimiento, se le recomendará que almacene en dicho equipo sólo la información estrictamente necesaria para cumplir con su misión fuera del establecimiento. Si fuera necesario, deberá transportar la información en un soporte externo extraíble. Como los riesgos de robo de microordenadores portátiles es importante aun dentro del establecimiento del organismo, deberá realizarse un inventario y control frecuente de las máquinas. Deberá formalizarse un procedimiento específico para definir las acciones que deben llevar a cabo el poseedor o el organismo en caso de robo del equipo.
ENV-14: Protección de los soportes de copias de seguridad	Los soportes de copias de seguridad deben estar protegidos contra cualquier riesgo de destrucción, divulgación o robo. Debe prestarse mucha atención a este tipo de soportes porque son, por su misma naturaleza, debido a que contienen parte de los datos que se encuentran en un sistema, uno de los blancos preferidos para robar información y destruir la capacidad del organismo para recuperarse tras un siniestro.
ENV-15: Protección de la documentación del sistema	La documentación de los sistemas (diseño de redes, plan de asignación de nombres...) contiene datos que, vinculados con otros (información sobre las vulnerabilidades...) conforman elementos vitales para el éxito de los ataques al sistema. Su divulgación fuera del organismo puede brindarle a algunas personas la oportunidad de llevar a cabo intentos de intrusión. Resulta esencial, por lo tanto, procurar que se clasifique dicha documentación y controlar su difusión fuera del organismo, incluso a los proveedores.

ENV-16: Uso fuera del establecimiento

La salida y el uso fuera del organismo de cualquier equipo informático deberá ser autorizada. Deben establecerse normas para restringir sus usos en lugares públicos o en otros sistemas de información.

Su conexión al sistema de información de un cliente o asociado deberá ser autorizada por ese otro organismo y su propietario deberá respetar la PSSI.

El equipo informático deberá estar protegido para evitar cualquier acceso no autorizado a los datos que dicho equipo almacena y procesa.

3.3.12 AUT : Identificación/autenticación

AUT-01: Uso de una misma clave para acceder a varios servicios

En función de las aplicaciones y sistemas, los medios utilizados para proteger las claves de autenticación pertenecerán a diferentes niveles de aseguramiento. Es fundamental que los usuarios se informen sobre la solidez de los sistemas de autenticación para poder utilizar una misma clave en sistemas cuya protección sea coherente (ejemplo: uso de una misma contraseña para autenticación en el sistema operativo y en diferentes aplicaciones).

Por tal razón, será conveniente utilizar una misma clave sólo para servicios con niveles de aseguramiento equivalentes.

AUT-02: Combinación de los medios de autenticación

Para acceder al sistema de información se requiere que los usuarios justifiquen su identidad al inicio de la sesión (y, en ciertos casos, durante la sesión), presentando un elemento de autenticación. Las técnicas de autenticación actuales se basan en tres medios:

- lo que se sabe, como, por ejemplo, las contraseñas;

- lo que se tiene, como, por ejemplo, las tarjetas inteligentes;

- lo que se es, es decir, una característica personal (huellas digitales, análisis de retina, reconocimiento de firma dinámica...).

La combinación de estos tres medios constituye una autenticación completa y eficaz pero representa un costo relativamente alto. En consecuencia, el responsable-poseedor debe determinar, con ayuda del agente de seguridad y a partir de estos tres conceptos, cuáles son las combinaciones más adecuadas para su subsistema de información o sus aplicaciones delicadas.

La reunión de al menos dos de estos conceptos se conoce normalmente como autenticación fuerte.

La elección de una autenticación basada sólo en el concepto de "lo que se sabe" representa el perfil mínimo de seguridad para un sistema de información. Será conveniente, por lo tanto, optar al menos por mecanismos dinámicos como las contraseñas que se pueden utilizar sólo una vez o bien por aquellos mecanismos sujetos a un límite de cantidad de usos. En este caso, el mecanismo utilizado es un contador de accesos en el cual se centra la protección.

Por lo tanto, será conveniente prever expresamente una gestión estricta de los elementos de autenticación en los que se basan los mecanismos utilizados.

AUT-03: Unicidad de la identidad de los usuarios

La identidad de los usuarios debe gestionarse bajo el control conjunto de la dirección del sistema y del responsable de la seguridad de un establecimiento o unidad operativa (nivel del agente de seguridad).

La identificación única (e inequívoca) del propietario de un acceso es

	fundamental para garantizar la trazabilidad de las operaciones y el diagnóstico de una anomalía de seguridad (cf. control y auditoría).
AUT-04: Entrega y alcance de los medios de autenticación	Las tecnologías utilizadas para controlar los accesos a un sistema de información deberían ser tan sofisticadas como sea posible. La entrega, uso y gestión de estos medios continúan siendo elementos vitales del sistema. Por ello, deben formalizarse claramente y respetarse estrictamente las siguientes normas: - la entrega de un acceso a un usuario debe estar precedida de un compromiso formal de este último respecto de las normas básicas de protección de los medios de acceso proporcionados y del deber de avisar en caso de robo (o incluso sólo de sospecha de divulgación de la clave) (cf. responsabilidades, cf. asignación de puestos delicados); - la entrega de los medios de acceso (contraseñas, tarjeta inteligente...) debe realizarse asegurándose de que sólo su propietario tendrá conocimiento de éstas; - el tratamiento para una declaración de robo o de pérdida de una clave debe garantizar la protección contra la usurpación de la identidad del usuario; - la partida de un miembro del personal (incluso su transferencia) debe conducir sistemáticamente a la supresión de todos sus accesos al sistema de información. Hay que considerar que hay una violación de la seguridad cuando dos personas o más conocen, por ejemplo, la contraseña correspondiente a una identidad de usuario, a menos que esto haya sido previsto para asegurar la continuidad de las funciones de administración del sistema. Si bien es inevitable, en ciertos casos, permitir que se compartan una identidad y un elemento de autenticación, pueden especificarse medidas especiales, tales como sobres sellados con justificación de su utilización, para prevenir cualquier abuso o uso incorrecto.

3.3.13 CAL : Control de acceso lógico a los bienes

CAL-01: Dispositivos y procedimientos de protección contra las intrusiones	La arquitectura de las infraestructuras de comunicación debe incluir dispositivos y procedimientos que garanticen el nivel adecuado de protección contra las instrucciones. El acceso al SI y a sus principales recursos (aplicaciones) debe ser controlado a fin de protegerlo de accesos maliciosos (intrusiones). Los medios que deben implementarse varían en función de los objetivos de seguridad y pueden incluir medidas tales como dispositivos guardabarrera (cortafuegos) y sistemas de autenticación y control de acceso. Luego de realizar un análisis de los riesgos SSI que incluya un inventario de cada uno de los objetivos potenciales y de los medios de acceso posibles de los atacantes, será conveniente implementar dispositivos de defensa adecuados para cubrir los objetivos de seguridad identificados.
CAL-02: Aislamiento de las redes y control de	El aislamiento de las redes tiene por objetivo: - facilitar el control de acceso;

los flujos

- lograr una mejor protección contra las intrusiones;

- impedir la fuga de información:

o hacia redes o puestos de trabajo internos de la empresa, llegando a personas que no tienen necesidad de conocer esa información;

o hacia redes o puestos fuera de la empresa;

o mediante la conexión desde el exterior de la empresa, utilizando la técnica de pasarela, por ejemplo, gracias a un puesto conectado al mismo tiempo con la red interna de la empresa y con un módem.

Este aislamiento permite crear zonas reservadas (perímetros de seguridad bien identificados) tomando en cuenta la necesidad existente de conocer determinada información. Tales perímetros internos deben implementarse cada vez que un análisis permita identificar subconjuntos o aplicaciones delicadas que justifiquen una política de seguridad y control de acceso y comunicaciones particulares.Las comunicaciones entre el interior y el exterior de un perímetro de seguridad deben pasar sistemáticamente por un dispositivo (guardabarrera) previsto a tal efecto, que tendrá a su cargo el control del cumplimiento de los requerimientos específicos de ese perímetro. Para ello es indispensable que exista y que se documente una "matriz de los flujos" en la frontera: ¿Qué comunicación? ¿Desde quién? ¿Hacia quién? ¿Con qué contenido? ¿En qué condiciones?El aislamiento de redes que permite controlar los flujos de información se basa en los derechos de acceso de las personas, funciones y procesos.

Una de las soluciones de aislamiento reside en la protección de los datos delicados durante su transmisión.

El principio consiste en controlar que se alcance correctamente el nivel de protección requerido para los datos transmitidos.

La protección de los datos delicados durante su transmisión se organiza de tal modo que los diferentes tipos de ataques a la red de transmisión sean lo menos eficaces posible.

La organización de esta protección apunta a:

- el encaminamiento del tráfico incluso en un ambiente de ruido o saturación (que consiste en impedir o dificultar el funcionamiento de las comunicaciones);

- la garantía contra la intrusión (que consiste en introducir o modificar mensajes con la intención de engañar);

- la defensa contra la intercepción (que es la recepción de emisiones no autorizadas);

- la defensa contra el análisis de tráfico (que permite obtener información a partir del estudio del tráfico).

El recurso a los medios de cifrado y la utilización de hardware protegido contra la emisión de ondas electromagnéticas que comprometen la seguridad del sistema constituyen los medios de protección clásicos en materia de seguridad de las comunicaciones.

El cifrado se define como el conjunto de medios criptológicos que permiten

proteger los datos transmitidos, de tal modo que se vuelvan ininteligibles para cualquier persona que no esté autorizada a conocerlos. Se utiliza el cifrado de los mensajes o bien el cifrado de los canales de transmisión.

El principio abarca el hecho de que, si las medidas de seguridad que corresponden al nivel de protección necesario requieren medios de cifrado, el uso de dichos medios se subordinará al cumplimiento de la ley y de la reglamentación vigentes y deberá ir acompañado de medidas organizacionales que permitan su gestión específica.

CAL-03: Modalidades de uso seguro de las redes de telecomunicación del organismo

El uso seguro de las redes de telecomunicación del organismo no debe implicar una nueva revisión de las medidas de seguridad tomadas a nivel de la infraestructura (por ejemplo, la creación de zonas reservadas), del personal (por ejemplo, la gestión de la necesidad de conocer la información), de la organización de la seguridad o de los recursos en hardware y software.

Es tanto más importante definir las modalidades de uso de las redes de telecomunicación del organismo cuando las posibilidades de acceso de los usuarios aumentan debido a las eventuales interconexiones de las redes internas.

El uso seguro de las redes de telecomunicación apela a la implementación de funciones y mecanismos destinados a garantizar la seguridad de los datos que se están transmitiendo. Se puede adoptar las siguientes subdivisión:

- la autenticación;

- el control de acceso;

- la confidencialidad de los datos;

- la integridad de los datos;

- el no repudio;

- la disponibilidad.

Entre estas funciones, el control de acceso se basa en medidas de gestión y control continuadas en el tiempo y centradas, por ejemplo, en los siguientes aspectos:

- el acceso de los usuarios a los servicios para los cuales han sido autorizados;

- la conexión al sistema de información de los ordenadores aislados o que se encuentran fuera del organismo;

- la separación de las redes dedicadas a áreas particulares;

- el encaminamiento de las comunicaciones por los canales autorizados.

CAL-04: Organización de los accesos al sistema de información

El organismo debe establecer reglas e identificar normas técnicas para garantizar el control y la gestión de los accesos al sistema de información.

Dichas normas deben definir los niveles de aseguramiento de los medios de control de acceso para:

- el acceso a la red de la empresa (a la intranet) y a los servicios transversales - principalmente correo electrónico y servicios de Internet- desde los establecimientos del organismo;

- de ser necesario, el acceso a una subred segura;

- el acceso a las aplicaciones del organismo;

- el acceso desde fuera del organismo a los servicios transversales de la empresa, en particular, al correo electrónico;

- el acceso a los equipos conectados a la red del organismo;

- el acceso desde las estaciones de trabajo del organismo a otras redes, desde el establecimiento del organismo o fuera del establecimiento;

- el acceso por parte de los proveedores al sistema de información;

- los accesos públicos o "invitados".

Las siguientes características deben definirse en función de las necesidades de seguridad de los datos y/o de las funciones del sistema de información:

- tecnología que debe utilizarse (algoritmo de autenticación, contraseña utilizada sólo una vez ...);

- protección de las claves (ficheros de contraseña generados por los sistemas o aplicaciones);

- condiciones para la asignación de un acceso (compromiso del usuario respecto de las normas básicas de protección del acceso);

- requerimientos de solidez de los medios de acceso y contraseñas -normas de elaboración - frecuencia de cambio de contraseñas - registro de contraseñas no reutilizables.

- vida útil de la asignación del acceso;- cualquier procedimiento de autenticación para accesos delicados o que utilicen medios de comunicación que no son considerados de confianza (redes públicas) debe garantizar la no divulgación de los elementos de autenticación;

- procedimiento en caso de repetidos intentos de conexión infructuosos;

- limitación del tiempo de conexión;

- procedimiento en caso de denuncia de pérdida de una clave; procedimiento para combatir las usurpaciones de identidad;

- procedimiento de supresión de los accesos en caso de partida del personal o de robo de hardware.

Debe prestarse especial atención a la protección (especialmente contra el robo de sesión, la divulgación de claves, la usurpación de identidad, la saturación voluntaria del acceso...) de los accesos al sistema de información, que pueden utilizarse en forma remota, fuera de los locales del organismo (accesos a Internet, accesos a la red conmutada).

Para cada uno de estos accesos, deben redactarse procedimientos referidos a la definición de perfiles (incluidos los perfiles de los administradores de la red y de las aplicaciones), a la asignación y a la gestión de los accesos (cf. permisos).

Se recomienda especialmente respetar el principio de asignar un acceso y diversos privilegios sólo cuando son necesarios para la realización de una tarea.

	Es fundamental que los usuarios sean conscientes de la protección de los datos y de los medios que les han sido asignados para acceder al sistema de información del organismo (las estaciones de trabajo son los principales puntos de acceso al sistema de información).
CAL-05: Ficheros que contienen contraseñas	En la medida de lo posible, todo fichero que contenga contraseñas (o claves) debe ser eliminado o cifrado (por ejemplo, el script de conexión).
CAL-06: Supresión de los accesos no controlados al sistema de información	Es importante poder controlar todos los accesos al sistema de información. Por tal motivo, debe prestarse mucha atención especialmente a los siguientes accesos: - equipo conectado al sistema de información que disponga también de un acceso público directo (por ejemplo, microordenador portátil conectado simultáneamente a un módem y a la red de la empresa); - conexión no autorizada de una estación de trabajo a un acceso físico de la red.
CAL-07: Asignación de privilegios de acceso a los servicios	La asignación de un acceso y de los privilegios asociados al mismo debe ser validada por él o los propietarios de los sistemas a los que se brinda acceso, a fin de que ellos verifiquen si dicha asignación ha sido establecida conforme a los permisos del usuario y si respeta los principios de responsabilidades (separación de poderes, menor privilegio). Es aconsejable llevar un inventario de los accesos y privilegios que han sido autorizados para los servicios delicados.
CAL-08: Protección de los accesos especiales (accesos de mantenimiento) al SI	Los accesos de mantenimiento son accesos que otorgan privilegios altos sobre los sistemas. Cuando se utilizan desde fuera del organismo (por ejemplo, por parte de proveedores de servicios), es fundamental definir medios de protección reforzados para evitar cualquier uso malicioso y establecer medios de trazabilidad. Deberán incluirse en los contratos de prestaciones de servicio (cf. contrato de servicios) compromisos de responsabilidades específicas.
CAL-09: Verificación de las listas de accesos al sistema de información	Para mantener el control de los accesos al sistema de información, es fundamental realizar periódicamente controles (incluyendo controles sorpresivos) de la lista de accesos y privilegios asociados. Este control puede realizarse en base a un cruce entre el inventario de los accesos, los compromisos archivados firmados por los usuarios y la lista de personal. Este tipo de controles puede reforzarse en caso de accesos a datos y/o funciones delicadas. Debe existir un procedimiento que prevea las acciones que hay que llevar a cabo en caso de detección de un incidente (por ejemplo, accesos que aparecen como injustificados, privilegios que parecen demasiado altos...). Estos procedimientos deberán contemplar los impactos que podría ocasionar, en el sistema de información, una reducción de los privilegios.
CAL-10: Control de los privilegios de los usuarios del sistema de información	Resulta importante especificar una norma de verificación del derecho de posesión de los privilegios, independientemente de los controles centrados en el uso seguro, que buscan verificar cómo se utilizan estos privilegios. Este control apuntará a limitar el uso de los privilegios que posee un usuario sobre un recurso del sistema de información, permitiendo solo las acciones que

se encuadran dentro de las normas de seguridad vigentes en el organismo.

Las medidas que se derivan de esta norma pueden basarse en los siguientes aspectos:

- las acciones para las cuales debe realizarse un control de los privilegios;

- las medidas que deben tomarse si se intenta una acción sin poseer el derecho adecuado;

- las autorizaciones para el control de los privilegios y sus condiciones de validez.

CAL-11: Aplicación de la noción de perfil de usuario del sistema de información

La aplicación de la noción de perfil de usuario del sistema de información requiere, como paso previo, la estructuración de los datos (u objetos) por funciones o actividades del organismo que son prerrogativas del responsable-poseedor. Los datos manipulados por los usuarios se estructuran en función de las aplicaciones que los usan dentro de una unidad funcional (por ejemplo, la gestión del stock para un departamento de aprovisionamiento), en el marco del uso de recursos compartidos (por ejemplo, las redes locales), o durante una misión o actividad particular que requiere el aislamiento de los puestos de trabajo.

Es necesario estructurar, del mismo modo, las diferentes categorías de personal (o sujetos) mediante la definición de perfiles de usuario del sistema de información que permitan especificar los privilegios de acceso a los datos en cuanto a la lectura (visualización, impresión) y los privilegios de procesos vinculados con la escritura (creación, modificación, destrucción) en el marco de sus responsabilidades o actividades.

También hay que definir y formalizar las normas de delegación.

CAL-12: Gestión de los privilegios de uso del sistema de información

Cada usuario poseerá los privilegios de uso para los recursos del sistema de información que correspondan al perfil que se le ha asignado. Es indispensable gestionar estos privilegios para verificar que las normas de seguridad vigentes se cumplan por completo.

Los criterios de aplicación de este principio deberán enunciarse claramente. Los mismos pueden inspirarse, por ejemplo, en los siguientes elementos:

- los perfiles de usuarios sujetos a la gestión de los privilegios;

- los privilegios existentes entre los diversos perfiles usuarios;

- las personas calificadas para otorgar o modificar esos privilegios;

- las condiciones que deben cumplirse antes de cualquier modificación u otorgamiento de privilegios;

- los privilegios de usuario incompatibles entre sí.

La protección de la integridad de los ficheros que contienen los privilegios requiere un control especial por parte del responsable del sistema y del agente de seguridad

CAL-13: Bloqueo de las sesiones de trabajo

Las estaciones de trabajo son los principales puntos de entrada del sistema de información. Debe concienciarse a los usuarios para que transformen en inaccesible su entorno de trabajo durante su ausencia (bloqueo de la sesión,

	apagado de la estación de trabajo). Para reforzar esta medida y evitar negligencias, se recomienda enfáticamente la implementación de medidas destinadas a proteger en forma automática una sesión de trabajo después de determinado período de inactividad (desconexión automática, bloqueo...).
CAL-14: Protección del entorno de trabajo	Debe establecerse y protegerse mediante derechos de acceso la lista de las acciones de cada perfil de usuario (gestión, participantes de mantenimiento, usuario principal del puesto de trabajo, usuario temporal).

3.3.14 JRN : Registro histórico

JRN-01: Medios de registro de las intrusiones o usos fraudulentos	El SI deberá incluir medios (dispositivos y/o procedimientos) de registro de las intrusiones o usos fraudulentos. Como no siempre será posible "bloquear" a tiempo intentos de intrusión, es conveniente, dentro de una lógica de gestión de los riesgos, implementar mecanismos de registro y rastreo (trazas) que permitan, en caso de intrusión exitosa, o de intento de intrusión, disponer de: - elementos de registro (trazas) que permitan la mejor identificación posible de las causas y orígenes de la intrusión (para remontarnos hasta los elementos peligrosos); - elementos de registro (trazas) suficientemente fiables como para que, de ser necesario, un juez pueda aceptarlos como pruebas de la intrusión (o intento la intrusión) o de uso fraudulento, en caso de presentación de alguna denuncia. Es conveniente, por lo tanto, implementar procedimientos de análisis de trazas y registros, con los medios técnicos y humanos necesarios, para detectar las intrusiones -aun después de ocurridas- y reunir los elementos de prueba necesarios. Estos elementos serán también indispensables para restablecer el estado inicial del sistema.
JRN-02: Registro de las operaciones	Para respetar el "principio de proporcionalidad" y la volumetría generada por el registro de trazas de seguridad, es fundamental definir las normas para la generación de trazas en función de los elementos buscados. Los recursos que permiten gestionar de manera útil estas trazas pueden influir en estas normas. La definición e implementación de estos sistemas de registro deberán contemplar las restricciones legales y reglamentarias referidas especialmente al tratamiento de los datos personales.
JRN-03: Constitución de pruebas	La conformación de elementos de prueba informáticos debe respetar la legislación y los códigos profesionales vigentes para poder presentarse, llegado el caso, ante un tribunal. Se trata, especialmente: - del cumplimiento del principio de proporcionalidad y transparencia; - de la admisibilidad de la prueba; - de la calidad y exhaustividad de la prueba; - del respeto de la vida privada; - de la calidad de elaboración de los elementos de prueba y de su

	almacenamiento hasta su presentación.
JRN-04: Gestión de las trazas	La gestión de las trazas de seguridad abarca varias tareas que hay que definir y organizar: - captura remota segura de las trazas de seguridad; - archivado de las trazas; - borrado de los ficheros de trazas obsoletas (deben establecerse la obsolescencia y el tiempo de archivado); - filtrado y análisis de las trazas; - protección de las trazas contra cualquier alteración o acceso no autorizado; - alerta en caso de detección de acontecimientos importantes; - control de la integridad de los mecanismos de rastreo (trazas); - procedimiento de análisis de las trazas, sabiendo que es necesario diferenciar entre quien analiza las trazas y el administrador de la red; - destrucción de las trazas una vez vencido el plazo legal.
JRN-05: Alerta de seguridad	Las normas que establecen las acciones que deben realizarse tras la detección de un incidente de seguridad dependen de la gravedad del incidente. De la clasificación puede depender: el método de transmisión de la alerta, los destinatarios, la velocidad y el tipo de reacción (cf. gestión de incidentes y gestión de crisis). Como norma general, cualquier de incidente de seguridad pertinente debe ser rastreado y debe poder ser analizado (identificación del autor, de la fecha, el tipo de operación, del objetivo...). Las normas para el registro y análisis de un incidente de seguridad dependen de la clasificación del incidente.
JRN-06: Análisis de los registros de datos de control de seguridad	La gestión segura del sistema de información implica el registro de los datos de control de seguridad en un registro de auditoría que permita verificar que la seguridad se ha respetado, en particular, en lo que respecta a los accesos al sistema de información, ya sea que se trate de accesos realizados por usuarios, técnicos o especialistas en informática. El análisis de los datos de control constituye una verificación a posteriori pero puede también revelar intentos infructuosos de penetración del sistema o, de manera más malintencionada, la preparación de un ataque mediante la recuperación de ficheros o cuentas que han caducado. Este examen aporta más información que la supervisión directa, siempre que se realice con regularidad y en forma minuciosa. La protección eficaz de los mecanismos que permiten el registro de los datos del control es una condición fundamental para justificar la confianza atribuida al análisis de los registros, dado que, efectivamente, todo intruso busca, en primer lugar, inhibir los mecanismos de registro y hacer desaparecer las pruebas del acto delictivo. La implementación de registros de auditorías puede constituir una restricción en períodos de gran demanda de servicio. Sin embargo, hay que ser conscientes del riesgo que representa, para la seguridad, su desactivación, y, especialmente,

	del riesgo jurídico que asume el organismo si sirve de pasarela para un ataque.

3.3.15 IGC : Infraestructuras de gestión de las claves criptográficas

IGC-01: Política de gestión de las claves	El uso de claves criptográficas en el marco de una infraestructura de gestión de las claves (IGC) requiere establecer, implementar, controlar y mantener una política de gestión de las claves. Dicha política toma generalmente la forma de una política de certificación (PC) y de una declaración de los procedimientos de certificación (DPC), que formalizan los requerimientos referidos a la gestión de las claves. Las mismas se refieren especialmente al ciclo de vida y al intercambio de las claves. Se recomienda que la estructura y el contenido de estos documentos respeten las normas internacionales (como, por ejemplo, la RFC 2527). Observamos también que la implementación de una PC se ve muy facilitado por la realización previa de un análisis de riesgos SSI y el estudio de otras PC centradas en el mismo tipo de necesidad (autenticación de servidor, autenticación de persona, firma, cifrado...).
IGC-02: Protección de las claves secretas o privadas	Ya sea debido al cifrado de confidencialidad, a la autenticación o la firma, los usuarios deben poder utilizar claves secretas o claves privadas. Garantizar la integridad y la no divulgación de dichas claves es, por definición, absolutamente fundamental para la solidez del sistema implementado. Deberá prestarse especial atención a este problema, a fin de garantizar que las opciones elegidas y los medios adoptados para cada caso sean coherentes con los objetivos planteados para el uso de estas claves. Se podrá, por lo tanto, exigir, para los documentos clasificados como "delicados", que cualquier cifrado se realice utilizando un dispositivo que garantice que la clave privada es almacenada y utilizada en un dispositivo material (como una tarjeta inteligente criptográfica), mientras que una solución lógica podría ser aceptable para otros usos.
IGC-03: Certificación de las claves públicas	En todo sistema de criptografía asimétrica existe un riesgo de usurpación de la clave pública. La seguridad del sistema se basa en la fiabilidad de la infraestructura de gestión de las claves y, especialmente, en el proceso de certificación que vincula a un elemento (persona, servidor) con una clave pública. Es fundamental controlar este aspecto redactando una política de certificación.

3.3.16 SCP : Emisiones electromagnéticas que podrían comprometer la seguridad del sistema

SCP-01: Zonificación	La zonificación es uno de los medios de protección contra las emisiones electromagnéticas que podrían comprometer la seguridad del sistema. Abarca dos partes: - la zonificación de los locales conforme a la directiva 495 del 19 de septiembre de 1997, - la zonificación de los equipos conforme a la guía 430 del 1º de junio de 1999. Considerando los resultados de la zonificación, los equipos deberán instalarse en conforme a la directiva 485 del 1º de septiembre de 2000.

SCP-02: Material TEMPEST

Unos de los medios para protegerse de las señales parásitas que podrían comprometer la seguridad del sistema es el uso de materiales TEMPEST (norma estándar sobre emisiones electromagnéticas transitorias).Estos materiales, que han sido sometidos a medidas especiales durante su desarrollo, para reducir, durante la emisión y transmisión, la emisión de señales parásitas que podrían comprometer la seguridad del sistema, se clasifican en cuatro categorías:

- A (conforme a la norma AMSG 720),
- B (conforme a la norma AMSG 788),
- C (conforme a la norma AMSG 784),
- D (no responde a ninguna de las normas anteriores).

Los materiales deberán instalarse conforme a la directiva 485 del 1º de septiembre de 2000.

Debe considerarse esta solución cuando la zonificación no permite dar una respuesta cabal a una necesidad.

SCP-03: Jaulas de Faraday

Unos de los medios, de los más onerosos, para protegerse de las señales parásitas que podrían comprometer la seguridad del sistema es el uso de jaulas de Faraday o aislamiento electromagnético de los locales.

SCP-04: Señales intencionales que podrían comprometer la seguridad del sistema

Los sistemas de transmisión inalámbricos, cuando se utilizan para transmitir información, se transforman en potenciales emisores de señales que podrían comprometer la seguridad del sistema. Se trata de "señales intencionales que podrían comprometer la seguridad del sistema" y que afectan a todos los sistemas de transmisión inalámbricos: infrarrojo, radiofrecuencia, óptico...

Para protegerse contra la emisión de este tipo de señales, es conveniente seguir las recomendaciones de la DCSSI y, en la mayoría de los casos, recurrir a un medio de cifrado y/o efectuar una zonificación de los equipos y locales.

Por otra parte, es conveniente tomar conciencia del riesgo asociado al uso de tales medios para la transmisión de información.

3.4 Otros requerimientos

3.4.1 CCS : Instrucción de seguridad

CCS_SIN: Instrucciones en caso de siniestro	
CCS_SIN.1.1	Las instrucciones de seguridad en caso de siniestro deben redactarse de manera clara y legible, respetando las normas y estándares en uso.
CCS_SIN.1.2	Las instrucciones de seguridad en caso de siniestro deben colocarse a la altura de la vista, en lugares despejados, respetando las normas y estándares en uso.
CCS_SIN.1.3	Las instrucciones de seguridad en caso de siniestro deben colocarse a la vista en diversos lugares del establecimiento y, especialmente, en los lugares de paso y lugares involucrados en las instrucciones (ascensor, instalación susceptible de provocar daños a causa del agua...)
CCS_SIN.1.4	Las instrucciones de seguridad en caso de siniestro deben imprimirse en un formato que llame la atención.
CCS_SIN.2.1	El procedimiento para llamar a los servicios de emergencia (bomberos, servicios médicos de urgencia, policía...) debe indicarse claramente en las instrucciones de seguridad en caso de siniestro.
CCS_SIN.2.2	El procedimiento de evacuación del establecimiento (vías de evacuación, lugar de encuentro...) debe indicarse claramente en las instrucciones de seguridad para siniestros que requieren evacuación (incendio, contaminación importante, atentado...).
CCS_SIN.2.3	Las instrucciones de seguridad deben indicar las acciones adecuadas que deben llevarse a cabo (qué hacer cuando uno es presa del humo, primeros auxilios a una persona electrocutada, medidas de emergencia en caso de daños ocasionados por el agua, protección del hardware en caso de siniestro...).
CCS_SIN.3.1	Las instrucciones de seguridad en caso de siniestro deben revisarse regularmente para garantizar que estén actualizadas (frecuencia que debe definirse pero que en ningún caso debe superar los 2 años).
CCS_SIN.3.2	El responsable de la revisión de las instrucciones de seguridad en caso de siniestro debe estar claramente identificado.
CCS_SIN.3.3	Las instrucciones de seguridad en caso de siniestro deben ser validadas regularmente por los servicios de emergencia en caso de siniestro (bomberos, servicios médicos de urgencia...).
CCS_SIN.3.4	Cualquier actualización de las instrucciones de seguridad en caso de siniestro debe ser notificada a la totalidad del personal del establecimiento.
CCS_SIN.3.5	Deben organizarse cursos de concienciación sobre las instrucciones de seguridad y, eventualmente, ejercicios prácticos (pruebas, ejercicios de evacuación, simulación de siniestro), en forma regular (frecuencia que debe definirse pero que en ningún caso debe superar los 2 años).
CCS_CSP: Instrucciones de seguridad preventivas	
CCS_CSP.1.1	Las instrucciones de seguridad preventivas (por ejemplo, la prohibición de fumar cerca de materiales inflamables) deben redactarse de manera clara y legible.
CCS_CSP.1.2	Las instrucciones de seguridad preventivas deben colocarse a la altura de la vista, en lugares despejados
CCS_CSP.1.3	Las instrucciones de seguridad preventivas deben colocarse a la vista en los lugares involucrados en dichas instrucciones
CCS_CSP.1.4	Las instrucciones de seguridad preventivas deben imprimirse en un formato que llame la atención.
CCS_CSP.2.1	Las instrucciones de seguridad preventivas deben revisarse regularmente para garantizar que estén actualizadas (frecuencia que debe definirse pero que en ningún caso debe superar los 2 años).
CCS_CSP.2.2	El responsable de la revisión de las instrucciones de seguridad preventivas debe

	estar claramente identificado.
CCS_CSP.2.3	Cualquier actualización de las instrucciones de seguridad preventivas debe ser notificada a la totalidad del personal del establecimiento.
CCS_CSP.2.4	Las personas ajenas al organismo deben ser informadas de las instrucciones de seguridad preventivas por su interlocutor.
CCS_SSE: Instrucciones de seguridad para los servicios esenciales	
CCS_SSE.1.1	Las instrucciones de seguridad para los servicios esenciales deben redactarse de manera clara y legible.
CCS_SSE.1.2	Las instrucciones de seguridad para los servicios esenciales deben incluir medidas preventivas para evitar la falta de disponibilidad de los servicios esenciales (por ejemplo, conexión de las estaciones de trabajo a la corriente alterna).
CCS_SSE.1.3	Las instrucciones de seguridad para los servicios esenciales deben incluir los procedimientos de alerta en caso de incidente (con quién hay que comunicarse en caso de corte de la línea de telecomunicaciones, por ejemplo).
CCS_SSE.1.4	Las instrucciones de seguridad para los servicios esenciales deben incluir las medidas de reacción en caso de incidente (por ejemplo, instalación del aire acondicionado de emergencia).
CCS_SSE.1.5	Las instrucciones de seguridad para los servicios esenciales deben revisarse regularmente para garantizar que estén actualizadas.
CCS_SSE.1.6	El responsable de la revisión de las instrucciones de seguridad para los servicios esenciales debe estar claramente identificado.
CCS_SSE.1.7	Cualquier actualización de las instrucciones de seguridad para los servicios esenciales debe ser notificada a la totalidad del personal del establecimiento.
CCS_CSG: Instrucciones de seguridad generales	
CCS_CSG.1.1	Instrucciones de seguridad para el buen uso del hardware y de los soportes de información deben elaborarse y notificarse a todos los usuarios potenciales.
CCS_CSG.1.2	Las instrucciones de seguridad para el buen uso deben indicar las prácticas que es conveniente evitar (prohibición de fumar, comer o beber cerca del hardware, concienciación sobre la saturación de los espacios de almacenamiento o de los recursos de tratamiento de la información...)
CCS_CSG.1.3	Las instrucciones de seguridad para el buen uso deben indicar las medidas preventivas que hay que implementar (protección durante el transporte, condiciones de almacenamiento...)
CCS_CSG.1.4	Las instrucciones de seguridad para el buen uso deben incorporar normas sobre el entorno operativo de las infraestructuras de procesamiento de la información (temperatura, higrometría...)
CCS_CSG.1.5	Las instrucciones de seguridad para el buen uso deben revisarse regularmente para garantizar que estén actualizadas.
CCS_CSG.1.6	El responsable de la revisión de las instrucciones de seguridad para el buen uso debe estar claramente identificado.
CCS_CSG.1.7	Cualquier actualización de las instrucciones de seguridad para el buen uso debe ser notificada a la totalidad del personal del establecimiento.
CCS_CHI: Guía informática	
CCS_CHI.1.1	Los usuarios del sistema de información (tanto internos como externos) deben comprometerse a respetar las instrucciones de uso, firmando una guía informática basada en las instrucciones de seguridad para el buen uso.
CCS_SRI: Parte del reglamento interno referida a la seguridad	
CCS_SRI.1.1	En el reglamento interno debe indicarse quiénes son los responsables de la seguridad del sistema de información.
CCS_RGI: Normas generales de instalación	
CCS_RGI.1.1	Deben establecerse, para la instalación del hardware, normas generales basadas en las recomendaciones de los fabricantes y en las necesidades de

	seguridad identificadas.

3.4.2 CRR : Riesgos residuales

CRR_ETU: Estudios de los riesgos residuales	
CRR_ETU.1.1	Un estudio de los riesgos debe llevarse a cabo y actualizarse regularmente, a fin de determinar los riesgos cubiertos, los riesgos por cubrir y los riesgos residuales.
CRR_ETU.1.2	Los riesgos residuales identificados deben evaluarse en términos de factibilidad/probabilidad así como en términos de impacto (financiero, profesional, organizacional, humano...).
CRR_ETU.2.1	Debe elaborarse un plan de acción para cada riesgo residual a fin de limitar lo más posible los impactos directos y evitar al máximo los impactos indirectos y los efectos secundarios en caso de materialización del riesgo.
CRR_ETU.2.2	Siempre que sea posible (existencia de contrato de seguro adecuado, primas de seguro controladas...), los riesgos residuales deben estar cubiertos por seguros adecuados.
CRR_SEN: Concienciación sobre los riesgos residuales	
CRR_SEN.1.1	Debe concienciarse al personal de la organización sobre los riesgos residuales y medidas tomadas para reducir su probabilidad/factibilidad y su impacto.
CRR_SEN.1.2	Debe brindarse formación al personal de la organización sobre los planes de acción en caso de materialización del riesgo residual.

3.4.3 CIS : Implantación de los establecimientos

CIS_PSI: Capítulo de la PSI referido a la seguridad física	
CIS_PSI.1.1	La política de seguridad debe incluir un capítulo referido a la seguridad física de los establecimientos.
CIS_PSI.1.2	El capítulo de la política de seguridad referido a la seguridad física de los establecimientos debe indicar las normas para la implantación de establecimientos.
CIS_PSI.1.3	Las normas para la implantación de establecimientos deben incluir medidas de protección y de reducción del impacto en caso de siniestro.
CIS_CSI: Instrucciones para la implantación de establecimientos	
CIS_CSI.1.1	Las normas para la implantación de establecimientos deben basarse en las normas y estándares nacionales y/o internacionales vigentes para la protección contra siniestros (incendio, accidente...).
CIS_CSI.1.2	Las normas para la implantación de establecimientos deben definir una nomenclatura de zonificación física que permita reducir los impactos de los siniestros (aislamiento de la zona mediante una puerta cortafuegos, por ejemplo).
CIS_CSI.1.3	La adecuación entre las normas para la implantación de establecimientos y las normas y estándares naciones y/o internaciones vigentes para la protección contra siniestros debe ser validada regularmente por los servicios de emergencia (bomberos, servicios médicos de urgencia...).
CIS_CSI.2.1	Debe auditarse regularmente la conformidad de los locales (y, en particular, los de establecimientos antiguos), para verificar si continúan respetando las normas y estándares vigentes para su implantación.
CIS_CSI.2.2	Los responsables de la evaluación de los establecimientos y sus suplentes deben estar claramente identificados.
CIS_CSI.2.3	Los responsables de la evaluación de los establecimientos y sus suplentes deben haber sido concienciados sobre la protección de los establecimientos y deben haber recibido formación en normas y estándares de implantación.
CIS_CSI.2.4	Las auditorías de conformidad de los establecimientos deben ser objeto de un informe detallado comunicado a la dirección.

CIS_CSI.2.5	Los informes de auditoría de conformidad de los establecimientos deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.
CIS_CDL: Construcción de los locales	
CIS_CDL.1.1	Durante la construcción y el acondicionamiento de los locales, deben contemplarse los riesgos inevitables más importantes (tormentas, huracanes, temblores.
CIS_ADL: Acondicionamiento de los locales	
CIS_ADL.1.1	En caso de encontrarse enfrentados a otros edificios, los vidrios de los locales deberán estar polarizados.
CIS_ADL.1.2	Debe evitarse que las ventanas que dan a la vía pública constituyan un fácil acceso a los locales (rejas, cristales reforzados, imposibilidad de abrir completamente la ventana, alarma cuando una ventana queda abierta fuera del horario de trabajo del establecimiento...).
CIS_ADL.2.1	El acondicionamiento de los locales debe contemplar los elementos que está previsto instalar allí (control de la temperatura, control de la higrometría, filtrado de polvo u otros elementos contaminantes...).
CIS_ADL.2.2	Los equipos deben instalarse lo más lejos posible de todo elemento que pudiera dañarlos (conductos de agua, fuente de emisiones electromagnéticas o fuente de calor...).
CIS_ADL.2.3	Los locales técnicos deben ser suficientemente espaciosos para permitir una organización clara de las instalaciones y no afectar la operatividad del hardware.
CIS_ADL.3.1	Las instalaciones estándares (cables de red, llave de corte de agua, fusibles...) deben estar identificadas para poder conocer su ubicación y función.
CIS_SSI: Selección del lugar de implantación	
CIS_SSI.1.1	La proximidad de servicios de emergencia debe ser uno de los criterios considerados para la elección del lugar de implantación de un establecimiento.
CIS_SSI.1.2	En la elección del lugar de implantación de un establecimiento deben considerarse los riesgos inherentes al sitio de implantación (zona anegadiza, proximidad de una implantación industrial de riesgo, contaminación...).
CIS_SSI.1.3	En la elección del lugar de implantación de un establecimiento deben considerarse las posibilidades de destrucción provocada por un hecho externo (choques, atentados...).
CIS_SSI.1.4	En la elección del lugar de implantación de un establecimiento deben considerarse los riesgos de atentados contra la disponibilidad del personal (lugar con escaso servicio de transporte público, accesos fáciles de bloquear..).
CIS_MPP: Medidas de protección	
CIS_MPP.1.1	Los sistemas de alimentación de los servicios esenciales deben contar con dispositivos de corte (entre los cuales debe incluirse un dispositivo de corte general) identificados y accesibles.
CIS_MPP.1.2	Los dispositivos de corte de los sistemas de alimentación de servicios esenciales así como cualquier otro elemento susceptible de provocar el corte en el suministro de los servicios esenciales deben estar protegidos contra accesos no autorizados.
CIS_MPP.1.3	Los elementos susceptibles de provocar un corte en el suministro de los servicios esenciales deben estar instalados, en la medida de lo posible, en el mismo establecimiento.
CIS_MPP.2.1	Los locales deben estar equipados con dispositivos de detección y lucha contra incendios.
CIS_MPP.2.2	Los dispositivos de detección y de lucha contra incendios deben adaptarse a los establecimientos y zonas de implantación y contar con dimensiones adecuadas.
CIS_MPP.3.1	Los establecimientos susceptibles de sufrir perjuicios importantes ocasionados por el agua deben estar equipados con dispositivos de evacuación de agua adecuados (sumidero, bomba...).

CIS_MPP.3.2	Las zonas particularmente sensibles a los perjuicios ocasionados por el agua (equipos eléctricos, archivos de papeles...) deben estar equipadas con detectores adecuados.
CIS_MPP.3.3	Los puntos de contacto con el exterior (techos, ventanas...) deben ser resistentes al agua y su estanqueidad debe verificarse regularmente.
CIS_MPP.3.4	Deben preverse dispositivos de protección específicos contra las inundaciones en los establecimientos situados en zonas anegadizas.
CIS_ZOS: Zonas de seguridad	
CIS_ZOS.1.1	Los organismos deben utilizar perímetros de seguridad para proteger las zonas que contienen equipos de producción o distribución de servicios esenciales.

3.4.4 CRI : Relaciones entre establecimientos

CRI_MOF: Control de las filiales	
CRI_MOF.1.1	Los establecimientos que pertenecen al organismo deben comprometerse a respetar las disposiciones de la política de seguridad.
CRI_MOF.2.1	Las modificaciones importantes en un establecimiento perteneciente al organismo deben ser objeto de un informe de implantación destinado al responsable de la seguridad del organismo (implantación inicial del establecimiento, modificación de la conexión de red...).

3.4.5 CET : Encuadramiento de terceros

CET_EGT: Encuadramiento general de terceros	
CET_EGT.1.1	Las personas ajenas al organismo no deben poder ingresar al establecimiento ni salir del mismo sin pasar por la recepción.
CET_EGT.1.10	Los acuses de recibo o de entrega de hardware o de soportes de información deben ser entregados en mano a la recepción por parte del interlocutor interno correspondiente, al momento de la salida del tercero involucrado.
CET_EGT.1.2	En la medida de lo posible, cada visita debe ser avisada y el personal de recepción debe tener la lista de nombres de todos los visitantes previstos cada día con la hora de llegada prevista y el interlocutor interno correspondiente.
CET_EGT.1.3	Cada visitante debe ser autenticado al momento de su llegada mediante una identificación oficial: se le debe entregar una identificación de visitante a cambio de su documento de identidad.
CET_EGT.1.4	Si la visita estaba prevista, el nombre de cada visitante debe validarse con la lista de visitantes previsto para ese día. Los nombres que no figuran en la lista deben agregarse.
CET_EGT.1.5	También debe consignarse la hora de entrada y de salida de cada visitante.
CET_EGT.1.6	El nombre, la hora de entrada, la hora de salida y el interlocutor interno de cada visitante deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.
CET_EGT.1.7	Hay que asignar un interlocutor interno a cada visitante no previsto y el visitante no debe ser autorizado a ingresar al establecimiento sin estar acompañado por su interlocutor interno.
CET_EGT.1.8	Si una persona ajena al organismo ingresa hardware o soportes de información a los locales, debe confeccionarse una lista precisa del material, que debe conservarse con el documento de identidad de dicha persona, y, en la medida de lo posible, el material debe ser marcado como material de terceros.
CET_EGT.1.9	Toda persona ajena a la organización que haya ingresado hardware o soportes de información debe salir de los locales con el mismo material o con un recibo firmado por el material de más o de menos que egresa.
CET_EGT.2.1	Se debe informar al interlocutor interno de un visitante tan pronto como éste último se presenta en la recepción
CET_EGT.2.2	El interlocutor interno de un visitante se hace cargo del visitante desde la

	recepción.
CET_EGT.2.3	A partir del momento que se hace cargo del visitante, el interlocutor interno es responsable del visitante, hasta su partida; y debe, en particular, asegurarse de que la visita se desarrolla conforme a los principios de seguridad enunciados en la política de seguridad.
CET_EGT.3.1	Los accesos a un establecimiento o a una zona con necesidades de seguridad específicas deben validarse mediante la autorización de los visitantes.
CET_EGT.3.2	Cuando se trate de un visitante ajeno al organismo, el responsable interno del visitante deberá contar con la autorización adecuada.
CET_EGT.3.3	Cuando se trate del acceso de un empleado del organismo, su autorización deberá verificarse en la recepción del establecimiento o de la zona correspondiente.
CET_EGT.3.4	La validación de las autorizaciones puede realizarse consultando manualmente la base de autorizaciones, una vez que se ha efectuado la autenticación mediante documento de identidad, o bien realizando una autenticación automática (por ejemplo, sobre la base de las identificaciones personales).
CET_EGT.3.5	Cuando la verificación de las autorizaciones se realice en forma automática, los datos de identificación así como la fecha y la hora de entrada deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.
CET_EIP: Encuadramiento de los participantes eventuales	
CET_EIP.1.1	Debe informarse a toda persona que trabaje en el sistema de información sobre las instrucciones de seguridad, antes de que comience a desarrollar sus tareas.
CET_EIP.1.2	El interlocutor interno de cualquier persona ajena a la organización que trabaje en el sistema de información es responsable –desde el punto de vista técnico, del cumplimiento de las instrucciones y de la política de seguridad, y, especialmente, en lo referido a protección de los datos– por todas las acciones que dicha persona realice durante el tiempo que duren dichas tareas.
CET_EIP.1.3	Toda tarea realizada en el sistema de información debe cerrarse con una validación de las tareas realizadas que permita controlar las operaciones efectuadas y los resultados obtenidos.
CET_EIP.1.4	Este informe de validación operativa debe especificar el nombre de la persona que ha trabajado en el sistema, la empresa a la que pertenece, el día y horario de realización de las tareas operativas, las tareas efectuadas, los resultados obtenidos, los eventuales problemas y el nombre del interlocutor interno.
CET_EIP.1.5	El informe de validación operativa debe estar firmado por la o las personas que trabajaron en el sistema, por el interlocutor interno y por el responsable de la recepción de las tareas realizadas, si éste difiere del interlocutor interno.
CET_EIP.1.6	Los informes de validaciones operativas deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información
CET_PLD: Encuadramiento de los servicios a largo plazo en el establecimiento	
CET_PLD.1.1	Una vez que se ha efectuado el procedimiento de recepción inicial, todo prestador que trabaje en el establecimiento debe poder ser tratado como personal temporal de la organización (tarjeta de acceso, derecho de acceso al sistema de información en función de las necesidades del servicio que prestará...).
CET_PLD.1.2	Todos los elementos provistos a un prestador que trabaje en el establecimiento en el marco de su misión (tarjeta de acceso, nombre de usuario y contraseña de conexión...) deben haber sido identificados y catalogados en una lista de elementos provistos al prestador, indicando la fecha en que le fueron entregados.
CET_PLD.1.3	La lista de los elementos provistos a un prestador que trabaje en el establecimiento debe conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.

CET_PLD.1.4	Al inicio de la prestación de servicios, debe entregarse a cada prestador que trabaje en el establecimiento una copia de las instrucciones de seguridad y de la política de seguridad.
CET_PLD.1.5	Antes de comenzar su trabajo, todo prestador que desempeñe tareas en el establecimiento debe comprometerse a respetar las instrucciones de seguridad y las disposiciones de la política de seguridad.
CET_PLD.1.6	Antes de iniciar la prestación de sus servicios, todo prestador que trabaje en el establecimiento debe firmar un compromiso formal de confidencialidad.
CET_PLD.2.1	Al finalizar la prestación de servicios, el prestador que ha trabajado en el establecimiento debe devolver todos los elementos físicos que se le han entregado durante su misión (por ejemplo, la tarjeta de acceso).
CET_PLD.2.2	La devolución de los elementos provistos a un prestador que ha trabajado en el establecimiento debe ser objeto de un acta de devolución fechada y firmada por el prestador y por un responsable de la organización.
CET_PLD.2.3	Al finalizar la prestación de servicios, todos los elementos lógicos (por ejemplo, la identificación y la contraseña de conexión) que se le han entregado a un prestador durante su misión deben ser desactivados o destruidos.
CET_PLD.2.4	La desactivación o destrucción de los elementos lógicos asignados a un prestatario durante su misión deben ser objeto de un acta de desactivación o de destrucción fechada y firmada por el responsable de dicha operación.
CET_PLD.2.5	Las actas de fin de prestación de servicios deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.

3.4.6 CAR : Gestión de la red

CAR_PAR: Protección de la gestión de la red	
CAR_PAR.1.1	Los programas de gestión de la red no deben ser susceptibles de denegaciones de servicio.
CAR_AAR: Atribución del administrador de la red	
CAR_AAR.1.1	La administración de las máquinas debe permitir detectar los consumos excesivos de recursos.

3.4.7 CGS : Gestión de la seguridad

CGS_GMP: Gestión de las contraseñas	
CGS_GMP.1.1	La política de contraseñas debe imponer un cambio periódico de las mismas.
CGS_GMP.1.2	La introducción de contraseñas debe resguardarse de miradas indiscretas.
CGS_GMP.1.3	Los usuarios deben ser concientes de las buenas prácticas en materia de seguridad sobre la elección y utilización de contraseñas.
CGS_SVG: Copias de seguridad	
CGS_SVG.1.1	La política de seguridad debe incluir una política referida a las copias de seguridad..
CGS_SVG.1.2	Todos los documentos electrónicos deben ser considerados dentro de la política referida a las copias de seguridad.
CGS_SVG.1.3	Es necesario identificar, en los procedimientos de respaldo específicos, los datos que deben ser respaldados.
CGS_SVG.1.4	Los procedimientos de respaldo deben indicar las modalidades de respaldo, los soportes que hay que utilizar, la frecuencia de realización de las copias de seguridad y los procedimientos de gestión de los soportes informáticos vírgenes y usados.
CGS_SVG.1.5	Los responsables de cada tarea de respaldo y sus suplentes deben estar claramente identificados.
CGS_SVG.1.6	os responsables de las copias de seguridad y sus suplentes deben recibir

	formación sobre operaciones de respaldo de información.
CGS_SVG.1.7	La política referida a las copias de seguridad debe revisarse regularmente para adaptarla a los cambios en el sistema de información, teniendo en cuenta la conservación de las copias de seguridad anteriores.
CGS_SVG.1.8	Los responsables de la revisión de los procedimientos de respaldo deben estar claramente identificados.
CGS_SVG.1.9	Cualquier modificación de un procedimiento de respaldo debe informarse a los responsables de las copias de seguridad involucrados así como a sus suplentes.
CGS_SVG.2.1	Las copias de seguridad deben gozar del mismo nivel de protección que los datos respaldados.
CGS_ARC: Archivado	
CGS_ARC.1.1	Todos los datos que deben archivarse tienen que generar una expresión de necesidades en términos de plazo de conservación y fiabilidad de los soportes de información.
CGS_ARC.1.2	Las medidas de conservación de los datos que deben archivarse deben establecerse conforme a las necesidades expresadas para el archivado de los datos involucrados.
CGS_ARC.1.3	Es necesario identificar, en los procedimientos de archivado específicos, los datos que deben ser archivados.
CGS_ARC.1.4	Los procedimientos de archivado deben indicar las modalidades de archivado, los soportes que hay que utilizar, la frecuencia de archivado y los procedimientos de gestión de los soportes de archivado vírgenes y usados.
CGS_ARC.1.5	Los responsables de cada tarea de archivado y sus suplentes deben estar claramente identificados.
CGS_ARC.1.6	Los responsables del archivado y sus suplentes deben recibir formación en operaciones de archivado.
CGS_ARC.1.7	Los procedimientos de archivado deben ser revisados regularmente para adaptarlos a los eventuales cambios de las necesidades de archivado de datos, teniendo en cuenta la conservación de los archivos anteriores.
CGS_ARC.1.8	Los responsables de la revisión de los procedimientos de archivado deben estar claramente identificados.
CGS_ARC.1.9	Cualquier modificación de un procedimiento de archivado debe informarse a los responsables de archivado involucrados así como a sus suplentes.
CGS_ARC.2.1	Los archivos deben gozar del mismo nivel de protección que los datos archivados.
CGS_PPS: Protección de las estaciones de trabajo	
CGS_PPS.1.1	Deben activarse las protecciones de la BIOS contra inicios con soportes extraíbles.
CGS_PPS.1.2	Los servicios, funciones e interfaces informáticas no utilizadas deben desactivarse.
CGS_PPS.1.3	Los servicios, funciones e interfaces utilizadas sólo esporádicamente deben desactivarse cuando no se utilizan.
CGS_PPS.2.1	Sólo el personal autorizado debe poder modificar el sistema o los programas instalados.
CGS_PPS.2.2	La configuración de los programas debe tener en cuenta el aspecto seguridad.
CGS_PPS.2.3	Los programas utilizados que no se empleen frecuentemente deben ser auditados.
CGS_PPS.2.4	Los programas utilizados deben estar exentos de fallas de seguridad conocidas.
CGS_PPS.2.5	La integridad de los códigos debe protegerse contra modificaciones no autorizadas.
CGS_PPS.3.1	El hardware debe protegerse contra robo (cable antirrobo, grabado...).
CGS_PPS.3.2	Los soportes extraíbles deben ser inventariados y protegidos contra robo y

	accesos no autorizados (almacenamiento en un armario cerrado del cual tienen llave sólo las personas autorizadas, restricción de acceso a los lugares donde se utilizan dichos soportes...).
CGS_GLI: Gestión de las licencias	
CGS_GLI.1.1	Debe implementarse un dispositivo operativo para la gestión de licencias.
CGS_GLI.1.2	Los números de las licencias deben guardarse por separado.
CGS_GLI.1.3	Los contratos de licencia deben conservarse en un lugar protegido contra incendios y otros siniestros susceptibles de inutilizarlos.
CGS_GLI.1.4	El acceso a las licencias debe restringirse a las personas autorizadas.
CGS_GLI.2.1	El acceso a las versiones instalables de los programas debe restringirse a las personas autorizadas.
CGS_OML: Garantía de origen del hardware y del software	
CGS_OML.1.1	Debe poder garantizarse el origen de las instalaciones, el hardware o el software, y de sus actualizaciones.
CGS_OML.1.2	Deben controlarse las eventuales certificaciones de las instalaciones, del hardware o del software, y de sus actualizaciones.
CGS_OML.1.3	Deben tomarse medidas tendientes a garantizar la autenticidad de los códigos.
CGS_GMA: Gestión del mantenimiento	
CGS_GMA.1.1	Debe realizarse regularmente el mantenimiento y control de las instalaciones, del hardware y del software del sistema de información, así como de aquellos que garantizan la protección del sistema de información y el aprovisionamiento de los servicios esenciales.
CGS_GMA.1.2	Las tareas de mantenimiento y pruebas funcionales de los elementos del sistema de información, de los elementos de seguridad y de los elementos que ofrecen servicios esenciales deben realizarse siguiendo las recomendaciones de los fabricantes y las normas y estándares vigentes.
CGS_GMA.2.1	Para poder realizar mantenimiento interno, es necesario que los responsables del mantenimiento y sus suplentes reciban formación en tareas de mantenimiento de las instalaciones, el hardware y/o el software que tienen a su cargo.
CGS_GMA.2.2	Para poder realizar mantenimiento interno, la documentación técnica de las instalaciones, del hardware y/o del software que debe repararse debe estar a disposición de los responsables de mantenimiento y ser accesibles para sus suplentes.
CGS_GMA.3.1	Para tareas de mantenimiento externo, debe designarse un responsable del seguimiento del mantenimiento para cada elemento (instalación, hardware, software...).
CGS_GMA.3.2	Para tareas de mantenimiento externo, el responsable del seguimiento del mantenimiento debe asegurarse de que las mismas se realizan de acuerdo con las frecuencias previstas en los contratos.
CGS_GMA.3.3	Para tareas de mantenimiento externo, el responsable del seguimiento del mantenimiento debe asegurarse de que hay un contrato de mantenimiento adecuado y permanentemente vigente para cada elemento que tiene a su cargo (renovación o firma de nuevos contratos).
CGS_GMA.4.1	Los medios de mantenimiento de los sistemas y del hardware deben gozar del mismo nivel de protección que los sistemas y hardware correspondientes.
CGS_GMA.5.1	El presupuesto asignado para el mantenimiento debe ser suficiente para garantizar un mantenimiento de calidad de todo el hardware y software del sistema de información.
CGS_GMA.6.1	Las tareas de mantenimiento que producen modificaciones en instalaciones, hardware y/o software deben siempre prever un procedimiento de vuelta atrás en caso de anomalía provocada por una modificación.
CGS_GSU: Gestión de la asistencia técnica	

CGS_GSU.1.1	Debe contarse con asistencia técnica disponible para las instalaciones, el hardware y el software del sistema de información, así como para aquellos elementos que garantizan la protección del sistema de información.
CGS_GSU.1.2	El procedimiento para que intervenga el equipo de asistencia técnica debe ser conocido por los usuarios del sistema de información, o al menos por los responsables de la gestión de los incidentes correspondientes.
CGS_GSU.1.3	Si hubiera empleados que debieran de utilizar el sistema de información del organismo fuera de los locales, la asistencia técnica deberá estar disponible también fuera del organismo y esta disponibilidad deberá abarcar incluso, cuando fuera necesario, países con los que se tiene una gran diferencia horaria.
CGS_GSU.2.1	Para tareas de asistencia técnica interna, es necesario que los responsables de la asistencia técnica y sus suplentes reciban una formación avanzada sobre las instalaciones, el hardware y/o el software que tienen a su cargo.
CGS_GSU.2.2	Para tareas de asistencia técnica interna, la documentación técnica de las instalaciones, del hardware y/o del software correspondientes debe estar a disposición de los responsables de la asistencia técnica y ser accesibles para sus suplentes.
CGS_GSU.2.3	Para el soporte técnico de elementos simples, el equipo de asistencia técnica debe aunar esfuerzos con el equipo correspondiente de gestión de los incidentes.
CGS_GSU.3.1	Para tareas de asistencia técnica externa, debe designarse un responsable del seguimiento de la asistencia técnica para cada elemento (instalación, hardware, software...) dentro de la estructura de gestión de los incidentes correspondiente.
CGS_GSU.3.2	Para tareas de asistencia técnica externa, el responsable del seguimiento del soporte técnico será responsable de la comunicación con el soporte técnico externo según las modalidades definidas en el contrato de asistencia técnica.
CGS_GSU.3.3	Para tareas de asistencia técnica externa, el responsable del seguimiento de la asistencia técnica debe asegurarse de que hay un contrato de asistencia técnica adecuado y constantemente vigente para cada elemento que tiene a su cargo (renovación o firma de nuevos contratos).
CGS_GDH: Gestión de los permisos	
CGS_GDH.1.1	Los usuarios deben contar con permisos para poder consultar y/o modificar los datos o los elementos del sistema de información en función de su necesidad de conocer o modificar dichos datos o elementos y no en función de su posición jerárquica.
CGS_GDH.1.2	Debe elaborarse un procedimiento de autorización de los usuarios para permitir la validación de la necesidad de cada usuario de conocer o modificar la información o los elementos del sistema de información, antes de autorizarlo.
CGS_GDH.1.3	El procedimiento de autorización debe ser lo más rápido y completo posible par no dificultar el acceso justificado a los datos, evitando así favorecer el préstamo de derechos de acceso.
CGS_GDH.1.4	Los diferentes tipos de permisos deben estar directamente vinculados con las necesidades de seguridad identificadas para las infraestructuras y datos correspondientes.
CGS_GDH.1.5	Los responsables de la asignación de permisos deben estar claramente identificados en función de los elementos para los cuales tienen la facultad de asignar permisos.
CGS_GDH.1.6	Los tipos de permisos y los permisos otorgados deben ser revisados regularmente para garantizar que se adapten a las necesidades del sistema de información.
CGS_GDH.1.7	La responsabilidad de revisión de los permisos no debe recaer en quienes tienen ya la responsabilidad de asignar los permisos.
CGS_GDH.1.8	La documentación referida a los permisos (identificación del usuario solicitante, permisos asignados...) debe ser fechada y archivada una vez que ha sido procesada.

CGS_GDH.1.9	La documentación referida a los permisos que se encuentra archivada debe ser tratada y protegida como información delicada.
CGS_GDH.2.1	Las atribuciones asociadas a cada permiso deben estar claramente definidas.
CGS_GDH.2.2	Al otorgar un permiso a un usuario, debe informársele sobre las atribuciones asociadas a dicho permiso.
CGS_PDI: Protección de las infraestructuras	
CGS_PDI.1.1	La política de seguridad debe enumerar los tipos de disposiciones a implementar para proteger las infraestructuras de procesamiento de la información.
CGS_CIR: Clasificación de la información y responsabilidades	
CGS_CIR.1.1	Los tipos de clasificación de la información utilizados para el organismo deben estar descritos en la política de seguridad.
CGS_CIR.1.2	Las disposiciones de seguridad asociadas a cada tipo de clasificación deben estar descritas en la política de seguridad.
CGS_CIR.1.3	La política de seguridad debe incluir una descripción de las responsabilidades en cuanto a la aplicación de las disposiciones de seguridad asociadas a cada tipo de clasificación en función del uso que se da a los datos.
CGS_PAI: Privilegio de acceso a la información	
CGS_PAI.1.1	Los responsables de la definición, implementación y control de acceso a la información deben estar claramente identificados.
CGS_PAI.1.2	Los controles de acceso a la información deben revisarse regularmente para verificar que se adecuan a las necesidades de seguridad.
CGS_PAI.1.3	Toda modificación de los controles de acceso a la información debe notificarse a todos los usuarios potenciales de los sistemas involucrados.
CGS_PAI.1.4	El procedimiento de gestión de los privilegios de acceso debe ser lo más rápido y completo posible para no obstaculizar el acceso a los datos, evitando así favorecer el préstamo de medios de acceso.
CGS_PAI.2.1	Todos los derechos asignables deben definirse en un reglamento específico.
CGS_PAI.2.2	El reglamento que define los derechos debe brindar una definición clara de los derechos utilizados, especialmente del derecho de conocer y del derecho de modificar datos o elementos del sistema de información.
CGS_PAI.2.3	El reglamento que define los derechos debe brindar instrucciones de uso de estos derechos en cuanto al control de acceso y en cuanto a los permisos.
CGS_REC: Recepción	
CGS_REC.1.1	La instalación y pruebas funcionales de los programas deben efectuarse en la totalidad de las plataformas sobre las cuales podrían llegar a instalarse.
CGS_GPC: Gestión de los procesos críticos	
CGS_GPC.1.1	En la medida de lo posible, los procesos críticos deben concentrarse en el organismo central.
CGS_GPC.1.2	Si un proceso crítico debiera ser ubicado fuera del organismo central, deberán implementarse medidas de control de dicho proceso por parte del organismo central (informe de actividad, administración a distancia...).
CGS_GPC.2.1	Los procesos críticos no deberán poder ser ejecutados por una sola persona.
CGS_GPC.2.2	Los resultados de los procesos críticos deberán ser validados antes de su utilización.
CGS_GPC.2.3	La validación de los procesos críticos deberá ser realizada al menos por dos responsables del organismo.
CGS_GPC.2.4	Los responsables de la validación de los procesos críticos y sus suplentes deben estar claramente identificados.
CGS_PEP: Protección de los espacios compartidos	
CGS_PEP.1.1	Los espacios reservados para compartir o intercambiar información deben estar protegidos contra accesos no autorizados (permiso, derecho de acceso, autenticación...) del mismo modo que el resto de los espacios del sistema de

	información.
CGS_OES: Organización y seguridad	
CGS_OES.1.1	La organización implementada en el organismo y entre el organismo y sus asociados debe favorecer la identificación individual de los usuarios.
CGS_OES.1.2	Los eventuales cambios en la organización luego de un cambio de política o estrategia de organización no deben reducir el perímetro de los riesgos cubiertos.
CGS_OES.1.3	Los períodos de transición durante un cambio en la organización deben planificarse y no deben permitir recuperar derechos de acceso y atribuciones.
CGS_HSI: Protección de seguridad fuera de los sistemas de información	
CGS_HSI.1.1	Los equipos de seguridad que no forman parte del sistema de información (detector de humo, mecanismo de detección de daños provocados por el agua, pararrayos...) deben protegerse del mismo modo que los equipos del sistema de información.
CGS_HSI.1.2	Debe concienciarse al personal de la organización sobre la protección de los equipos de seguridad que no forman parte del sistema de información.
CGS_GSS: Gestión de los sistemas de emergencia	
CGS_GSS.1.1	Los mecanismos de emergencia deben consistir, al menos, en equipos redundantes suficientemente dimensionados para garantizar de manera satisfactoria los servicios identificados como estratégicos.
CGS_GSS.1.2	El dimensionamiento de los equipos redundantes de emergencia debe revisarse regularmente y tras cada modificación importante del sistema de información, para garantizar que aún es adecuado.
CGS_GSS.1.3	Todos los equipos de emergencia (redundantes o no) deben dimensionarse para ofrecer una calidad de servicio que se corresponda con los objetivos identificados para las soluciones de funcionalidad reducida para emergencias.
CGS_GSS.1.4	En la medida de lo posible, los equipos de emergencia no deben utilizarse en régimen nominal; si así fuera, su dimensionamiento debe considerar el previsible aumento de las necesidades de recursos en caso de incidente.
CGS_GSS.2.1	La activación de los equipos redundantes de emergencia debe ser, dentro de lo posible, automática.
CGS_GSS.2.2	Si los equipos de emergencia no se activan automáticamente, el tratamiento de un incidente que provoca un corte de servicio debe comenzar por la activación urgente del equipo de emergencia adecuado.
CGS_GMR: Gestión de los desechos	
CGS_GMR.1.1	Los soportes de información que contengan datos internos del organismo deberán eliminarse de tal modo que sean inaccesibles para el público.
CGS_GMR.1.2	Los soportes de información que contengan datos confidenciales deberán eliminarse de tal modo que sean inaccesibles para toda persona no autorizada.
CGS_GDA: Gestión de las autenticaciones	
CGS_GDA.1.1	La autenticación debe ser obligatoria a partir de cierto nivel de seguridad, ya sea para consulta o modificación.
CGS_GDA.1.2	Cuando sea aplicable, la autenticación debe desembocar en la consulta de los privilegios de la persona o de la aplicación autenticada.
CGS_GDA.1.3	Los accesos a los sistemas deben ser incluidos en el registro, indicando, de ser posible, como mínimo, la identidad del usuario, el sistema involucrado y la fecha y la hora de acceso.
CGS_GDA.1.4	Las operaciones realizadas utilizando los dispositivos de acceso deben ser rastreadas e incluidas en el registro del mismo modo que los accesos a los sistemas.
CGS_GDA.2.1	La autenticación de una persona debe basarse, obligatoriamente, en un dato que ésta conozca (contraseña, código PIN...) y, eventualmente, en un objeto que posea (identificación, tarjeta inteligente...) o en una característica física

	(biometría), o incluso en ambas opciones.
CGS_GDA.3.1	La autenticación de una aplicación debe basarse en un sistema que garantice que no haya usurpación de aplicación (certificado de firma electrónica, por ejemplo).
CGS_GDA.3.2	Algunas funciones delicadas (definir) deben autenticarse en forma automática.
CGS_CSR: Configuración de los servicios de la red	
CGS_CSR.1.1	Todos los servicios de las redes deben estar configurados de tal modo que no puedan ser utilizados para funcionalidades que difieran de las previstas.
CGS_CSR.1.2	Las conexiones deben filtrarse de tal modo que no se permita tráfico no previsto (aprovechamiento de funcionamiento asíncrono, acceso a puertos no autorizados, spam...).
CGS_CSR.1.3	El dispositivo de acceso debe permitir minimizar las posibilidades de acciones ilegales o fraudulentas.
CGS_CME: Configuración del correo electrónico	
CGS_CME.1.1	La configuración del correo electrónico debe permitir controlar los flujos de datos generados (reducción de los envíos automáticos, listas de correo accesibles para todos...).
CGS_SUP: Supervisión	
CGS_SUP.1.1	La supervisión de los sistemas debe ser lo más simple y ergonómica posible (claridad de los datos, herramienta adaptada y única que permita una supervisión central...).
CGS_GDT: Gestión de las trazas	
CGS_GDT.1.1	Los trazas deben gozar, como mínimo, del mismo nivel de protección que las operaciones a las que se refieren y, eventualmente, de un nivel más elevado, si contienen datos personales.

3.4.8 CDO : Documentación

CDO_APP: Documentación sobre las aplicaciones	
CDO_APP.1.1	Los manuales de mantenimiento, de gestión y de uso de las aplicaciones, así como la eventual documentación interna complementaria sobre el tema, deben ser accesibles para los actores involucrados.
CDO_APP.1.2	Los procedimientos de mantenimiento, de gestión y de uso de las aplicaciones deben ser accesibles para los actores involucrados.
CDO_APP.1.3	La documentación interna debe actualizarse con regularidad.
CDO_SDC: Seguimiento de las configuraciones	
CDO_SDC.1.1	Debe elaborarse un inventario actualizado de los sistemas y de su configuración, actualizándolo al momento de cada modificación de los sistemas o configuraciones y difundiéndolo a los actores que precisen conocerlo (encargado de su mantenimiento, desarrollador, asistencia técnica interna...).
CDO_SDC.1.2	Cualquier modificación de las configuraciones del hardware o software debe contemplar la compatibilidad con el resto del sistema de información y con las anteriores copias de seguridad o archivos y prever un procedimiento de vuelta atrás en caso de anomalía.

3.4.9 CGI : Gestión de los incidentes

CGI_GDC: Gestión de crisis	
CGI_GDC.1.1	Deben identificarse las potenciales situaciones de crisis.
CGI_GDC.1.2	Deben definirse niveles de alerta de crisis para cada crisis potencial identificada, de tal modo que permita saber cuándo un organismo o un establecimiento entra en una situación de crisis.
CGI_GDC.1.3	Debe elaborarse una métrica específica que permita detectar si se han superado los límites de alerta.

CGI_GDC.1.4	Deben implementarse informes de alerta automáticos que permitan poner en marcha el procedimiento de gestión de crisis en cuanto se alcance un límite de alerta.
CGI_GDC.2.1	El procedimiento de gestión de crisis debe ponerse en marcha de forma automática apenas se alcance un nivel de alerta.
CGI_GDC.2.2	El procedimiento de gestión de crisis puede ser puesto en marcha en forma manual por el último escalón de la lista de escalamiento de gestión de incidente aunque no se haya alcanzado el nivel de alerta.
CGI_GDC.2.3	Si el último escalón de la lista de escalamiento estuviera ausente, la responsabilidad de poner en marcha en forma manual el procedimiento de gestión de crisis deberá transferirse a una persona presente (suplente del último escalón de la lista de escalamiento o persona específicamente designada a tal fin).
CGI_GDC.2.4	La cadena de transferencia de la responsabilidad de puesta en marcha manual del procedimiento de gestión de crisis debe identificarse claramente, de tal forma que siempre haya un responsable, incluso en caso de falta de disponibilidad de varias personas.
CGI_GDC.2.5	Debe concienciarse y formarse en la puesta en marcha manual del procedimiento de gestión de crisis a las personas susceptibles de ponerlo en marcha manualmente.
CGI_GDC.2.6	La puesta en marcha del procedimiento de gestión de crisis debe consistir, como mínimo, en una comunicación rápida del miembro responsable de la célula de crisis involucrada en la situación.
CGI_GDC.3.1	Deben conformarse diversas células de crisis para cada tipo de crisis potencial (accidente físico, ataque a la red, procedimiento legal...).
CGI_GDC.3.2	Una célula de crisis debe estar integrada, como mínimo, por un especialista del área y un responsable de la toma de decisiones de nivel jerárquico suficientemente alto como para tomar decisiones que involucren a todo el organismo.
CGI_GDC.3.3	Debe identificarse claramente a un responsable y sus suplentes por cada célula de crisis.
CGI_GDC.3.4	El responsable de una célula de crisis debe convocar inmediatamente a una reunión de la célula en cuanto se haya puesto en marcha el procedimiento de gestión de crisis y haya sido informado de la crisis.
CGI_GDC.3.5	Debe preverse una cantidad suficiente de suplentes para cada miembro de una célula de crisis.
CGI_GDC.3.6	Debe concienciarse y formarse a los miembros titulares y suplentes de una célula de crisis en la gestión de las crisis del área correspondiente.
CGI_GDC.4.1	Una célula de crisis debe contar con toda la información necesaria para el control o la resolución de una crisis
CGI_GDC.4.2	Una célula de crisis debe poder tomar todas las decisiones necesarias para el control o la resolución de una crisis.
CGI_GDC.4.3	Las decisiones tomadas por una célula de crisis deben ser implementadas con la mayor brevedad.
CGI_GDC.4.4	Toda decisión tomada por una célula de crisis debe ser consignada por escrito y fechada, adjuntándole todos los datos que permitieron tomar tal decisión.
CGI_GDC.4.5	La responsabilidad de consignar las decisiones de una célula de crisis no debe recaer sobre el responsable de la célula de crisis, sino que debe ser asignada a otra persona.
CGI_GDC.4.6	Las decisiones tomadas por una célula de crisis deben conservarse, utilizarse y gestionarse igual que el resto de las trazas de seguridad del sistema de información.
CGI_LCI: Lucha contra incendios	
CGI_LCI.1.1	Debe implementarse una estructura de lucha contra incendios.

CGI_LCI.1.2	La estructura de lucha contra incendios debe establecerse conforme a las normas y estándares vigentes.
CGI_LCI.1.3	La estructura de lucha contra incendios debe identificar perfiles de lucha contra incendios.
CGI_LCI.1.4	La función y las responsabilidades de cada perfil establecido para la lucha contra incendios deben estar claramente definidas, especialmente, en lo que respecta a la responsabilidad de la evacuación.
CGI_LCI.1.5	Los perfiles deben asignarse a personas identificadas dentro del organismo.
CGI_LCI.1.6	Debe preverse una cantidad suficiente de suplentes para cada perfil de lucha contra incendios.
CGI_LCI.1.7	Debe concienciarse y formarse a los titulares y los suplentes para los perfiles de lucha contra incendios sobre sus funciones y responsabilidades.
CGI_GIS: Gestión de los incidentes de seguridad	
CGI_GIS.1.1	Los equipos de gestión de incidentes deben ser capaces de resolver la mayor parte de los incidentes comunes en su área.
CGI_GIS.1.2	Los equipos de gestión de incidentes deben tener la posibilidad de comunicarse con niveles superiores de la lista de escalamiento en cuanto ocurriera algún incidente que dichos equipos no pudieran resolver.
CGI_GIS.1.3	Los equipos de gestión de incidentes deben efectuar siempre el seguimiento de los incidentes (tipo de incidente, fecha, interlocutor, seguimiento de las acciones, fecha de cierre), aun cuando se tratara de incidentes que ellas mismas no hubieran resuelto).
CGI_GIS.1.4	Debe realizarse un seguimiento regular de los incidentes para verificar que siguen buscándose soluciones.
CGI_GIS.1.5	Todos los incidentes resueltos deben ser archivados con una descripción de los síntomas del incidente, de su causa y del método de resolución.
CGI_GIS.1.6	El procedimiento de tratamiento de los incidentes de seguridad debe revisarse regularmente para garantizar que se adecue al sistema de información y a la organización.
CGI_GIS.1.7	El responsable de la revisión del procedimiento de tratamiento de los incidentes debe estar claramente identificado.
CGI_GIS.1.8	Toda modificación del procedimiento de gestión de los incidentes debe ser notificada a todos los usuarios del sistema de información.
CGI_GIS.2.1	El equipo de gestión de los incidentes de seguridad vinculados con el robo debe ocuparse de los trámites de denuncia de robo ante las autoridades policiales.
CGI_GIS.2.2	El equipo de gestión de los incidentes de seguridad vinculados con el robo debe imputar el robo en el inventario de los bienes de la organización.
CGI_GIS.2.3	El equipo de gestión de los incidentes de seguridad vinculados con el robo debe ocuparse de los trámites de anulación de los eventuales elementos de autenticación presentes en el material robado.
CGI_GIS.2.4	El equipo de gestión de los incidentes de seguridad vinculados con el robo debe ocuparse de los eventuales trámites administrativos o judiciales necesarios.
CGI_GIS.2.5	Todos los incidentes de seguridad vinculados con el robo deben ser archivados con la fecha, hora y lugar, además de la descripción de las circunstancias del robo.
CGI_GIS.3.1	Los incidentes archivados deben ser analizados para evaluar si es posible mejorar la cobertura de la vulnerabilidad aprovechada al momento del incidente y, eventualmente, para prever incidentes posteriores (avería o saturación, por ejemplo)
CGI_GIS.3.2	Los incidentes archivados deben ser utilizados dentro de una base de conocimientos para acelerar y simplificar la resolución de incidentes posteriores del mismo tipo.
CGI_GIS.3.3	Los incidentes archivados deben ser sintetizados y comunicados, con los resultados del análisis, a los responsables de la toma de decisiones identificados

	para que sean contemplados en la estrategia de seguridad del organismo.
CGI_GIS.3.4	Los responsables de la toma de decisiones que se ocupan del análisis de la síntesis de los incidentes y sus suplentes deben estar claramente identificados.
CGI_GIS.3.5	Deben concienciarse y formarse en este tipo de análisis a los responsables de la toma de decisiones que se ocupan del análisis de la síntesis de los incidentes y sus suplentes.
CGI_GIS.3.6	Los responsables de la toma de decisiones que se ocupan del análisis de la síntesis de los incidentes o, llegado el caso, sus suplentes deben tener la posibilidad de tomar decisiones que permitan paliar los cambios previsibles.

3.4.10 CEI : Estudios preliminares y diseño del SI

CEI_ABS: Análisis de las necesidades de seguridad	
CEI_ABS.1.1	La protección de las partes no unificadas del sistema de información debe realizarse en función de las necesidades de seguridad de los componentes funcionales afectados.
CEI_ABS.1.2	Cada componente funcional debe ser estudiado a fin de determinar sus necesidades de seguridad, especialmente en términos de confidencialidad, disponibilidad, integridad y control/prueba.
CEI_ABS.1.3	Toda necesidad específica no cubierta por las disposiciones de seguridad generales del sistema de información debe, en lo posible, ser cubierta mediante disposiciones específicas del elemento funcional (diseño técnico, procedimientos de seguridad...).
CEI_ABS.1.4	Toda necesidad específica que no pueda ser cubierta de manera satisfactoria debe someterse a un estudio de riesgos residuales (ver CRR_ETU).
CEI_ABS.1.5	El estudio inicial debe permitir evaluar los recursos necesarios y obtener un primer dimensionamiento del sistema (en horas de mayor demanda e incluyendo emergencias) y de los equipos (incluidos los de emergencia), así como de los recursos necesarios para su desarrollo.
CEI_ABS.1.6	Las necesidades de seguridad identificadas deben contemplar los desafíos y el contexto del entorno local (económico, social, político, legislativo...).
CEI_ABS.1.7	Las necesidades de seguridad identificadas deben contemplar los potenciales impactos de un incidente.
CEI_CDT: Elección de las tecnologías	
CEI_CDT.1.1	La posibilidad de actualización permanente debe ser un factor importante en la elección de las tecnologías para el sistema de información (hardware, aplicaciones, lenguajes de desarrollo...).
CEI_CDT.1.2	Las tecnologías anticuadas del sistema de información deben ser reemplazadas lo más rápidamente posible por tecnologías actualizadas.
CEI_CDT.2.1	La ergonomía de uso y de gestión debe tomarse en cuenta para la elección del software, del hardware y de las instalaciones.
CEI_CDT.2.2	Las normas y estándares sanitarios deben tomarse en cuenta para la elección del software, del hardware y de las instalaciones.
CEI_ERS: Estudio de los riesgos específicos vinculados con el hardware y el software utilizados	
CEI_ERS.1.1	Los riesgos eventuales específicos de los elementos albergados en el organismo (material explosivo, productos inflamables, fuentes de emisiones electromagnéticas o fuentes de calor...) deben ser estudiados y contemplados para la implantación de los establecimientos.

3.4.11 CPS : Políticas de seguridad

CPS_PPT: Política de protección de las estaciones de trabajo	
CPS_PPT.1.1	La política de seguridad debe incluir una política de protección de las estaciones de trabajo fijas o móviles (integridad, control de acceso, lucha contra los códigos

	malignos...).
CPS_PPT.1.2	La política de protección de las estaciones de trabajo debe adecuarse a las necesidades de seguridad del organismo.
CPS_PPT.1.3	La política de protección de las estaciones de trabajo debe revisarse regularmente para validar su adecuación a las necesidades de seguridad del organismo.
CPS_PPT.1.4	El responsable de la revisión de la política de protección de las estaciones de trabajo debe estar claramente identificado.
CPS_PPT.1.5	Toda modificación de la política de protección de las estaciones de trabajo debe notificarse a todos los usuarios potenciales de los sistemas involucrados.
CPS_PAQ: Política de aseguramiento de la calidad	
CPS_PAQ.1.1	Las operaciones realizadas en el sistema de información deben estar cubiertas por el plan de aseguramiento de la calidad del organismo.
CPS_PAQ.1.2	Las disposiciones del plan de aseguramiento de la calidad del organismo deben estar consignadas en el manual de aseguramiento de la calidad.
CPS_PAQ.1.3	Todos los empleados del organismo deben tener acceso al manual de aseguramiento de la calidad.
CPS_PAQ.1.4	El manual de aseguramiento de la calidad debe revisarse regularmente para verificar su adecuación a los objetivos de calidad del organismo.
CPS_PAQ.1.5	El responsable de la revisión del manual de aseguramiento de la calidad debe estar claramente identificado.
CPS_PAQ.1.6	Toda modificación del manual de aseguramiento de la calidad debe notificarse a todos los empleados del organismo.
CPS_PAQ.2.1	El manual de aseguramiento de la calidad debe tratar los aspectos de aseguramiento de la calidad del oficio del organismo.
CPS_PAQ.2.2	Debe concienciarse a todos los empleados del organismo sobre las disposiciones referidas a la calidad profesional, para lograr que adhieran al procedimiento de calidad.
CPS_PAQ.3.1	En la medida de lo posible, los procesos manuales deben estar validados por un responsable antes de ser utilizados.
CPS_DEV: Política de seguridad para los desarrollos	
CPS_DEV.1.1	El desarrollo de aplicaciones para el sistema de información debe ser controlado y enmarcado por reglas de desarrollo.
CPS_DEV.1.2	Las reglas de desarrollo deben apoyarse en normas y estándares de desarrollo nacionales e internacionales.

3.4.12 CPD : Protección de los datos

CPD_DGL: Datos de ubicación geográfica	
CPD_DGL.1.1	Los datos que pueden utilizarse para ubicar a una persona o localizar un hardware deben ser considerados como datos delicados y, como tales, debe protegerse su confidencialidad.
CPD_DGL.1.2	Debe concienciarse al personal de la organización sobre la protección de los datos que pueden utilizarse para ubicar a una persona o localizar un hardware.
CPD_INP: Identificación de los niveles de protección	
CPD_INP.1.1	El nivel de protección de un sistema debe estar identificado físicamente en el sistema, así como en la documentación correspondiente.

3.4.13 CFO : Formación

CFO_SPS: Concienciación sobre los problemas de seguridad	
CFO_SPS.1.1	Debe concienciarse a todos los usuarios del sistema de información sobre los riesgos que pesan sobre el sistema de información, los métodos de ataque, los

	problemas de seguridad potenciales y las medidas para cubrir dichos riesgos o limitar sus impactos.
CFO_SPS.1.2	Debe concienciarse a todo el personal sobre las conductas inofensivas susceptibles de deteriorar la calidad de servicio del sistema de información (reenvió de mensajes en cadena, por ejemplo)
CFO_FRS: Formación de suplentes o sucesores	
CFO_FRS.1.1	Debe identificarse una cantidad adecuada de suplentes para las funciones importantes de la organización para el caso eventual de que sus titulares no estuvieran disponibles.
CFO_FRS.1.2	Los suplentes designados para hacerse cargo de las funciones eventualmente vacantes deben recibir formación en las tareas vinculadas con dichas funciones.
CFO_FRS.1.3	Los suplentes designados para hacerse cargo de las funciones eventualmente vacantes deben recibir información sobre las responsabilidades vinculadas con dichas funciones.
CFO_FRS.1.4	En función de las funciones que requieran de un suplente, éste podría ser relevado de algunas o todas sus funciones habituales.
CFO_FRS.1.5	Durante el reemplazo, el suplente debe gozar de todos los privilegios, derechos, atribuciones y responsabilidades de la persona reemplazada.
CFO_FRS.2.1	En la medida de lo posible, debe preverse y prepararse, con la mayor anticipación posible, toda ausencia del titular de una función.
CFO_FRS.2.2	Si, tras la partida de un titular, el dimensionamiento de un equipo ya no se adecua a las funciones que tiene a su cargo, deberá designarse un sucesor para el titular que se ha ido.
CFO_FRS.2.3	Debe preverse un período de transición suficientemente largo durante el cual el titular que se va del organismo y su sucesor cumplen las mismas funciones.
CFO_FRS.2.4	Antes de partir, el titular que deja la organización debe brindar formación a su sucesor y presentarlo a sus interlocutores habituales.

3.4.14 CCC : Cláusulas contractuales

CCC_CLR: Cláusulas contractuales que limitan las responsabilidades de ambas partes	
CCC_CLR.1.1	Las responsabilidades, sanciones y multas atribuidas a cada parte firmante de un contrato deben adaptarse al contexto y guardar relación con los impactos potenciales (deben evitarse las multas y sanciones desmesuradas)
CCC_CLR.1.2	Las responsabilidades de cada parte firmante de un contrato deben limitarse, indicando claramente su nivel máximo.
CCC_RGF: Reversibilidad y garantías financieras	
CCC_RGF.1.1	Deben implementarse medidas para la evaluación de la continuidad financiera y/o técnica al momento de la elección de un subcontratista o prestador.
CCC_RGF.1.2	Los contratos de subcontratación y los contratos de prestación de servicios a largo plazo deben incluir una cláusula de rescisión.

3.4.15 CRH : Recursos humanos

CRH_DDE: Dimensionamiento de los equipos	
CRH_DDE.1.1	Los equipos deben estar dimensionados para poder cumplir sus funciones de manera satisfactoria.
CRH_DDE.1.2	Los equipos deben estar dimensionados para poder cumplir con sus funciones esenciales aun si parte de sus miembros no están disponibles.
CRH_PDP: Protección del personal	
CRH_PDP.1.1	Si el entorno general es difícil, la organización debe implementar medidas de protección del personal (servicio de seguridad, alojamiento cerca del establecimiento...).
CRH_PDP.1.2	Si el entorno general es difícil, la organización debe implementar medidas de

	protección del personal (servicio de seguridad, alojamiento cerca del establecimiento.
CRH_PDP.1.3	El organismo debe prever la implementación de soluciones de emergencia en caso de dificultad de acceso al establecimiento (ómnibus para transporte del personal en caso de huelgas del transporte público, alquiler de quitanieves para las entradas del establecimiento...).
CRH_CDT: Condiciones de trabajo	
CRH_CDT.1.1	El acondicionamiento de los locales debe ser lo más favorable posible para el trabajo requerido (iluminación suficiente, temperatura adecuada, aislamiento sonoro, espacios donde ubicar los elementos de trabajo...).
CRH_CDT.1.2	Deben tomarse disposiciones específicas para reducir las perturbaciones en el lugar de trabajo (no realizar reuniones en los espacios abiertos, ubicar la máquina de café lejos de las áreas de trabajo...).
CRH_QDP: Cualificación del personal	
CRH_QDP.1.1	Las misiones asignadas a cada empleado deben corresponder a su nivel de cualificación.

3.4.16 CDS : Dimensionamiento de los sistemas

CDS_DES: Dimensionamiento de los servicios esenciales	
CDS_DES.1.1	Los servicios esenciales y de emergencia deben estar dimensionados de tal modo que ofrezcan servicios adecuados y de calidad, incluso durante eventuales períodos de mayor demanda.
CDS_DES.1.2	El dimensionamiento de los servicios esenciales debe revisarse regularmente y tras cada modificación importante del sistema de información o de los establecimientos, para garantizar que aún es adecuado y de calidad, incluso durante eventuales períodos de mayor demanda.

4 Propuesta de cobertura de las vulnerabilidades mediante objetivos de seguridad genéricos

Los objetivos de seguridad (cuyos códigos corresponden a los de las partes anteriores) se presentan por método de ataque y vulnerabilidad.
Los siguientes cuadros permiten determinar con facilidad los objetivos de seguridad genéricos que permitirían cubrir cada vulnerabilidad genérica. Sirven, por lo tanto, para el tratamiento de las vulnerabilidades, pero deberán ser completados con objetivos que cubran los orígenes y consecuencias de los riesgos, a fin de tratar estos riesgos en forma completa.

4.1.1 INCENDIO

Vulnerabilidad	Cobertura
Ejemplar único de las licencias	LOG_07
Aplicaciones únicas desarrolladas internamente	MAT_02
Falta de hardware de repuesto	MAT_01
Hardware que utiliza materiales inflamables (por ej.: impresoras de gran capacidad que ocasionan polvo)	PHY_09
Falta de respaldo de los datos contenidos en los soportes	ORG_08
Soportes originales	MAT_02 ORG_08
Falta de cobertura de seguridad en caso de siniestro grave	ORG_44
No asistencia al establecimiento de los servicios de emergencia (bomberos)	ORG_22 ORG_25
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales para el restablecimiento de las actividades, aplicables en caso de crisis declarada en el establecimiento del proveedor	ORG_38
Ausencia de instrucciones de seguridad para el personal externo que trabaja dentro del organismo	ORG_25
Falta de gestión de los informes de control de los equipos de emergencia	ORG_27
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	ORG_17
Ausencia de estructura para combatir los incendios (descripción de los roles, responsabilidades)	ORG_14 ORG_24
Falta de seguimiento de los contratos de mantenimiento de los dispositivos de protección contra incendios	ORG_27
Ausencia de una estructura de gestión de crisis	ORG_14 ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Falta de concienciación sobre la protección de los dispositivos de seguridad	PER_05
Clima social conflictivo	
Presencia de aberturas que dan a la vía pública (ventanas)	PHY_03
Antigüedad de los locales	PHY_10
Falta de control de acceso al establecimiento o a los locales de éste	PHY_03
Falta de aislamiento antifuego	PHY_09
Falta de consideración, durante la fase de instalación, de los riesgos contra incendios específicos de los equipos alojados	PHY_06

Ausencia o dimensionamiento inadecuado del dispositivo automático de extinción de incendios	PHY_09
Falta de mantenimiento de los equipos de aire acondicionado	PHY_01 ORG_27

4.1.2 PERJUICIOS OCASIONADOS POR EL AGUA

Vulnerabilidad	Cobertura
Ejemplar único de las licencias	LOG_07
Aplicaciones únicas desarrolladas internamente	MAT_02
Falta de hardware de repuesto	MAT_01
Falta de respaldo de los datos contenidos en los soportes	ORG_08
Soportes originales	MAT_02 ORG_08
Falta de cobertura de seguridad en caso de siniestro grave	ORG_44
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada del subcontratista o proveedor	ORG_38
Ausencia de instrucciones de seguridad para el personal externo que trabaja dentro del organismo	ORG_25
Falta de gestión de los informes de control de los equipos de emergencia	ORG_27
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	ORG_17
Falta de instrucciones de alerta, de reacción, de información en caso de perjuicios ocasionados por el agua (Falta de identificación de llaves de paso,...)	ORG_24 ORG_24
Falta de garantía de buen funcionamiento de los detectores de presencia de agua	ORG_27
Falta de estructura de gestión de crisis	ORG_14 ORG_24
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de concienciación sobre la protección de los dispositivos de seguridad	PER_05
Clima social conflictivo	
Establecimiento ubicado en una zona anegadiza	PHY_04
Falta de control en los accesos físicos a los locales	PHY_03
Aberturas no herméticas que dan al exterior	PHY_03
Presencia aspersores	PHY_03
Techos o aberturas no herméticas que dan al exterior	PHY_03
Falta de identificación clara de las llaves de paso del agua	PHY_07
Acceso no protegido	PHY_03
Tubería de agua cerca de los equipos	PHY_03
Aspersores	PHY_10
Tubería de agua cerca de las terminales	PHY_03
Falta de sumidero	PHY_03
Acceso no protegido a los locales que alojan equipos de producción o distribución de los servicios esenciales	PHY_03
Cableado colocado en el suelo	PHY_07

Antigüedad de los conductos de refrigeración	PHY_10
Falta de mantenimiento de los equipos de aire acondicionado	PHY_01 ORG_27
Falta de llave de paso del agua	PHY_07

4.1.3 CONTAMINACIÓN

Vulnerabilidad	Cobertura
Ejemplar único de las licencias	LOG_07
Aplicaciones únicas desarrolladas internamente	MAT_02
Soporte sensible a las condiciones de conservación	MAT_03
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Falta de seguimiento de los contratos de mantenimiento	ORG_27
Falta de determinación de las medidas que deben adoptarse en caso de interrupción del servicio de climatización	ORG_16
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de concienciación sobre la protección de los equipos de seguridad	PER_05
Clima social conflictivo	
Proximidad de fuentes de contaminación (ruido, humo, vapor...)	PHY_04
Atmósfera contaminada (hangar, taller...)	PHY_04
Falta de mantenimiento de los equipos de aire acondicionado	PHY_01 ORG_27
Falta de hardware redundante correctamente dimensionado	PHY_01
Antigüedad de los filtros de climatización	PHY_10
Acceso no protegido a los equipos	PHY_03

4.1.4 SINIESTRO MAYOR

Vulnerabilidad	Cobertura
Ejemplar único de las licencias	LOG_07
Aplicaciones únicas desarrolladas internamente	MAT_02
Falta de hardware de repuesto	MAT_01
Falta de respaldo de los datos contenidos en los soportes	ORG_08
Soportes originales	MAT_02 ORG_08
Falta de servicio de emergencia cercano al organismo	ORG_24
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	ORG_17
Falta de cobertura de seguridad en caso de siniestro grave	ORG_44
Falta de estructura de gestión de crisis	ORG_14 ORG_24
Desconocimiento de las medidas de seguridad	PER_03

	PER_11
Falta de procedimientos de gestión de situaciones de emergencia	PER_11
Posibilidades de destrucción causada por un hecho externo (colisiones, atentados)	PHY_04
Proximidad de actividad industrial o establecimiento de riesgo	PHY_04
Locales donde los riesgos de explosión/implosión no han sido tenidos en cuenta	PHY_03

4.1.5 DESTRUCCIÓN DE HARDWARE O DE SOPORTES

Vulnerabilidad	Cobertura
Ejemplar único de las licencias	LOG_07
Aplicaciones únicas desarrolladas internamente	MAT_02
Falta de hardware de repuesto	MAT_01
Fragilidad del hardware	ORG_04
Hardware accesible a otras personas que no sean los propietarios (ej.: ubicado en un lugar de paso)	PHY_03
Soporte accesible a otras personas que no sean los propietarios	PHY_03
Falta de procedimiento de archivado	ORG_07
Fragilidad de los soportes	ORG_04
Ausencia de medidas de conservación de los archivos adaptadas a los plazos de conservación (antigüedad de las cintas magnéticas, desgaste del CD-ROM)	MAT_04
Falta de respaldo de los datos contenidos en los soportes	ORG_08
Soportes originales	MAT_02 ORG_08
Falta de instrucciones para el personal externo que trabaja dentro del organismo	ORG_25
Falta de cobertura de seguridad en caso de destrucción de hardware	ORG_44
Ausencia de normas para el uso y el almacenamiento de hardware y de soportes informáticos (condiciones de protección durante el transporte de los mismos, prohibición de fumar...)	ORG_04
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Clima social conflictivo	
Falta de concienciación sobre la protección física de los equipos	PER_01 PER_03
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03
Acceso físico no protegido a los locales donde hay hardware o soportes	PHY_03
Soportes accesibles a personas no autorizadas	ORG_01
Soportes bajo tierra no identificados	PHY_03
Equipo accesible a personas no autorizadas	ORG_01
Fragilidad de los equipos	ORG_04

4.1.6 FENÓMENO CLIMÁTICO

Vulnerabilidad	Cobertura
Condiciones de uso que exceden los límites de funcionamiento del hardware	PHY_01
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Falta de servicio de emergencia cercano al organismo	ORG_24
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	

Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Falta de medios de ventilación o de climatización en período estival excesivo calor	PHY_01
Falta de consideración de las condiciones climáticas para la construcción de los locales	PHY_04
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	MAT_03

4.1.7 FENÓMENO SÍSMICO

Vulnerabilidad	Cobertura
Hardware sensible a las vibraciones	PHY_03
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Falta de servicio de emergencia cercano al organismo	ORG_24
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Falta de consideración de los riesgos sísmicos para la construcción de edificios	PHY_04
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	MAT_03

4.1.8 FENÓMENO DE ORIGEN VOLCÁNICO

Vulnerabilidad	Cobertura
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Falta de servicio de emergencia cercano al organismo	ORG_24
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Falta de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Establecimiento reputado como de riesgo	PHY_04
Falta de consideración de los riesgos sísmicos para la construcción de edificios	PHY_04
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	MAT_03

4.1.9 FENÓMENO METEOROLÓGICO

Vulnerabilidad	Cobertura
Condiciones de uso que exceden los límites de funcionamiento del hardware	PHY_01
Falta de servicio de emergencia cercano al organismo	ORG_24

Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	PER_11
Establecimiento que sufre periódicamente fenómenos meteorológicos extremos (tempestades, huracanes, ciclones...)	PHY_04
Ausencia de protección contra rayos	PHY_04
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	MAT_03

4.1.10 INUNDACIÓN

Vulnerabilidad	Cobertura
Falta de servicio de emergencia cercano al organismo	ORG_24
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Establecimiento ubicado en una zona anegadiza	PHY_04
Falta de protección contra crecidas	PHY_03
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	MAT_03

4.1.11 FALLAS EN LA CLIMATIZACIÓN

Vulnerabilidad	Cobertura
Hardware que necesita climatización para funcionar	MAT_03 PHY_01
Archivos que requieren climatización para ser conservados	MAT_03 PHY_01
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	ORG_38
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	ORG_38
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de revisión de las necesidades de climatización en caso de modificación de los locales o de incorporación de hardware	PHY_01
Dispositivo que depende de un proveedor de agua helada o de energía eléctrica	PHY_01
Dispositivo incorrectamente dimensionado en relación con a las necesidades	PHY_01
Falta de mantenimiento de los equipos de aire acondicionado	PHY_01 ORG_27
Falta de hardware redundante correctamente dimensionado	PHY_01

Acceso no protegido a los dispositivos de suministro de agua y energía eléctrica	PHY_03

4.1.12 PÉRDIDA DE SUMINISTRO DE ENERGÍA

Vulnerabilidad	Cobertura
Hardware sensible a las perturbaciones eléctricas (bajas de tensión, sobretensiones, microcortes)	PHY_01
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	ORG_38
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	ORG_38
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de información sobre las condiciones de uso de los suministros de energía auxiliares	PER_11
Terminal de comunicación que no dispone de alimentación auxiliar	PHY_01
Los locales que resguardan baterías cuya composición es a base de ácido no están dedicados únicamente a eso y no están aislados físicamente del hardware con el cual están conectadas	PHY_06
Dimensionamiento inadecuado de los dispositivos de energía de emergencia (inversor, baterías...)	PHY_01
Acceso físico no protegido a los locales que alojan equipos de aprovisionamiento y distribución eléctrica	PHY_03
Los locales donde se conservan baterías cuya composición es a base de ácido no disponen de ventilación mecánica y no están acondicionados eléctricamente a prueba de explosiones	PHY_06
Los diversos revestimientos de suelos o muros no son antiestáticos	PHY_03
El tablero general de baja tensión no es accesible	PHY_01
No hay un puesto de transformación de media tensión/baja tensión instalado en el establecimiento (con acceso controlado del proveedor)	PHY_01
Falta de análisis de la potencia energética auxiliar, necesario en caso de incorporación de hardware	PHY_01
Las conexiones a masa y las conexiones a tierra no han sido realizadas conforme a la reglamentación vigente	PHY_10

4.1.13 PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN

Vulnerabilidad	Cobertura
Mantenimiento remoto de hardware utilizando medios de telecomunicación	PHY_01
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	ORG_23 ORG_38
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	ORG_38
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	ORG_38
Ausencia de instrucciones (alerta, prevención, reacción...)	ORG_24
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de mantenimiento de las terminales y los equipos de distribución	PHY_01

Fallas de gestión de la red telefónica interna	PHY_01
Funcionamiento incorrecto ya constatado en la provisión del servicio de telecomunicaciones	PHY_01
Acceso físico no protegido a los locales que alojan equipos de alimentación y distribución eléctrica o medios de telecomunicación	PHY_03

4.1.14 EMISIONES ELECTROMAGNÉTICAS

Vulnerabilidad	Cobertura
Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_03
Ausencia de cláusula contractual referida a la compatibilidad electromagnética	ORG_38
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	PHY_03
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	PHY_03
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	PHY_03
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_10

4.1.15 RADIACIONES TÉRMICAS

Vulnerabilidad	Cobertura
Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_03
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	PHY_03
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	PHY_03
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	PHY_03
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_10

4.1.16 IMPULSOS ELECTROMAGNÉTICOS

Vulnerabilidad	Cobertura
Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_03
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	PHY_03
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	PHY_03
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	PHY_03
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	PHY_10

4.1.17 INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

Vulnerabilidad	Cobertura
Falta de consideración de las normas de instalación	MAT_14 PHY_10
Falta de consideración de la zonificación del hardware	PHY_03
Hardware susceptible de emitir señales parásitas comprometedoras	PHY_05

Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de reglas que impongan el cumplimento de normas	ORG_04
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
Falta de procedimiento de verificación del hardware antes de su compra o luego de un mantenimiento	ORG_20
Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de una política de protección de la información	ORG_15
La política de seguridad no se aplica	ORG_18
Falta de realización de zonificación TEMPEST	PHY_05
Acceso público cerca de los edificios del organismo	PHY_05
Sala situada cerca de la vía pública	PHY_05
Soporte que facilita la captura de señales parásitas comprometedoras (cables eléctricos, tuberías...)	PHY_05
Falta de protección de los accesos a los equipos	PHY_03
Medios y soportes susceptibles de emitir señales parásitas comprometedoras	PHY_05

4.1.18 ESPIONAJE A DISTANCIA

Vulnerabilidad	Cobertura
Falta de protector de pantalla en caso de inactividad	LOG_16
Utilización de contraseñas de acceso al sistema o a la aplicación simples de observar (forma en un teclado, contraseña corta)	ORG_10
Sin cambios o pocos cambios en la contraseña de acceso al sistema o a la aplicación	ORG_10
Pantalla observable desde el exterior	PHY_02
Lectura de documentos delicados en lugares públicos (observación de documentos por parte de personas ajenas al organismo...)	ORG_15
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Ausencia de normas de protección para el intercambio de información de carácter confidencial	ORG_15
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
La política de seguridad no se aplica	ORG_18
Falta de identificación de los bienes delicados	ORG_26
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	ORG_14 ORG_15
Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de una política de protección de la información	ORG_15
Falta de identificación de las necesidades de seguridad de un proyecto	ORG_32
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Escasa concienciación sobre la protección de la información	PER_02
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Presencia de un lugar de observación desde fuera del establecimiento	PHY_02

Zona que dispone de una abertura que da a la vía pública	PHY_02
Zona observable desde un lugar de paso	PHY_07

4.1.19 ESCUCHA PASIVA

Vulnerabilidad	Cobertura
Falta de dispositivo de control de acceso en caso de inactividad	LOG_13
Posibilidad de agregar un software de escucha de tipo troyano	LOG_08
Falta de protección de los registros que recogen la traza de las actividades	ORG_15 ORG_39
Sin cambios o pocos cambios en la contraseña de acceso al sistema o a la aplicación	ORG_10
Falta de protección contra el uso de privilegios avanzados	LOG_11
Pocos cambios o ningún cambio en la contraseña de acceso al software de soporte de base	ORG_10
Acceso lógico al hardware que permite la instalación de un software de escucha	MAT_10
Hardware que dispone de una interfaz de comunicación susceptible de escucha (infrarrojos, 802.11, Bluetooth...)	RES_02
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Ausencia de normas de protección para el intercambio de información de carácter confidencial	ORG_15
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
Falta de control de la aplicación de la política de seguridad	ORG_22
Falta de identificación de los bienes delicados	ORG_26
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	ORG_14 ORG_15
La política de seguridad no se aplica	ORG_18
Ausencia de una política de protección de la información	ORG_15
Falta de identificación de las necesidades de seguridad de un proyecto	ORG_32
Falta de formación sobre las medidas y herramientas de protección de las comunicaciones internas y con el exterior del organismo	PER_03
Personal manipulable	PER_02
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Escasa concienciación sobre la protección de la confidencialidad de los intercambios de información	PER_09
Obtención de un beneficio para la captación de información	PER_08
Posibilidad de captar las transmisiones desde fuera del establecimiento	PHY_05
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03
Falta de protección de los accesos a las terminales de comunicación	RES_01
Medios y soportes que poseen características que permiten la escucha pasiva (ej.: Ethernet, sistemas de comunicación sin cable)	RES_02
Soporte o equipo de comunicación físicamente accesible que permite la instalación de dispositivos de escucha	ORG_01
Falta de autenticación del hardware conectado a la red	RES_03

Acceso físico o lógico a un repetidor que permita la instalación de un dispositivo de escucha	RES_01 PHY_03
Comunicación que se efectúa en modo Broadcast	RES_02
Complejidad del encaminamiento entre las subredes	RES_05
Interfaz que dispone de una función que permite la escucha	RES_01 RES_02
Circulación de información sin cifrar	RES_02
Falta de aislamiento de las redes de comunicación	RES_02
Posibilidad de escuchar las comunicaciones con los servidores de autenticación	RES_02
Posibilidad de escuchar las comunicaciones con los servidores de aplicación	RES_02
Posibilidad de introducir en las instalaciones de los clientes un software de escucha	LOG_08
Posibilidad de colocar un dispositivo de escucha lógica en las pasarelas de correo electrónico	LOG_08
Lagunas en la gestión de los privilegios de acceso a las pasarelas de correo electrónico	LOG_11

4.1.20 ROBO DE SOPORTES O DOCUMENTOS

Vulnerabilidad	Cobertura
Aplicaciones únicas desarrolladas internamente	MAT_02
Falta de inventario del hardware	MAT_06
Hardware atractivo (valor mercantil, tecnológico, estratégico)	MAT_07
Falta de protección del hardware contra robo (cable antirrobo)	MAT_07
Disco duro fácilmente desmontable	MAT_07
Hardware de libre uso que puede ser utilizado por un grupo de personas	MAT_07
Falta de protección de acceso a los equipos de respaldo de datos	MAT_07
Presencia de impresora en los lugares de paso	PER_02 ORG_01
Los soportes son accesibles a todos	MAT_07 ORG_15 ORG_30
Transmisión de soportes mediante servicios postales (proveedores externos, correo interno,...)	ORG_03
Falta de protección del almacenamiento de los soportes	MAT_07
Falta de inventario de los soportes utilizados	MAT_06
Falta de respaldo de los datos contenidos en los soportes	ORG_08
Soportes fácilmente transportables (ej.: disco duro extraíble, cartucho para respaldo de datos)	MAT_07
Soportes originales	MAT_02 ORG_08
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	ORG_15 ORG_38
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
Las responsabilidades de seguridad en cuanto a la clasificación de la información no han sido formalizadas ni son conocidas por todos	ORG_14 ORG_15
La política de seguridad no se aplica	ORG_18
Falta de estructura de gestión de los incidentes de seguridad	ORG_21
Falta de identificación de los bienes delicados	ORG_26
Falta de control de los bienes delicados	ORG_04 ORG_15

Falta de control de la aplicación de la política de seguridad	ORG_22
Falta de identificación de las necesidades de seguridad de un proyecto	ORG_32
Ausencia de una política de protección de la información	ORG_15
Personal manipulable	PER_02
Incumplimiento de las normas vinculadas con el procesamiento de las informaciones	PER_03
Falta de concienciación sobre la protección de documentos de carácter confidencial que provoca una falta de cuidado	PER_02
Obtención de un beneficio para la divulgación de información	PER_08
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Falta de compromiso individual para la protección de documentos de carácter confidencial	PER_05
Soportes o documentos enviados o presentes fuera del establecimiento	PER_01
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03

4.1.21 ROBO DE HARDWARE

Vulnerabilidad	Cobertura
Falta de hardware de repuesto	MAT_01
Falta de inventario del hardware	MAT_06
Hardware de libre uso que puede ser utilizado por un grupo de personas	MAT_07
Hardware atractivo (valor mercantil, tecnológico, estratégico)	MAT_07
Posible reventa del hardware (falta de marcado, utilización sin contraseña)	MAT_07
Hardware fácilmente desmontable	MAT_07
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
Falta de estructura de gestión y tratamiento de los incidentes de seguridad vinculados con robos	ORG_21
Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de normas de control de las entradas/salidas del hardware del organismo	ORG_02
Falta de identificación de los bienes delicados	ORG_26
Falta de identificación de las necesidades de seguridad de un proyecto	ORG_32
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Escasa concienciación sobre la protección del hardware fuera del organismo	PER_01
Personal manipulable	PER_02
Incumplimiento de las normas de protección física aplicables a los equipos portátiles	PER_01 PER_08
Obtención de un beneficio para la reventa de algún hardware	PER_08
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	PER_01
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03

4.1.22 RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS

Vulnerabilidad	Cobertura
Presencia de datos residuales utilizados por el software	MAT_08
Presencia de datos residuales sin que lo sepa el usuario, de hardware reasignado o desechado	MAT_08
Ausencia de medios para la destrucción de los soportes	MAT_08
Falta de identificación de los bienes delicados	ORG_26
Falta de control de los bienes delicados	ORG_04 ORG_15
Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de política de protección de la información aplicable al reciclado y desecho	ORG_15
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	ORG_38
Personal manipulable	PER_02
Incumplimiento de las normas de destrucción de los soportes vinculadas con la clasificación de la información	PER_02
Falta de información y de concienciación sobre la remanencia de los datos informáticos en los soportes	PER_02
Obtención de un beneficio para la divulgación de información	PER_08
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Presencia de soporte desechado fuera del establecimiento	ORG_15
Presencia de un soporte desechado en lugares públicos	ORG_15
Presencia de un soporte desechado en zonas accesibles a personas que no tienen necesidad de conocer la información involucrada	ORG_15

4.1.23 DIVULGACIÓN

Vulnerabilidad	Cobertura
Falta de verificación de los accesos compartidos concedidos	MAT_10 LOG_13
Procedimientos de gestión de los privilegios de acceso demasiado complicados de ejecutar	ORG_36
Funciones de gestión de los derechos de acceso demasiado complicadas de utilizar y que pueden ser fuente de error	MAT_11
Presencia de una red de comunicación con el exterior que permite el intercambio de información	MAT_10
Soportes capaces de realizar intercambios de información de carácter delicado	MAT_10
Falta de estructura responsable de la definición, la aplicación y el control de los privilegios de acceso a la información	ORG_14 ORG_30
Falta de identificación de los bienes delicados	ORG_26
La política de seguridad no se aplica	ORG_18
Falta de compromiso personal de protección de la confidencialidad	PER_05 ORG_37
Procedimientos de gestión y de aplicación de los permisos demasiado complicados de ejecutar	ORG_36
Las responsabilidades de seguridad en cuanto a la clasificación de la información no han sido formalizadas ni son conocidas por todos	ORG_14 ORG_15
Falta de control de los bienes delicados	ORG_04 ORG_15
Ausencia de una política de protección de la información	ORG_15

Incumplimiento de las normas vinculadas con el procesamiento de la información	PER_03
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Personal manipulable	PER_02
Falta concienciación sobre la protección de la información delicada	PER_03
Incumplimiento del deber de reserva	PER_09
Obtención de un beneficio para la divulgación de información	PER_08
Falta de control (inclusive de trazas) del intercambio con el exterior	PHY_07
Presencia de algún directorio compartido para almacenar información	RES_02
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Interfaz estándar que permite el intercambio de información (ej.: interfaz Bluetooth que acepte todas las comunicaciones por defecto)	RES_02
Posibilidad de utilizar los recursos sin generar trazas	RES_03
Falta de notificación de los usuarios	RES_03
Complejidad del encaminamiento entre las subredes	RES_05
Falta de encaminamiento estricto entre las subredes	RES_05
Falta de filtrado y de registro en los repetidores de comunicación entre redes	RES_02 RES_03
El sistema está conectado a redes externas	RES_02
Falta de control de acceso a los datos almacenados en el directorio	LOG_11
Falta de registro de los accesos	RES_03
Falta de dispositivo de filtrado	RES_02
Falta de gestión o dificultad para gestionar los privilegios de acceso a la información compartida (definición, implementación, control)	LOG_11
Falta de aislamiento entre las redes de comunicación	RES_02
Ausencia de medidas que permitan evitar una negligencia durante el envío de información	LOG_17
El sistema puede ser utilizado por todo el personal	LOG_13
El sistema permite el intercambio de ficheros adjuntos	PER_02
Falta de protección antivirus eficaz y operativa	ORG_06
Falta de gestión de los privilegios de acceso a los datos (posibilidad de alterar información pública...)	LOG_11
El sistema facilita la divulgación de información fuera del organismo	PER_02

4.1.24 INFORMACIÓN SIN GARANTÍA DEL ORIGEN

Vulnerabilidad	Cobertura
Recuperación de software desde un medio no autenticado	LOG_06 LOG_08
Posibilidad de instalar correcciones, actualizaciones, parches, hotfixes...	LOG_03 LOG_08 LOG_11
Ausencia de un medio seguro de identificación	LOG_13
Falta de conservación de trazas de las actividades	LOG_10
Falta de medios que permitan garantizar la procedencia del hardware	ORG_20
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	ORG_15 ORG_38
Falta de medios que permitan garantizar la procedencia de los suministros	ORG_20

Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de una política de conservación y de análisis de las trazas de las actividades	ORG_39
Falta de información referente a la división de responsabilidades y a los medios de garantizar la legitimidad de una petición	ORG_14
Falta de organización que permita garantizar la identificación de una persona dentro del organismo o en el marco de un proyecto	ORG_33
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Falta de concienciación sobre los riesgos de usurpación de identidad (uso incorrecto de los medios que garantizan la autenticación tales como las contraseñas)	PER_03
Credulidad	PER_02
Desconocimiento de la importancia de la calificación de la información	PER_10
Personal manipulable	PER_02
Clima social conflictivo	
Obtención de un beneficio gracias a la desinformación	PER_08
Falta de medios que permitan garantizar la autenticidad de los códigos	ORG_20
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Posibilidad de alterar una comunicación	RES_02
Protocolo que no permite autenticar en forma segura al emisor de una comunicación	RES_03
Posibilidad de utilizar los recursos sin generar trazas	RES_03
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Los repetidores no identifican ni las fuentes ni los destinos (ejemplo de impacto: sistema vulnerable a los ataques basados en "spoofing")	RES_03
Posibilidad de usurpar la función del directorio	RES_01
El sistema no permite identificar al autor de una modificación	LOG_10
El dispositivo permite acceder a datos que no han sido autenticados (ej.: menajes en cadena)	ORG_12
El sistema no dispone de medios de conservación del registro histórico de las actividades	RES_03
El sistema permite el almacenamiento o la modificación de información sin autenticación de sus autores	RES_03
El sistema permite la emisión y la recepción de información sin autenticación de emisores ni destinatarios	RES_03
El sistema no dispone de filtros para impedir la recepción de mensajes falsos en cadena procedentes del exterior	ORG_12
El sistema permite retransmisiones de mensajes	RES_01
El sistema no permite la identificación de la persona que emitió una petición	RES_03

4.1.25 SABOTAJE DEL HARDWARE

Vulnerabilidad	Cobertura
Posibilidad de colocar otros elementos de hardware para almacenar, enviar o alterar información (ej.: capturador de teclado físico)	MAT_10 RES_01
Ausencia de procedimiento para el control de las intervenciones de personal externo en los equipos del organismo	ORG_25
Falta de control de la aplicación de la política de seguridad	ORG_22
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30

	ORG_33 ORG_38
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de procedimientos de calificación operativa	ORG_26
Falta de control de los bienes delicados	ORG_04 ORG_15
Falta de identificación de los bienes delicados	ORG_26
Ausencia de procedimientos de validación de los componentes de hardware durante la entrega inicial o cuando se reincorporan tras un mantenimiento	ORG_20
Software no probado lo suficiente dentro de los valores límite especificados	ORG_26
Personal manipulable	PER_02
Falta de cuidado durante la intervención de personal de mantenimiento en un puesto de trabajo o un servidor	PER_05
Escasa concienciación sobre la protección del hardware fuera del organismo	PER_01
Obtención de un beneficio gracias a la desinformación	PER_08
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	PER_01
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03
Posibilidad de colocar una desviación de circuito	RES_01

4.1.26 ALTERACIÓN DE PROGRAMAS

Vulnerabilidad	Cobertura
El enlace de mantenimiento remoto está permanentemente activado	LOG_12 RES_06
Posibilidad de que existan funciones escondidas introducidas durante las fases de diseño y desarrollo	ORG_20 ORG_38
Posibilidad de modificar, de alterar el software	LOG_01
Falta de protección contra el uso de privilegios avanzados	LOG_11
Uso de programas no evaluados	LOG_06
Falta de implementación de normas de seguridad de base aplicables al sistema operativo y al software	LOG_04
Posibilidad de crear o modificar comandos de sistemas	LOG_08 LOG_11
Recuperación de software desde un medio no autenticado	LOG_06 LOG_08
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	RES_02
Contraseñas de conexión demasiado simples	ORG_10
Posibilidad de instalar correcciones, actualizaciones, parches, hotfixes...	LOG_03 LOG_08 LOG_11
Posibilidad de gestionar el sistema en forma remota	RES_01 RES_06
Uso de un sistema operativo estándar que ya ha sufrido ataques lógicos	LOG_06
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	LOG_11
Posibilidad de borrar, modificar o instalar nuevos programas	LOG_08
El dispositivo SNMP está activado	LOG_12 RES_06

El dispositivo SNMP está activado.: disquete, CD-ROM)	MAT_10
Falta de medios que permitan el control de inocuidad de los soportes cuando se ingresan al organismo	ORG_06
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de procedimiento para el control de las intervenciones de personal externo en los equipos del organismo	ORG_25
Ausencia de cláusulas contractuales referentes a la garantía de inocuidad de los suministros entregados por el subcontratista o proveedor	ORG_20 ORG_38
Ausencia de política global de lucha contra el código malicioso	ORG_06
Falta de identificación de los bienes delicados	ORG_26
Falta de control de la aplicación de la política de seguridad	ORG_22
Falta de control de los bienes delicados	ORG_04 ORG_15
Ausencia de política de protección de los puestos de trabajo	ORG_04 ORG_06
Ausencia de una política de conservación y de análisis de las trazas de las actividades	ORG_39
Ausencia de medidas de control de los desarrollos	ORG_20
Ausencia de medidas de protección de la integridad de los códigos en las fases de diseño, puesta en servicio y gestión	ORG_04 ORG_20
Uso de software sin garantía de su origen	PER_10
Clima social conflictivo	
Falta de concienciación sobre la amenaza de los códigos maliciosos	PER_03
Desconocimiento de las reacciones reflejas necesarias en caso de detección de anomalías	PER_11
Incumplimiento de las normas de actualización de los programas antivirus	PER_03
Personal manipulable	PER_02
Obtención de un beneficio gracias a la alteración del sistema informático	PER_08
Situación conflictiva	
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de medios que permitan garantizar la autenticidad de los desarrollos	ORG_20
Operador del sistema o personal de mantenimiento que dispone de privilegios extendidos	PER_02
Desconocimiento de los procedimientos en caso de detección de anomalías	PER_03
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	PER_01
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	PHY_03
La red facilita el uso de los recursos por parte de personas no autorizadas	RES_01
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Posibilidad de agregar desviaciones lógicas	RES_01
La red permite modificar los recursos del sistema o actuar sobre ellos	RES_01
Posibilidad de agregar software adicional para almacenar, enviar o alterar (ej.: capturador de teclado)	RES_01

Posibilidad de utilizar los recursos sin generar trazas	RES_03
Posibilidad de modificar o cambiar aplicaciones	LOG_11
Posibilidad de borrar o modificar programas o ficheros de sistema	LOG_11
Falta de concienciación sobre los riesgos generados por la descarga de software	PER_03
Falta de control antivirus en los intercambios de información	ORG_06
El dispositivo permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: componentes javascript que exploran el contenido del disco duro)	LOG_04 LOG_11
Presencia de un dispositivo que permite modificar o instalar aplicaciones en forma remota	LOG_11
Uso de un espacio de almacenamiento compartido	LOG_11
Utilización de una versión obsoleta del servidor de correo electrónico	LOG_09 ORG_13
Utilización de una lista de difusión que incluya gran parte del personal	ORG_12
Presencia de un protocolo que no dispone de función de autenticación	RES_03
El correo electrónico permite el envío automático de mensajes	LOG_14 ORG_06
Falta de concienciación sobre los riesgos provocados por la ejecución de ficheros adjuntos	PER_03
El correo electrónico permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: envío automático de ficheros adjuntos)	LOG_04
No se realiza ninguna verificación de las aplicaciones antes de su instalación	LOG_06
El correo electrónico permite instalar actualizaciones de software (ej.: parches, antivirus...)	LOG_11
Falta de medios de filtrado antivirus	ORG_06
Posibilidad de instalar programas piratas	LOG_11

4.1.27 GEOLOCALIZACIÓN

Vulnerabilidad	Cobertura
Hardware localizable (ej.: triangulación)	PHY_05
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	ORG_15 ORG_38
Ausencia de normas de protección de la confidencialidad de la información utilizada para localizar al personal (pedido de pasajes, registro de entrada/salida...)	ORG_15
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de discreción o de cuidado	PER_09
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13

4.1.28 AVERÍA DEL HARDWARE

Vulnerabilidad	Cobertura
Falta de función de diagnóstico para la prevención de fallos del hardware	LOG_14
Falta de protección contra perturbaciones eléctricas	PHY_03
Malas condiciones de uso	MAT_14
Problemas de mantenimiento	ORG_27
Poca fiabilidad del hardware	MAT_15
Envejecimiento del hardware	ORG_13
Soporte no adaptado a la vida útil de los datos que se van a archivar	MAT_03

	MAT_04
Malas condiciones de almacenamiento	PHY_03
Falta de cláusula referente a los plazos de intervención y de reemplazo en caso de avería del hardware	ORG_38
Falta de estructura de seguimiento de los contratos de mantenimiento	ORG_27
Falta de seguimiento de los contratos de mantenimiento y de soporte con los proveedores	ORG_27
Falta de informes sobre los fallos (cantidad, coste de los incidentes, duración)	ORG_21
Ausencia de normas referentes a las condiciones de uso de las infraestructuras de tratamiento de la información (prohibición de consumo de tabaco, de bebida, de alimentos) en los locales donde se conserva hardware informático)	PHY_08 ORG_04
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	ORG_16
Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio	ORG_24
Ausencia de estructura destinada al análisis de la adecuación de las capacidades de los equipos a las necesidades	ORG_09
Ausencia de normas referentes a las condiciones de uso de las infraestructuras de tratamiento de la información (prohibición de consumo de tabaco, de bebida, de alimentos) en los locales donde se conserva hardware informático)	
Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	PER_05
Falta de envío de informes para un análisis centralizado de los fallos	PER_05
Desconocimiento de las instrucciones de uso del hardware	PER_03
Falta de consideración del entorno específico que aumenta los riesgos de fallos (atmósfera sobrecalefaccionada, entorno industrial,...)	PHY_10
Ausencia de control del buen funcionamiento de los recursos de emergencia	ORG_16
Desencadenamiento manual de la solución de emergencia	ORG_16
Poca fiabilidad de los soportes	MAT_15
Envejecimiento de los soportes de información	ORG_13

4.1.29 FALLA DE FUNCIONAMIENTO DEL HARDWARE

Vulnerabilidad	Cobertura
Falta de función de diagnóstico para la prevención de fallos del hardware	LOG_14
Falta de protección contra perturbaciones eléctricas	PHY_03
Malas condiciones de uso	MAT_14
Poca fiabilidad del hardware	MAT_15
Posibilidad de incompatibilidad entre los distintos componentes del hardware	RES_04
Soporte no adaptado a la vida útil de los datos que se van a archivar	MAT_03 MAT_04
Malas condiciones de almacenamiento	PHY_03
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos	ORG_09
Ausencia de reglas que impongan el cumplimento de normas	ORG_04
Falta de cláusula referente a los plazos de intervención y de tratamiento en caso de falla de funcionamiento	ORG_38
Ausencia de informes sobre las fallas de funcionamiento	ORG_21
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	ORG_16
Ausencia de procedimientos de calificación operativa	ORG_26
Ausencia de normas referentes al entorno de uso de las infraestructuras de tratamiento	PHY_10

de la información (temperatura, higrometría...)	ORG_04
Ausencia de estructura destinada al análisis de la adecuación de las capacidades de los equipos a las necesidades	ORG_09
Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	PER_05
Desconocimiento de las instrucciones de uso del hardware	PER_03
Falta de envío de informes para un análisis centralizado de los fallos	PER_05
Falta de consideración del entorno específico que aumenta los riesgos de fallos (atmósfera sobrecalefaccionada, entorno industrial,...)	PHY_10
Ausencia de control del buen funcionamiento de los recursos de emergencia	ORG_16
Desencadenamiento manual de la solución de emergencia	ORG_16
Envejecimiento de los soportes de información	ORG_13
Posibilidad de incompatibilidad entre los soportes y otros componentes	RES_04
Medios y soportes que incorporan características técnicas específicas de su localización (ej.: diferentes parámetros de configuración ADSL entre Francia y el Reino Unido)	RES_04
Poca fiabilidad de los soportes	MAT_15
Problemas de mantenimiento	ORG_27
Interfaz que incorpora características técnicas referidas al país (ej.: conexiones telefónicas diferentes entre Francia y el reino Unido)	RES_04
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	RES_04
Envejecimiento del hardware	ORG_13
Posibilidad de incompatibilidad entre los distintos recursos	RES_04

4.1.30 SATURACIÓN DEL SISTEMA INFORMÁTICO

Vulnerabilidad	Cobertura
Falta de filtros que protejan al sistema contra saturaciones	LOG_14
Consumo inútil de recursos	LOG_14
Aplicación que requiere recursos informáticos que no se adaptan al hardware (ej.: falta de memoria RAM)	MAT_09
Falta de consideración, en la definición de los requerimientos de un proyecto, de situaciones particulares que ponen al sistema en condiciones límite	LOG_14
Falta de calificación de los desarrollos en un contexto representativo del uso	LOG_06
Dimensionamiento inadecuado de los recursos (ej.: falta de autonomía de una batería de ordenador portátil)	MAT_09
Persistencia involuntaria de los datos en los soportes	ORG_09
Ausencia de reglas que impongan el cumplimento de normas	ORG_04
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	ORG_09
Falta de cláusula contractual sobre la calidad de servicio de los sistemas que funcionan en condiciones límite (intensa demanda del sistema, ingreso de datos no conformes, ingreso de datos en los límites de funcionamiento)	ORG_38
Ausencia de una política de seguimiento del buen dimensionamiento de los equipos de la infraestructura de tratamiento de la información, incluidos los equipos de emergencia	ORG_09
Falta de instrucciones sobre el buen uso de los recursos informáticos a fin de evitar comportamientos que conducen a la saturación de los espacios de almacenamiento o de los recursos de tratamiento	ORG_09
Falta de instrucciones referidas a los incidentes (detección, acción...)	ORG_24
Falta de decisión de redimensionamiento que considere los significativos aumentos en el uso de los recursos informáticos	PER_05

Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	PER_05
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	PER_03 PER_12
Obtención de un beneficio mediante la alteración del sistema informático	PER_08
Falta de concienciación sobre las necesidades de economizar los recursos informáticos del organismo (uso incorrecto de los espacios de almacenamiento...)	PER_03
Dimensionamiento inadecuado de los recursos de telecomunicación, por ejemplo, como consecuencia del uso diario de recursos destinados a la solución de emergencia	ORG_16
Dimensionamiento inadecuado de los recursos de emergencia	ORG_16
Posibilidad de que los repetidores sean sometidos a una gran demanda o una intensa interferencia (ej.: ataque de denegación de servicio del tipo "smurf", "SYN flood"...)	MAT_05 LOG_14
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	RES_04
Dimensionamiento inadecuado (ej.: demasiados datos en relación con el ancho máximo de banda)	RES_02
Dimensionamiento inadecuado de los recursos (ej.: demasiados usuarios en relación con la capacidad máxima del directorio)	ORG_09
Posibilidad de someter el dispositivo a una enorme demanda que excede sus límites	ORG_09
Acontecimiento puntual o período durante el cual se produce un aumento muy significativo del uso del sistema	ORG_09
Dimensionamiento inadecuado de los recursos (ej.: demasiados usuarios en relación con la cantidad de conexiones posible y el ancho de banda)	ORG_09
Falta de gestión de los derechos de escritura en los espacios de almacenamiento compartidos	LOG_11
Dimensionamiento inadecuado de los recursos (ej.: espacio para almacenar o compartir ficheros demasiado limitado)	ORG_09
Falta de aislamiento entre las redes de comunicación	RES_02
Utilización de una lista de difusión interna accesible a todos	ORG_12
Dimensionamiento inadecuado de los espacios de almacenamiento de los mensajes recibidos	ORG_09
El correo electrónico permite la emisión automática de mensajes	LOG_14 ORG_06
Ausencia de protección contra spam	ORG_12
Falta de limitación del tamaño de los ficheros adjuntos	LOG_14
Uso incorrecto del servicio de correo electrónico por parte de los usuarios (utilización de los buzones de correo electrónico como espacio de archivado)	PER_03
Acceso público al portal	ORG_09
Dimensionamiento inadecuado de los recursos (ej.: demasiadas conexiones simultáneas)	ORG_09

4.1.31 FALLA DE FUNCIONAMIENTO DEL SOFTWARE

Vulnerabilidad	Cobertura
Posibles efectos secundarios vinculados con la actualización de un componente lógico	LOG_02
Falta de conservación de trazas de los procesamientos de información	LOG_10
Falta de formación en el uso y mantenimiento del nuevo software	PER_06 PER_12 ORG_14
Falta de procedimiento de mantenimiento	LOG_09 ORG_41
Falta de procedimiento de calificación antes de toda instalación o actualización	LOG_06

Falta de procedimiento de sincronización de los relojes	LOG_10
Falta de envío de informes para un tratamiento centralizado de las fallas de funcionamiento	LOG_15
Posibilidad de configurar, instalar o modificar en forma incorrecta el sistema operativo	LOG_04
Falta de informes de las operaciones de mantenimiento	LOG_03 LOG_08
Ausencia de gestión o error de gestión en la configuración de los componentes lógicos (ej.: aplicación de un parche de origen inglés no adaptado a una versión francesa)	LOG_08
Falta de documentación actualizada	ORG_28
No se realiza ninguna verificación de las aplicaciones antes de su instalación	LOG_06
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	LOG_09 ORG_13
Ausencia de reglas que impongan el cumplimento de normas	ORG_04
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	ORG_09
Ausencia de cláusulas contractuales referentes a las condiciones de asistencia y servicio técnico	ORG_38
Ausencia de política que permita el aislamiento de los entornos de usuario a fin de evitar conceder derechos de modificación de los sistemas y aplicaciones	ORG_33
Falta de instrucciones sobre el uso correcto de los recursos informáticos a fin de evitar conductas riesgosas	ORG_04
Falta de instrucciones referidas a los incidentes (detección, acción...)	ORG_24
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	ORG_16
Falta de homogeneidad del parque informático	ORG_42
Software no probado lo suficiente (conjunto de juegos de prueba que no cubren la totalidad de las condiciones de funcionamiento – intensa demanda del sistema, ingreso de datos no conformes, ingreso de datos en los límites de funcionamiento)	ORG_26
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallas de funcionamiento (esquemas orientativos)	PER_05
Falta de formación	PER_12
Ausencia de normas de seguridad durante los desarrollos	PER_10
Falta de formación en el mantenimiento y uso de los nuevos equipos	PER_12
Dimensionamiento inadecuado de los recursos de gestión y mantenimiento	ORG_09
Incumplimiento de los procedimientos de intervención	PER_03
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	PER_03 PER_12
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	RES_04
Gestión incorrecta de las versiones y configuraciones de los pilotos	RES_04
Efectos secundarios de las interfaces (problemas de compatibilidad entre protocolos...)	RES_04
Posibilidad de que el dispositivo esté sometido a peticiones o datos mal formados (ej.: buffer overflow, denegación de servicio en el servidor LDAP)	LOG_14
Incumplimiento de los procedimientos de instalación o de mantenimiento	ORG_04
Posibilidad de someter el dispositivo a una gran demanda que excede sus límites	ORG_09
Incompatibilidad de software (ej.: efecto secundario de un software antivirus que filtre los mensajes...)	RES_04
Posibilidad de que el dispositivo esté sometido a peticiones o datos mal formados (ej.: buffer overflow, denegación de servicio en el servidor SMTP, POP3, IMAP)	LOG_14
Utilización de una versión obsoleta del servidor de correo electrónico	LOG_09 ORG_13

4.1.32 PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN

Vulnerabilidad	Cobertura
No se realiza ninguna verificación de las aplicaciones antes de su instalación	LOG_06
Falta de procedimiento de emergencia	ORG_24
Falta de procedimiento de vuelta atrás en caso de anomalía durante una modificación	LOG_02
Falta de procedimiento de mantenimiento	LOG_09 ORG_41
Falta de documentación actualizada	ORG_28
Falta de informes de las operaciones de mantenimiento	LOG_03 LOG_08
Falta de conservación de las trazas de los procesos y modificaciones	LOG_03
Software específico	ORG_09
Falta de formación en el uso y mantenimiento del nuevo software	PER_06 PER_12 ORG_14
Software obsoleto	LOG_09
Software de configuración no escalable	LOG_06
Falta de medios para una asistencia técnica accesible desde fuera del organismo o desde un país con importante diferencia horaria	MAT_13
Hardware de configuración no escalable	ORG_13
Hardware obsoleto	ORG_13
Hardware específico	ORG_09 ORG_27
Modificación de los equipos, del software o de los procedimientos de respaldo de datos sin tener en cuenta anteriores respaldos o archivos	ORG_05
Soporte obsoleto	ORG_13
Pérdida o gestión incorrecta de los documentos originales (contratos de asistencia técnica, licencias...)	ORG_08
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Falta de cláusula contractual que asegure el restablecimiento de la actividad (en caso de cese de la actividad, en caso de quiebra del proveedor,...)	ORG_38
Falta de garantía referida a la continuidad del organismo	ORG_27
Falta de seguimiento de los contratos de mantenimiento y de soporte con los proveedores	ORG_27
Falta de instrucciones referidas a los incidentes (detección, acción...)	ORG_24
Falta de manual de aseguramiento de la calidad	ORG_29
Falta de estructura de protección de la documentación y de los medios de mantenimiento de los sistemas	ORG_30
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	ORG_16
Falta de procedimientos de gestión de la configuración de los sistemas	LOG_08
Falta de aplicación de normas o estándares durante el desarrollo del sistema de información	ORG_04 ORG_04
Falta de plan de formación en el mantenimiento de los nuevos sistemas	ORG_14
Elección de tecnología sin garantía de actualización permanente	ORG_13
Bajo presupuesto asignado al mantenimiento	PER_13

Existencia de componentes obsoletos en la infraestructura de tratamiento de la información (desarrollo en lenguajes más utilizados...)	ORG_13
Incumplimiento de las normas de calidad	PER_10
Ausencia de estándares o de normas	PER_10
Incumplimiento de las normas de calidad	PER_10
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	PER_03 PER_12
Uso de software o de desarrollos fuera de las normas y estándares del organismo	PER_10
Problemas de mantenimiento	ORG_27
Falta de plano del cableado	PHY_11
El mantenimiento o la gestión de los equipos requiere la disponibilidad de los soportes de red	RES_02
El mantenimiento o la gestión del sistema se realiza por intermedio de la red	RES_02
Falta de plazos máximos de garantía para los soportes de comunicación	MAT_04
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	LOG_09 ORG_13
Utilización de una versión obsoleta del servidor de correo electrónico	LOG_09 ORG_13
Uso de un sistema obsoleto	LOG_09
Uso de un sistema no estandarizado	ORG_28
Falta de cumplimiento de procedimientos de instalación y mantenimiento (especificaciones de configuración y parámetros)	ORG_04
Falta de medios de soporte internos	ORG_27

4.1.33 USO ILÍCITO DEL HARDWARE

Vulnerabilidad	Cobertura
Falta de gestión de licencia, de dispositivo de registro y de activación	LOG_07
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	LOG_08 LOG_13
Uso compartido de una identificación de conexión	LOG_11
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	LOG_12
El hardware está conectado a redes externas	MAT_10
El hardware utilizado permite un uso diferente del previsto (desarrollo de software no destinado al organismo...)	LOG_11 PER_03
Los soportes son accesibles a todos	MAT_07 ORG_15 ORG_30
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	ORG_02 ORG_04 ORG_27 ORG_30 ORG_33 ORG_38
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Falta de concienciación del personal sobre el riesgo de ser sancionado	PER_08 ORG_37

Ausencia de cláusulas contractuales referidas al uso del material informático	ORG_04
Falta de instrucciones referidas al uso del material informático	ORG_04
Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	LOG_11 ORG_33
Falta de procedimiento de control	ORG_33
La política de seguridad no se aplica	ORG_18
Ausencia de guía informática que especifique los requerimientos de uso	PER_03 ORG_04
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de concienciación sobre los riesgos de sanciones	PER_08
Derechos otorgados fuera de la legítima necesidad	PER_07
Obtención de un beneficio	PER_08
Incumplimiento de la guía informática que especifica los requerimientos de uso	PER_03
Falta de control de las necesidades materiales para desarrollar una aplicación	ORG_32
Ausencia de normas morales o éticas	PER_08
Falta de gestión del parque de hardware	PER_05
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	PHY_07
Falta de registro del ingreso de personas	PHY_07
Falta de protección de las líneas y equipos de comunicación	PHY_07
Los equipos permiten utilizar los recursos del sistema desde el exterior del organismo	RES_01
Los equipos son accesibles a todos	RES_01
Los equipos están conectado a redes externas	RES_01
Los equipos utilizados permiten usos diferentes de los previstos	RES_06
El dispositivo utilizado permite usos diferentes de los previstos	PER_03
Falta de auditorías o de supervisión de los accesos (particularmente, inventario de los accesos usados con el exterior del organismo y tipología de los flujos)	ORG_22
Ausencia de normas de acceso	LOG_11
El hardware está conectado a redes externas	RES_01 RES_03
El dispositivo es accesible a todos	LOG_11 ORG_01

4.1.34 COPIA ILEGAL DE SOFTWARE

Vulnerabilidad	Cobertura
Falta de gestión de los privilegios asociados a los perfiles (administradores, usuarios, invitados...)	LOG_11 LOG_11
Falta de gestión de licencia, de dispositivo de registro y de activación	LOG_07
Software atractivo para el "público en general"	ORG_04
Posibilidad de copiar fácilmente software o paquetes de programas	ORG_04
Posibilidad de copiar fácilmente las versiones de los sistemas operativos propietarios	ORG_04
Sistema operativo atractivo para el "público en general"	ORG_04
Hardware que permite el registro de datos en soportes (disquete, ZIP, grabadora de CD/DVD)	
Hardware que permite el registro de datos en soportes (disquete, ZIP, grabadora de CD-	ORG_15

ROM/DVD)	
Desinformación sobre las leyes y los reglamentos que se aplican al tratamiento de la información	ORG_40 ORG_41
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Ausencia de una política de control de las licencias impuesta a los establecimientos del organismo	LOG_07 ORG_38
Ausencia de cláusulas contractuales sobre el uso de copias ilegales de software	ORG_38 ORG_40
Ausencia de guía informática que especifique los requerimientos de uso	PER_03 ORG_04
Falta de concienciación del personal sobre el riesgo de ser sancionado	PER_08 ORG_37
Falta de concienciación o de información sobre la legislación referida a los derechos de autor	ORG_40 ORG_41
Falta de procedimiento de control	ORG_33
La política de seguridad no se aplica	ORG_18
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Obtención de un beneficio	PER_08
Incumplimiento de la guía informática que especifica los requerimientos de uso	PER_03
Falta de concienciación sobre los riesgos de sanciones	PER_08
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	PHY_07
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de registro del ingreso de personas	PHY_07
No se realiza ninguna verificación del origen de las aplicaciones antes de su instalación	ORG_20
El dispositivo de acceso permite el almacenamiento de software	RES_01
El dispositivo de acceso permite la descarga de software	RES_01

4.1.35 USO DE SOFTWARE FALSIFICADO O COPIADO

Vulnerabilidad	Cobertura
Falta de gestión de licencia, de dispositivo de registro y de activación	LOG_07
Posibilidad de copiar fácilmente software o paquetes de programas	ORG_04
Software atractivo para el "público en general"	ORG_04
Posibilidad de que los sistemas funcionen con sistemas operativos copiados en forma ilícita o falsificados	LOG_07 LOG_08 ORG_04
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Ausencia de una política de control de las licencias impuesta a los establecimientos del organismo	LOG_07 ORG_38
Ausencia de cláusulas contractuales sobre la identificación y la verificación del origen del software	ORG_38
Falta de concienciación o de información sobre la legislación referida a los derechos de autor	ORG_40 ORG_41
Falta de control de certificación de los productos	ORG_20

Falta de control del origen de los productos	ORG_20
Ausencia de guía informática que especifique los requerimientos de uso	PER_03 ORG_04
La política de seguridad no hace referencia a la notificación de las obligaciones y responsabilidades de cada uno en materia civil, penal y reglamentaria	ORG_40 ORG_41
Falta de definición de privilegios que limiten la posibilidad de realizar instalaciones en las estaciones de trabajo	LOG_11 ORG_33
Falta de concienciación del personal sobre el riesgo de ser sancionado	PER_08
Incumplimiento de la guía informática que especifica los requerimientos de uso	PER_03
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Ninguna certificación de los productos	LOG_06
Ningún procedimiento de evaluación de los productos	ORG_20
Falta de procedimiento y medios de verificación del origen del software (firma del código, del binario...)	ORG_20
Falta de registro del ingreso de personas	PHY_07
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	PHY_07
No se realiza ninguna verificación del origen de las aplicaciones antes de su instalación	ORG_20
El dispositivo de acceso permite el almacenamiento de software	RES_01
El dispositivo de acceso permite la descarga de software	RES_01

4.1.36 ALTERACIÓN DE DATOS

Vulnerabilidad	Cobertura
Falta de control de la integridad de los datos	LOG_01
Falta de procedimiento y de dispositivo de autorización para la modificación de datos	LOG_11
El enlace de mantenimiento remoto está permanentemente activado	LOG_12 RES_06
Falta de restricción en los puntos de ingreso del software	LOG_13
No se realiza ninguna verificación de las aplicaciones antes de su instalación	LOG_06
Falta de implementación de normas de seguridad de base aplicables al sistema operativo y al software	LOG_04
El software permite acceder a datos (contenido del disco duro, base de datos...)	LOG_11
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	LOG_11
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	RES_02
El sistema operativo permite acceder a datos (base de datos...)	LOG_11
Contraseñas de conexión demasiado simples	ORG_10
No se realiza ninguna verificación del sistema operativo antes de su instalación	LOG_06
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	LOG_12
Posibilidad de gestionar el sistema en forma remota	RES_01 RES_06
El dispositivo SNMP está activado	LOG_12 RES_06
Ausencia de normas de protección de datos	ORG_15

El hardware puede ser inicializado por cualquier persona a partir de un periférico (ej.: disquete, CD-ROM)	MAT_10
Hardware obsoleto	ORG_13
Falta de redundancia o procedimiento de respaldo de datos	MAT_01 ORG_08
Desgaste de los soportes	MAT_14
Falta de medios de protección y control de la integridad de los datos	LOG_01 LOG_01
Ausencia de normas y de procedimientos sobre la autorización del personal	ORG_30
Ausencia de una política de gestión y de control de las autorizaciones impuesta a los establecimientos del organismo	LOG_11 ORG_14 ORG_15 ORG_38
Ausencia de una política de protección de la información impuesta a los establecimientos del organismo	ORG_15 ORG_38
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Ausencia de una política de permisos de acceso a la información	ORG_30
Falta de seguridad de los accesos al SI (pasarelas, detección de intrusos, supervisión de los acontecimientos de seguridad,...)	ORG_30
Ausencia de cláusulas contractuales referidas a la protección del material informático	ORG_38
Falta de control de la aplicación de la política de seguridad	ORG_22
Falta de instrucciones referidas al uso del material informático	ORG_04
Falta de prevención y de detección de virus y otros programas maliciosos	ORG_06
Falta de control de acceso a la información	ORG_15 ORG_30
Falta de plan de formación sobre los problemas de seguridad	PER_02
Falta de procedimientos de control de los disquetes provenientes de fuera del organismo	ORG_06
Ausencia de guía informática que especifique los requerimientos de uso	PER_03 ORG_04
Incumplimiento de la guía informática que especifica los requerimientos de uso	PER_03
Falta de protección y clasificación de la información	ORG_15
Falta de concienciación del personal sobre el riesgo de ser sancionado	PER_08
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Personal manipulable	PER_02
Situación conflictiva entre personas	
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	PHY_07
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de registro del ingreso de personas	PHY_07
Falta de protección de las líneas y equipos de comunicación	PHY_07
Falta de protección física y lógica (aislamiento...)	RES_01 RES_02
Posibilidad de actuar sobre los datos enviados utilizando los medios de comunicación	RES_02
La red permite modificar los recursos del sistema o actuar sobre ellos	RES_01
La red facilita el uso de los recursos por parte de personas no autorizadas	RES_01

Falta de dispositivo sólido de control de acceso	MAT_10 RES_01
Falta de procedimiento respaldo de datos	ORG_08
El dispositivo permite borrar, modificar o instalar programas en forma remota	LOG_11
El dispositivo permite introducir programas hostiles tales como troyanos, virus, gusanos, bombas lógicas...	ORG_06
El dispositivo permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: componentes javascript que exploran el contenido del disco duro)	LOG_04 LOG_11
Falta de aislamiento entre las redes de comunicación	RES_02
El correo electrónico permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: envío automático de ficheros adjuntos)	LOG_04
Falta de auditorías o de supervisión de los accesos	ORG_22
Ausencia de normas de acceso	LOG_11

4.1.37 TRATAMIENTO ILÍCITO DE LOS DATOS

Vulnerabilidad	Cobertura
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	LOG_13
Falta de dispositivo de cifrado	RES_02
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	LOG_08 LOG_13
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	LOG_08
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	
Falta de protección física	RES_01 PHY_03 ORG_01
Falta de medio de identificación de la sensibilidad de los datos que contienen los soportes	ORG_15
Los soportes son accesibles a todos	MAT_07 ORG_15 ORG_30
Soportes atractivos (valor mercantil, tecnológico, estratégico)	MAT_07
Soportes móviles o fácilmente transportables (ej.: disquete, ZIP, disco duro extraíble)	MAT_07
Falta de medio de cifrado	ORG_15
Falta de procedimiento y medio de destrucción	MAT_08
Desinformación sobre las leyes y los reglamentos que se aplican al tratamiento de la información	ORG_40 ORG_41
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Ausencia de una política de protección de la información impuesta a los establecimientos del organismo	ORG_15 ORG_38
Ausencia de cláusula contractual de confidencialidad	PER_09
Falta de dispositivo de control y de sanción	PER_08 ORG_37
Falta de instrucciones referidas a los incidentes (detección, acción...)	ORG_24

Falta de control de acceso a la información	ORG_15 ORG_30
Falta de concienciación sobre las responsabilidades individuales	PER_05 ORG_14
Falta de designación de un responsable de la protección de datos e informaciones vinculadas con los individuos	ORG_14 ORG_15
La política de seguridad no se aplica, particularmente en lo que se refiere al tratamiento de los datos personales	ORG_18
Falta de concienciación del personal	PER_05 ORG_14
Falta de protección y de auditorías de acceso a los datos delicados	ORG_15 ORG_35
Falta de concienciación del personal sobre el riesgo de ser sancionado	PER_08
Falta de formación que especifique las condiciones de uso lícito de la información	PER_10
Falta de protección y clasificación de la información	ORG_15
Desconocimiento de las medidas de seguridad	PER_03 PER_11
Presencia de un acceso de escucha ilícito	RES_02
Falta de identificación de los niveles de protección de los sistemas	ORG_22
Falta de control del contenido	ORG_30
Falta de auditorías o de supervisión de los accesos	ORG_22
Falta de gestión de autorización de los accesos	LOG_11
El dispositivo facilita la divulgación de información fuera del organismo	PER_02
El dispositivo está conectado a redes externas	RES_01 RES_03

4.1.38 ERROR DE USO

Vulnerabilidad	Cobertura
Falta de documentación explícita sobre las aplicaciones	ORG_28
Conocimientos técnicos insuficientes del usuario	PER_12
Falta de procedimientos de prueba y de recepción conforme a las especificaciones	LOG_06
Falta de validación de los datos de entrada (de ingreso)	LOG_17
Falta de responsabilidad	PER_05 ORG_14
Aplicación de uso complejo	LOG_17
Falta de asistencia al usuario accesible	ORG_27
Uso no intuitivo del software	LOG_17
Conocimientos técnicos insuficientes	ORG_14
Falta de asistencia accesible	ORG_27
Falta de formación en el uso y mantenimiento del nuevo software	PER_06 PER_12 ORG_14
Software de uso complejo	LOG_17
Hardware de uso complejo o poco ergonómico	MAT_11
Malas condiciones de uso	MAT_14
Posibilidad de que cierto hardware provoque perjuicios al personal usuario (trabajo frente a un monitor, ondas...)	MAT_11 MAT_12
Falta de etiquetado de los soportes	MAT_06

Soportes de uso complejo o poco ergonómico	MAT_11
Falta de un control de los procesos críticos por parte del organismo central	ORG_38
Falta de doble control de los procesos críticos	ORG_43
Falta de formación referida al hardware o software utilizado	PER_12
Desconocimiento de las responsabilidades	PER_05
Falta de formalización de las responsabilidades conocidas por todos	PER_05
Condiciones de trabajo desfavorables	ORG_45
Falta de profesionalismo	PER_05
Incumplimiento de las instrucciones	PER_10
Personal usuario que ha recibido poca formación o formación de mala calidad	PER_12
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	PER_07
Falta de documentación sobre el uso de las aplicaciones existentes	PER_12
Falta de motivación para los trabajos vinculados con el ingreso de datos	PER_05
Personal poco acostumbrado al ingreso de datos	PER_06
Entorno de trabajo desfavorable (locales demasiado pequeños, falta de espacio para ubicar los elementos de trabajo...)	PHY_12
Falta de etiquetado de los cables o falta de plano del cableado	PHY_11
Espacio insuficiente en los locales técnicos	PHY_12
Falta de procedimiento de uso	ORG_04
Falta de etiquetado y de esquema de diseño actualizado	MAT_06
Falta de plano del cableado	PHY_11
Interfaz que incorpora características técnicas referidas al país (ej.: conexiones telefónicas diferentes entre Francia y el Reino Unido)	RES_04
Medios y soportes que incorporan características técnicas específicas de su localización (ej.: diferentes parámetros de configuración ADSL entre Francia y el Reino Unido)	RES_04
Falta de medidas de protección (sólo lectura...)	LOG_11
Falta de herramientas de supervisión	MAT_13

4.1.39 ABUSO DE DERECHO

Vulnerabilidad	Cobertura
Ausencia de una política de auditorías	ORG_22
Falta de respaldo de los registros de acontecimientos	ORG_08
Falta de registro de los acontecimientos	LOG_15
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Contraseñas de conexión demasiado simples	ORG_10
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	RES_02
La base de contraseñas del sistema operativo puede descifrarse fácilmente	ORG_10
El dispositivo SNMP está activado	LOG_12 RES_06
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	LOG_14
El enlace de mantenimiento remoto está permanentemente activado	LOG_12 RES_06
Posibilidad de gestionar el sistema en forma remota	RES_01 RES_06
Los logs o registros del sistema operativo pueden ser modificados por todos	LOG_11

Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	LOG_12
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	LOG_11
El sistema operativo no actualiza los registros o los acontecimientos del sistema	LOG_15
El sistema operativo permite realizar conexiones anónimas	LOG_13
El sistema operativo permite abrir una sesión sin ingresar la contraseña	LOG_13
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	LOG_11
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	LOG_09 ORG_13
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	ORG_10
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	LOG_08
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	LOG_13
Falta de protección física	RES_01 PHY_03 ORG_01
Falta de dispositivo sólido de control de acceso	MAT_10 RES_01
Falta de auditorías de los procedimientos de control de acceso físico	ORG_22
Ausencia de una política de gestión y de control de las autorizaciones impuesta a los establecimientos del organismo	LOG_11 ORG_14 ORG_15 ORG_38
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de cláusulas contractuales que limiten las responsabilidades de ambas partes	ORG_38
Falta de definición del derecho de conocer la información	ORG_33
Falta de dispositivo de control y de sanción	PER_08 ORG_37
Falta de un reglamento que defina los derechos	ORG_33
Las atribuciones de los usuarios no están claramente definidas	ORG_14
Falta de control de las atribuciones de los derechos de los usuarios	LOG_11
Preeminencia de la categoría de personal	PER_05
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	PER_07
Obtención de un beneficio	PER_08
Para el personal, no está definida la noción de derecho	PER_05
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de protección física y lógica	RES_01
No se aplica el principio del menor privilegio	LOG_11
Posibilidad de utilizar los recursos sin generar trazas	RES_03
El dispositivo es accesible a todos	LOG_11 ORG_01

4.1.40 USURPACIÓN DE DERECHO

Vulnerabilidad	Cobertura
Ausencia de una política de auditorías	ORG_22
Falta de respaldo de los registros de acontecimientos	ORG_08
Falta de registro de los acontecimientos	LOG_15
Los logs o registros del sistema operativo pueden ser modificados por todos	LOG_11
El sistema operativo permite abrir una sesión sin ingresar la contraseña	LOG_13
El sistema operativo permite realizar conexiones anónimas	LOG_13
El sistema operativo no actualiza los registros o los acontecimientos del sistema	LOG_15
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	LOG_11
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	LOG_12
La base de contraseñas del sistema operativo puede descifrarse fácilmente	ORG_10
El dispositivo SNMP está activado	LOG_12 RES_06
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	RES_02
Posibilidad de gestionar el sistema en forma remota	RES_01 RES_06
El enlace de mantenimiento remoto está permanentemente activado	LOG_12 RES_06
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	ORG_10
Contraseñas de conexión demasiado simples	ORG_10
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	LOG_09 ORG_13
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	LOG_14
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	LOG_08
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	LOG_11
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	LOG_13
El hardware está conectado a redes externas	MAT_10
Falta de dispositivo sólido de control de acceso	MAT_10 RES_01
Falta de aislamiento de los equipos	MAT_10
Falta de protección de los soportes	ORG_30
Falta de auditorías de los procedimientos de control de acceso físico	ORG_22
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	ORG_34
Ausencia de normas y de procedimientos sobre la autorización del personal	ORG_30
Falta de concienciación sobre los riesgos de sanciones	PER_08 ORG_37
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Falta de procedimiento de control	ORG_33

Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	LOG_11 ORG_33
Falta de protección de los espacios dedicados a intercambiar o a compartir información	ORG_30
Falta de procedimiento de autorización del personal	LOG_11 ORG_30
Ausencia de un clima de confianza entre los individuos	PER_05 ORG_37
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	ORG_14 ORG_15
Falta de comunicación y de información de los procedimientos de autorización del personal	ORG_41
Falta de procedimiento de envío de informe en caso de detección de anomalías	ORG_24
La política de seguridad no se aplica	ORG_18
Organización no adaptada	ORG_14
Derechos otorgados fuera de la legítima necesidad	PER_07
Situación conflictiva entre personas	
Ausencia de normas morales o éticas	PER_08
Obtención de un beneficio	PER_08
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	PER_07
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Misiones poco adaptadas al personal	ORG_14
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	PHY_07
Falta de protección física y lógica (aislamiento...)	RES_01 RES_02
Falta de aislamiento de la red	RES_01 RES_02
Las interfaces están conectadas a redes externas	RES_01
Los soportes y los medios están conectados a redes externas	RES_01
Posibilidad de modificar características técnicas (ej.: dirección MAC de una tarjeta Ethernet)	LOG_11
Falta de protección física	RES_01 PHY_03 ORG_01
La red permite modificar los recursos del sistema o actuar sobre ellos	RES_01
Presencia de un protocolo que no dispone de función de autenticación	RES_03
Las interfaces son accesibles a todos	RES_01
La red facilita el uso de los recursos por parte de personas no autorizadas	RES_01
Los repetidores no identifican ni las fuentes ni los destinos (ejemplo de impacto: sistema vulnerable a los ataques basados en "spoofing")	RES_03
El dispositivo es accesible a todos	LOG_11 ORG_01
Posibilidad de que el dispositivo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	LOG_14
No se realiza ningún control de las aplicaciones antes de su instalación	LOG_06
Se puede acceder al dispositivo de correo electrónico desde Internet	RES_01
Utilización de una versión obsoleta del servidor de correo electrónico	LOG_09 ORG_13

4.1.41 NEGACIÓN DE ACCIONES

Vulnerabilidad	Cobertura
Ausencia de una política de auditorías	ORG_22
Falta de respaldo de los registros de acontecimientos	ORG_08
Falta de registro de los acontecimientos	LOG_15
El sistema operativo no actualiza los registros o los acontecimientos del sistema	LOG_15
El dispositivo SNMP está activado	LOG_12 RES_06
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	RES_02
Ficheros de imputación complejos o poco ergonómicos	ORG_42
Contraseñas de conexión demasiado simples	ORG_10
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	ORG_10
La base de contraseñas del sistema operativo puede descifrarse fácilmente	ORG_10
El sistema operativo permite realizar conexiones anónimas	LOG_13
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	LOG_14
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	LOG_11
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	LOG_09 ORG_13
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	LOG_11
Posibilidad de gestionar el sistema en forma remota	RES_01 RES_06
Los logs o registros del sistema operativo pueden ser modificados por todos	LOG_11
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	LOG_08
El sistema operativo permite abrir una sesión sin ingresar la contraseña	LOG_13
El enlace de mantenimiento remoto está permanentemente activado	LOG_12 RES_06
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	LOG_12
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	LOG_13
Falta de dispositivo de trazas y de auditoría	RES_03 ORG_39
El hardware es accesible y puede ser utilizado por todos	MAT_10
Los soportes son accesibles a todos	MAT_07 ORG_15 ORG_30
Falta de procedimiento de acceso a la información clasificada	ORG_15
Cambio de política o de estrategia de organización	ORG_14 ORG_33
Falta de definición de las responsabilidades	ORG_14
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	ORG_14
Falta de procedimientos disciplinarios	ORG_37
Presencia de un interés político-económico	ORG_31

Ausencia de una política global de gestión y de archivado de las trazas y otros elementos de prueba	ORG_39
Falta de cláusula contractual referida a la definición de los procedimientos de comunicación e intercambio de información	ORG_03 ORG_38
Falta de control mutuo de códigos	ORG_20 ORG_38
Presencia de cláusula de multa o sanción desmesurada o no adaptada al contexto	ORG_37 ORG_38
Ausencia de un mecanismo de seguimiento de actividad, de registros de acontecimientos y de alertas	ORG_39
Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	LOG_11 ORG_33
Falta de estructura jerárquica y procedimientos de informes	ORG_21
Ausencia de funciones de auditoría separadas de las funciones de seguimiento	PER_07 ORG_22
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	PER_13
Obtención de un beneficio	PER_08
Falta de confianza en la organización	
No se conoce la responsabilidad de cada uno	PER_05
Situación conflictiva entre personas	
Falta de registro histórico de las entradas y salidas de personas	PHY_07
Los repetidores son accesibles a todos	RES_01
El soporte de comunicación permite utilizar los servicios del sistema desde el exterior del organismo	RES_01
Los soportes y medios son accesibles a todos y están activos por defecto (ej.: conjunto de conectores RJ45 fijos)	RES_01
La red facilita el uso de los recursos por parte de personas no autorizadas	RES_01
El protocolo no permite la identificación segura del emisor	RES_03
La red permite modificar los recursos del sistema o actuar sobre ellos	RES_01
El protocolo no permite el envío de acuses de recibo	RES_03
Posibilidad de utilizar los recursos sin generar trazas	RES_03
El dispositivo de acceso no registra las trazas provenientes de su uso	ORG_39
El acceso al dispositivo de trazas no está protegido	LOG_11
El dispositivo es accesible a todos (ej.: dispositivo que no autentica las estaciones de trabajo de clientes ni los usuarios)	LOG_11
El dispositivo está conectado a redes externas	RES_01 RES_03

4.1.42 DAÑO A LA DISPONIBILIDAD DEL PERSONAL

Vulnerabilidad	Cobertura
Posibilidad de que cierto hardware provoque perjuicios al personal usuario (trabajo frente a un monitor, ondas...)	MAT_11 MAT_12
Falta de procedimiento de archivado	ORG_07
Presencia de un clima social desfavorable	
Presencia de un conflicto político-económico entre el país de origen de la organización y el país que la acoge	ORG_31
Falta de cláusulas o procedimientos de transferencia de los conocimientos	PER_06 ORG_38
Falta de continuidad financiera o tecnológica del organismo	ORG_13

Falta de cláusula de continuidad de provisión del servicio	ORG_16 ORG_38
Falta de elementos para la protección del personal	ORG_45
Presencia de una epidemia viral local	PER_04
Falta de procedimientos de transferencia de conocimientos	PER_06
Presencia, en la organización, de un clima social desfavorable para la actividad	
Falta de plan de concienciación y de formación sobre los procedimientos de contingencia para las actividades profesionales	PER_10 ORG_16
Falta de procesos de gestión de la continuidad de las actividades profesionales del organismo	ORG_16
Subdimensionamiento de la organización	PER_04 ORG_14
Falta de suplentes del personal estratégico	PER_04
Falta de estructura redundante de las funciones delicadas	PER_04 ORG_14
Falta de procesos de gestión de la continuidad de las actividades profesionales del equipo de proyecto	ORG_16
Ausencia de base documental de las normas y procedimientos	ORG_41
Falta de disponibilidad provocada por una actitud competitiva	PER_05
Falta de disponibilidad por causa de enfermedad	PER_04
Falta de disponibilidad debida al ausentismo	PER_04 PER_05
Falta de disponibilidad provocada (agresión física, toma de rehenes...)	PER_04
Problemas sociales	
Clima social conflictivo	
Clima social complicado que puede provocar huelgas de transporte	PHY_04
Personal especializado alojado en locales remotos	PHY_04
Personal que reside lejos de los locales del organismo	PHY_04
Posibilidad de consecuencias nocivas para el personal usuario (transmisión por vía hertziana, ondas...)	MAT_12

5 Propuesta de cobertura de los objetivos de seguridad genéricos mediante requerimientos de seguridad

Los siguientes cuadros permiten determinar con facilidad los requerimientos de seguridad genéricos que permitirían satisfacer cada objetivo de seguridad genérico (cuyos códigos corresponden a los de las partes anteriores).

5.1 MAT : Hardware

MAT_01	
Cobertura	BGC_INT.1.1 BGC_PRE.1.1 CGS_GSS.1.1 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9 FRU_FLT.1.1 FRU_FLT.2.1

MAT_02	
Cobertura	BGC_INT.1.1 CGS_SVG.1.1 CGS_SVG.1.2

MAT_03	
Cobertura	BMA_MAA.2.1 BPE_SEM.1.1

MAT_04	
Cobertura	BGC_MSS.1.1 CGS_ARC.1.1 CGS_ARC.1.2

MAT_05	
Cobertura	CAR_AAR.1.1 CAR_PAR.1.1 FRU_FLT.1.1

MAT_06	
Cobertura	BCM_RLC.1.1

MAT_07	
Cobertura	BCM_RLC.1.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BSP_RIS.5.1 BSP_RIS.5.2 CET_EGT.1.10 CET_EGT.1.8 CET_EGT.1.9 CET_EGT.2.3 CET_EGT.3.1 CGS_PPS.2.1

	CGS_PPS.3.1 CGS_PPS.3.2 FIA_UAU.1.2/2.1 FIA_UAU.6.1 FIA_UID.1.2/2.1
MAT_08	
Cobertura	BGC_INT.1.1 BGC_MSS.2.1 CGS_SVG.1.2
MAT_09	
Cobertura	BDM_ESS.1.1 BGC_PRS.1.1 CAR_AAR.1.1 CEI_ABS.1.5
MAT_10	
Cobertura	BGC_EIL.2.1 BGC_MSS.3.1 BGC_PRE.4.1 BPE_SEM.1.1 BPE_ZOS.2.1 CGS_GLI.2.1 FTA_TAB.1.1
MAT_11	
Cobertura	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_12	
Cobertura	BSP_FOU.2.1 CEI_CDT.2.1 CEI_CDT.2.2
MAT_13	
Cobertura	CGS_GSU.1.1 CGS_GSU.1.3 CGS_SUP.1.1
MAT_14	
Cobertura	CGS_OML.1.1

5.2 LOG : Software

LOG_01	
Cobertura	BDM_COC.3.1 FDP_ITT.3.1 FDP_ITT.3/4.2 FDP_SDI.1/2.1 FDP_SDI.2.1 FPT_ITI.1/2.2 FPT_ITT.3.1 FPT_ITT.3.2 FPT_TST.1.2

LOG_02	
Cobertura	BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.2.1 BGC_PRS.2.1 CDO_SDC.1.2 CGS_GMA.6.1

LOG_03	
Cobertura	BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BMA_SAS.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6

LOG_04	
Cobertura	CGS_CSR.1.2 FMT_MSA.3.1

LOG_05	
Cobertura	

LOG_06	
Cobertura	BDM_SED.4.1 BDM_SFS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 CGS_OML.1.1 CGS_OML.1.2 CGS_PPS.2.4

LOG_07	
Cobertura	BCM_RLC.1.1 BCO_CEL.3.1 CGS_GLI.1.1 CGS_GLI.1.2 CGS_GLI.1.3 CGS_GLI.1.4

LOG_08

Cobertura	BCM_RLC.1.1 BCO_RPS.2.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BGC_PRE.2.1 BGC_PRE.2.2 BGC_PRS.2.1 BMA_MAS.3.1 CDO_SDC.1.1 CGS_PPS.1.1 CGS_PPS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FPT_RVM.1.1 FPT_SEP.1.1

LOG_09

Cobertura	BGC_PRE.1.1 CDO_APP.1.1 CDO_APP.1.2 CEI_CDT.1.1 CEI_CDT.1.2

LOG_10

Cobertura	BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.3.1 FPT_STM.1.1

LOG_11

Cobertura	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.6.1 BGC_MSS.2.1 BGC_MSS.3.1 BGC_PRE.2.1 BGC_PRS.2.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAA.1.1 BMA_MAR.1.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.5.1 BPE_SEM.6.1 BPS_PSI.1.5 CGS_CSR.1.2 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4

	CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDT.1.1 CGS_GLI.2.1 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PEP.1.1 CGS_PPS.2.1 CGS_PPS.2.5 FDP_RIP.1.1 FDP_RIP.2.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1
LOG_12	
Cobertura	FAU_SAA.2.3
LOG_13	
Cobertura	BDM_SED.4.1 BMA_MAS.3.1 BMA_MAS.7.1 BMA_MAS.8.1 CGS_GDH.1.2 CGS_GDH.2.1 CGS_PPS.2.3 CGS_PPS.2.4 FIA_UAU.7.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_14	
Cobertura	BDM_SSA.1.1 BGC_EIL.4.1 CAR_AAR.1.1 CGS_CME.1.1 CGS_PPS.2.4 FRU_FLT.1.1
LOG_15	
Cobertura	BMA_SAS.1.1 CET_EGT.1.6 FAU_GEN.1.1 FAU_GEN.1.2
LOG_16	
Cobertura	BMA_MAS.7.1 BMA_MAS.8.1 CIS_ADL.1.1 FTA_SSL.1.1 FTA_SSL.2.1 FTA_SSL.3.1
LOG_17	
Cobertura	BGC_EIL.4.1

	BGC_EIL.5.1 CGS_PPS.2.3

5.3 RES : Red

RES_01	
Cobertura	BCO_CEL.5.1 BDM_COC.2.1 BDM_COC.4.1 BGC_EIL.1.1 BGC_EIL.4.1 BGC_PLM.1.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_REU.2.1 BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CAR_PAR.1.1 CET_EGT.1.1 CGS_CSR.1.1 CGS_CSR.1.2 CGS_CSR.1.3 CGS_GDA.1.1 CGS_GDA.3.1 CGS_GDA.3.2 CGS_GDH.1.1 CIS_PSI.1.1 FMT_MOF.1.1 FMT_MSA.1.1 FMT_MSA.3.2 FMT_MTD.1.1 FMT_MTD.2.1 FPT_ITA.1.1 FPT_ITI.1/2.1 FPT_ITI.1/2.2 FPT_ITI.2.3 FPT_ITT.3.1 FPT_ITT.3.2 FTA_TAB.1.1 FTA_TSE.1.1

RES_02	
Cobertura	BDM_COC.1.1 BDM_COC.2.1 BDM_COC.4.1 BDM_COC.5.1 BGC_GER.1.1 BGC_PRE.4.1 BGC_PRS.1.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1

	BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.6.1 BMA_MAR.7.1 BPE_SEM.1.1 BPE_SEM.3.1 BPE_ZOS.2.1 CAR_PAR.1.1 CGS_CSR.1.2 CGS_PPS.1.2 CGS_PPS.1.3 FCO_NRO.2.1 FCS_COP.1.1 FDP_ITT.1/2.1 FDP_UCT.1.1 FPT_ITC.1.1 FPT_ITT.1/2.1 FTA_TAB.1.1
RES_03	
Cobertura	BDM_COC.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BMA_MAR.4.1 BMA_MAS.1.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_MAS.6.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.1.1 CGS_GDA.1.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FCO_NRO.1.1 FCO_NRO.1.2 FCO_NRO.1.3 FCO_NRO.2.1 FCO_NRR.1.1 FCO_NRR.1.2 FCO_NRR.1.3 FCO_NRR.2.1 FDP_UCT.1.1 FIA_UAU.1.2/2.1 FTA_TAB.1.1
RES_04	
Cobertura	BGC_PRS.2.1 BMA_MAR.8.1 CGS_PPS.2.2 CGS_PPS.2.3 CIS_PSI.1.2
RES_05	
Cobertura	BMA_MAR.8.1 BPE_SEM.3.1
RES_06	
Cobertura	BDM_COC.4.1

	BGC_PLM.1.1 BMA_GAU.2.1 BMA_MAR.5.1

PER : Personal

PER_01	
Cobertura	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_EIL.7.1 BGC_MSS.1.1 BMA_IMT.1.1 BMA_IMT.2.1 BPE_SEM.5.1 BSP_FOU.1.1 CCS_CSG.1.3

PER_02	
Cobertura	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_EIL.6.1 BGC_MSS.2.1 BOS_ISI.3.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CET_EGT.2.3 CFO_SPS.1.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_CIR.1.3 CRR_SEN.1.1

PER_03	
Cobertura	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_SED.1.1 BDM_SED.3.1 BDM_SED.4.1 BDM_SFS.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_INT.3.1 BGC_MSS.3.1 BGC_PLM.1.1 BGC_PRE.1.1

	BGC_PRE.2.1 BGC_PRE.2.2 BMA_GAU.2.1 BMA_MAS.5.1 BMA_REU.1.1 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_FOU.2.1 BSP_RIS.1.1 BSP_RIS.3.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CFO_SPS.1.1 CGI_GIS.1.1 CGI_GIS.1.8 CGS_GDH.1.2 CGS_GDH.2.1 CGS_GMP.1.1 CGS_GMP.1.3 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPD_DGL.1.1 CPD_DGL.1.2 CRR_SEN.1.1
PER_04	
Cobertura	BSP_RIS.5.1 BSP_RIS.5.2 CFO_FRS.1.1 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CRH_DDE.1.1 CRH_DDE.1.2 CRH_PDP.1.1
PER_05	
Cobertura	BGC_PRS.1.1 BOS_ISI.3.1 BOS_SAT.1.3 BPS_PSI.1.3 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CFO_FRS.1.1 CFO_FRS.1.2

	CFO_FRS.1.3 CFO_FRS.1.4 CFO_FRS.1.5 CFO_SPS.1.1 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGI_GIS.3.4 CGI_GIS.3.5 CGI_GIS.3.6 CGS_GDH.1.2 CGS_HSI.1.1 CGS_HSI.1.2 CGS_PAI.2.1 CGS_PAI.2.3 CPS_PAQ.2.1 CPS_PAQ.2.2 CRH_DDE.1.1 CRH_DDE.1.2
PER_06	
Cobertura	BSP_FOU.1.1 BSP_FOU.2.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.2.1 CFO_FRS.2.2 CFO_FRS.2.3 CFO_FRS.2.4 CPS_PAQ.3.1
PER_07	
Cobertura	BOS_ISI.7.1 CGS_GDH.1.1 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.7 CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
PER_08	
Cobertura	BMA_MAS.6.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CCS_CHI.1.1
PER_09	
Cobertura	BGC_PRE.6.1 BOS_SOT.1.1 BOS_SOT.1.2 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.3.1 CFO_SPS.1.1 CPD_DGL.1.1 CPD_DGL.1.2
PER_10	
Cobertura	BCM_CLI.1.1

	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.4.1 BDM_SFS.1.1 BDM_SFS.3.1 BMA_GAU.2.1 BMA_MAS.5.1 BPS_PSI.1.3 BPS_PSI.1.4 BPS_PSI.1.5 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CFO_SPS.1.1 CGS_OML.1.2 CGS_PPS.2.1 CGS_PPS.2.3 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.6
PER_11	
Cobertura	BCA_AGC.1.1 BCA_AGC.5.1 BGC_INT.3.1 BPS_PSI.1.4 BSP_FOU.1.1 BSP_RIS.1.1 BSP_RIS.3.1 CCS_SIN.2.1 CCS_SIN.2.2 CCS_SIN.2.3 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.7 CGI_GDC.1.4 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.3 CGI_GDC.3.4 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GIS.1.8 CRR_SEN.1.2
PER_12	
Cobertura	BSP_FOU.1.1 BSP_FOU.2.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2

	CGS_GMA.2.1
PER_13	
Cobertura	BOS_ISI.1.1 BPS_PSI.1.1 CGS_GMA.5.1

PHY : Establecimiento

PHY_01	
Cobertura	BGC_PRE.6.1 BPE_SEM.2.1 BPE_SEM.4.1 BSP_FOU.2.1 CAR_AAR.1.1 CDS_DES.1.1 CDS_DES.1.2 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSS.1.1 CGS_GSS.1.2 CIS_ADL.2.1 CIS_MPP.1.1 CIS_MPP.1.2 CIS_MPP.1.3

PHY_02	
Cobertura	BPE_MMG.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2

PHY_03	
Cobertura	BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.2.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ERS.1.1 CET_EGT.1.1 CGS_PDI.1.1 CIS_ADL.1.2 CIS_ADL.2.1 CIS_ADL.2.2 CIS_MPP.1.2 CIS_MPP.2.2 CIS_MPP.3.1 CIS_MPP.3.2 CIS_MPP.3.3 CIS_MPP.3.4 CIS_PSI.1.1 CIS_PSI.1.2 CIS_SSI.1.2 CIS_ZOS.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1

PHY_04

Cobertura	CIS_ADL.2.1 CIS_CDL.1.1 CIS_SSI.1.1 CIS_SSI.1.2 CIS_SSI.1.3 CIS_SSI.1.4 CRH_PDP.1.1 CRH_PDP.1.2 CRH_PDP.1.3 CRR_ETU.1.1 CRR_ETU.1.2 CRR_ETU.2.1 CRR_ETU.2.2

PHY_05

Cobertura	BGC_GER.1.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.4.1 CIS_ADL.1.1 CIS_ADL.1.2 CPD_DGL.1.1

PHY_06

Cobertura	CEI_ERS.1.1

PHY_07

Cobertura	BGC_GER.1.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BPE_SEM.3.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.4.1 CET_EGT.1.3 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.3.1 CET_EGT.3.2 CET_EGT.3.3 CET_EGT.3.4 CET_EGT.3.5 CIS_ADL.1.1 CIS_ADL.3.1 CIS_CSI.1.1 CIS_MPP.1.1

PHY_08

Cobertura	CCS_CSG.1.2

PHY_09

Cobertura	CIS_CSI.1.1 CIS_CSI.1.2 CIS_MPP.2.1 CIS_MPP.2.2

PHY_10

Cobertura	BPE_SEM.4.1 CCS_RGI.1.1 CGS_GMA.1.1 CGS_GMA.1.2

	CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CIS_ADL.2.1 CIS_CSI.1.1 CIS_CSI.2.1 CIS_MPP.2.2 CIS_PSI.1.1 CIS_PSI.1.2
PHY_11	
Cobertura	CIS_ADL.3.1 CIS_CSI.1.1
PHY_12	
Cobertura	CIS_ADL.2.3 CRH_CDT.1.1

ORG : Organización

ORG_01	
Cobertura	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 CET_EGT.1.1 CET_EGT.2.3 CET_EGT.3.1 CGS_GDH.1.2 CGS_GDH.2.1 CIS_PSI.1.1 CIS_PSI.1.2 FCO_NRO.2.1

ORG_02	
Cobertura	BPE_SEM.1.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CET_EGT.1.10 CET_EGT.1.8 CET_EGT.1.9 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3

ORG_03	
Cobertura	BGC_EIL.1.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1

ORG_04	
Cobertura	BCM_CLI.2.1 BCM_RLC.1.1 BCO_CEL.2.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_SED.3.1 BDM_SED.5.1 BDM_SFS.1.1 BDM_SFS.2.1 BDM_SFS.3.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_MSS.3.1 BGC_PRE.1.1 BGC_PRE.2.2 BMA_IMT.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BOS_SAT.2.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.1.1 BPE_SEM.2.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_SEM.5.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_FOU.1.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1 CCS_CHI.1.1 CCS_CSG.1.1 CCS_CSG.1.2 CCS_CSG.1.3 CCS_CSG.1.4 CCS_CSG.1.5 CCS_CSG.1.6 CCS_CSG.1.7 CDO_SDC.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_EIP.1.6 CGS_GLI.1.4 CGS_GLI.2.1 CGS_PDI.1.1 CGS_PPS.2.1 CGS_PPS.2.5 CPS_DEV.1.1 CPS_DEV.1.2 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_05	
Cobertura	CDO_SDC.1.2 CGS_ARC.1.7 CGS_SVG.1.7
ORG_06	
Cobertura	BDM_SED.4.1 BGC_EIL.4.1 BGC_EIL.5.1 BGC_MSS.1.1 BGC_PLM.1.1 CGS_CME.1.1 CGS_OML.1.1 CGS_OML.1.3 CGS_PPS.2.3 CGS_PPS.2.4 CPS_PPT.1.1 CPS_PPT.1.2 CPS_PPT.1.3 CPS_PPT.1.4 CPS_PPT.1.5
ORG_07	

Cobertura	BGC_PRE.1.1 CGS_ARC.1.3 CGS_ARC.1.4 CGS_ARC.1.5 CGS_ARC.1.6 CGS_ARC.1.7 CGS_ARC.1.8 CGS_ARC.1.9

ORG_08

Cobertura	BGC_INT.1.1 BGC_PRE.1.1 CGS_GLI.1.2 CGS_GSS.1.1 CGS_SVG.1.1 CGS_SVG.1.2 CGS_SVG.1.3 CGS_SVG.1.4 CGS_SVG.1.5 CGS_SVG.1.6 CGS_SVG.1.7 CGS_SVG.1.8 CGS_SVG.1.9

ORG_09

Cobertura	BCA_AGC.1.1 BCA_AGC.3.1 BCA_AGC.5.1 BGC_MSS.2.1 BGC_PRS.1.1 BGC_PRS.2.1 BPE_SEM.6.1 BSP_FOU.1.1 CCS_CSG.1.2 CDO_APP.1.1 CDO_APP.1.2 CDS_DES.1.1 CEI_ABS.1.5 CFO_FRS.2.2 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3 CGS_CSR.1.2 CRH_DDE.1.1 CRH_DDE.1.2 FDP_RIP.1.1 FDP_RIP.2.1

ORG_10

Cobertura	BMA_MAS.4.1 BMA_REU.1.1 BMA_REU.2.1 CGS_GMP.1.1 CGS_GMP.1.2 FIA_SOS.1.1 FIA_SOS.2.1 FIA_SOS.2.2

ORG_11

Cobertura	

ORG_12

Cobertura	BGC_EIL.4.1

	CCS_CSG.1.1 CCS_CSG.1.2 CFO_SPS.1.1 CFO_SPS.1.2 CGS_CME.1.1 CGS_CSR.1.2
ORG_13	
Cobertura	BGC_PRS.2.1 BPE_SEM.4.1 CCC_RGF.1.1 CCC_RGF.1.2 CEI_CDT.1.1 CEI_CDT.1.2
ORG_14	
Cobertura	BCM_CLI.1.2 BDM_SSA.3.1 BGC_EIL.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.2.1 BOS_ISI.3.1 BPS_PSI.1.3 BSP_FOU.1.1 BSP_FOU.2.1 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCS_SRI.1.1 CDO_APP.1.1 CDO_APP.1.2 CFO_FRS.1.2 CFO_FRS.1.3 CFO_FRS.1.5 CGI_GDC.2.3 CGI_GDC.2.4 CGI_GDC.2.5 CGI_GDC.3.3 CGI_GDC.3.5 CGI_GDC.3.6 CGI_GDC.4.5 CGI_LCI.1.4 CGI_LCI.1.5 CGI_LCI.1.6 CGI_LCI.1.7 CGS_CIR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GDH.2.1 CGS_GDH.2.2 CGS_GMA.2.1 CGS_OES.1.1 CGS_OES.1.2

	CGS_OES.1.3 CGS_PAI.1.1 CGS_PAI.1.2 CGS_PAI.1.3 CRH_DDE.1.1 CRH_DDE.1.2 CRH_QDP.1.1
ORG_15	
Cobertura	BCM_CLI.1.1 BCM_CLI.1.2 BCM_CLI.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_EIL.2.1 BGC_EIL.4.1 BGC_EIL.7.1 BGC_GER.1.1 BGC_MSS.1.1 BGC_MSS.2.1 BGC_MSS.3.1 BMA_IMT.2.1 BMA_MAA.1.1 BPE_MMG.1.1 BPE_MMG.2.1 BPE_SEM.6.1 BPS_PSI.1.5 BSP_SPR.3.1 CGS_CIR.1.1 CGS_CIR.1.2 CGS_GDH.1.1 CGS_GDH.1.4 CGS_GMR.1.1 CGS_GMR.1.2 CPD_DGL.1.1 FDP_RIP.1.1 FDP_RIP.2.1
ORG_16	
Cobertura	BCA_AGC.1.1 BCA_AGC.2.1 BCA_AGC.3.1 BCA_AGC.4.1 BCA_AGC.5.1 BGC_PRE.3.1 BSP_RIS.1.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GSS.1.3 CGS_GSS.1.4 CGS_GSS.2.1 CGS_GSS.2.2
ORG_17	
Cobertura	CCS_SIN.1.1 CCS_SIN.1.2

	CCS_SIN.1.3 CCS_SIN.1.4 CCS_SIN.2.1 CCS_SIN.3.1 CCS_SIN.3.2
ORG_18	
Cobertura	BCO_CEL.4.1 BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BPS_PSI.1.4 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.4.1
ORG_19	
Cobertura	
ORG_20	
Cobertura	BDM_ESS.1.1 BDM_SED.1.1 BDM_SED.2.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.3.1 BGC_MSS.1.1 BGC_PLM.1.1 BGC_PRS.2.1 BOS_SAT.1.3 CGS_OML.1.1 CGS_OML.1.2 CGS_OML.1.3 CGS_PPS.2.3
ORG_21	
Cobertura	BOS_ISI.1.2 BSP_RIS.1.1 BSP_RIS.4.1 CGI_GIS.2.1 CGI_GIS.2.2 CGI_GIS.2.3 CGI_GIS.2.4 CGI_GIS.2.5 CGI_GIS.3.1 CGI_GIS.3.2 CGI_GIS.3.3
ORG_22	
Cobertura	BCO_RPS.1.1 BCO_RPS.1.2 BCO_RPS.2.1 BDM_COC.4.1 BGC_PRE.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_ISI.7.1 BOS_SAT.1.1 CCS_SIN.3.3 CCS_SSE.1.1 CIS_CSI.1.3

	CPD_INP.1.1 FAU_ARP.1.1 FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1 FAU_SAA.1.1 FAU_SAA.1.2 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_SAA.4.1 FAU_SAA.4.2 FAU_SAA.4.3
ORG_23	
Cobertura	BCO_RPS.1.1 BCO_RPS.1.2 BPE_ZOS.1.1 CIS_CSI.1.1 CIS_CSI.1.2 CIS_PSI.1.1 CIS_PSI.1.2 CIS_PSI.1.3
ORG_24	
Cobertura	BGC_PRE.1.1 BGC_PRE.3.1 BSP_RIS.1.1 BSP_RIS.2.1 CCS_SIN.2.1 CCS_SIN.2.3 CCS_SIN.3.1 CCS_SIN.3.2 CCS_SIN.3.4 CCS_SIN.3.5 CCS_SSE.1.1 CCS_SSE.1.2 CCS_SSE.1.3 CCS_SSE.1.4 CCS_SSE.1.5 CCS_SSE.1.6 CCS_SSE.1.7 CGI_GDC.1.1 CGI_GDC.1.2 CGI_GDC.1.3 CGI_GDC.1.4 CGI_GDC.2.1 CGI_GDC.2.2 CGI_GDC.2.6 CGI_GDC.3.1 CGI_GDC.3.2 CGI_GDC.3.4 CGI_GDC.4.1 CGI_GDC.4.2 CGI_GDC.4.3 CGI_GDC.4.4 CGI_GDC.4.6 CGI_GIS.1.1 CGI_GIS.1.2 CGI_GIS.1.3

	CGI_GIS.1.4 CGI_GIS.1.5 CGI_GIS.1.6 CGI_GIS.1.7 CGI_GIS.1.8 CGI_LCI.1.1 CGI_LCI.1.2 CGI_LCI.1.3 CGS_GSS.2.1 CGS_GSS.2.2 CIS_SSI.1.1
ORG_25	
Cobertura	BOS_SAT.1.3 BOS_SAT.2.1 CCS_CSP.1.1 CCS_CSP.1.2 CCS_CSP.1.3 CCS_CSP.1.4 CCS_CSP.2.1 CCS_SIN.1.1 CET_EGT.1.1 CET_EGT.1.2 CET_EGT.1.3 CET_EGT.1.4 CET_EGT.1.5 CET_EGT.1.6 CET_EGT.2.1 CET_EGT.2.2 CET_EGT.2.3 CET_EIP.1.1 CET_EIP.1.3 CET_EIP.1.4 CET_EIP.1.5 CET_PLD.1.4
ORG_26	
Cobertura	BCM_RLC.1.1 BDM_ESS.1.1 BDM_SED.4.1 BDM_SED.5.1 BDM_SFS.1.1 BGC_PRS.2.1 CGS_PPS.2.3 CGS_PPS.2.4 CGS_REC.1.1
ORG_27	
Cobertura	BGC_INT.2.1 BGC_PRS.2.1 BOS_SAT.1.2 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2 BPE_SEM.4.1 BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CCC_RGF.1.1 CCC_RGF.1.2 CET_EIP.1.3

	CET_EIP.1.6 CGS_GMA.1.1 CGS_GMA.1.2 CGS_GMA.2.1 CGS_GMA.3.1 CGS_GMA.3.2 CGS_GMA.3.3 CGS_GSU.1.1 CGS_GSU.1.2 CGS_GSU.2.1 CGS_GSU.2.2 CGS_GSU.2.3 CGS_GSU.3.1 CGS_GSU.3.2 CGS_GSU.3.3 CGS_PDI.1.1 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_28	
Cobertura	CDO_APP.1.1 CDO_APP.1.3 CGS_PPS.2.3
ORG_29	
Cobertura	CPS_PAQ.1.1 CPS_PAQ.1.2 CPS_PAQ.1.3 CPS_PAQ.1.4 CPS_PAQ.1.5 CPS_PAQ.1.6
ORG_30	
Cobertura	BCM_RLC.1.1 BCO_CEL.5.1 BDM_COC.2.1 BGC_GER.1.1 BGC_MSS.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.1.1 BMA_GAU.2.1 BMA_GAU.4.1 BMA_MAR.1.1 BMA_MAR.2.1 BMA_MAR.3.1 BMA_MAR.4.1 BMA_MAR.5.1 BMA_MAR.7.1 BMA_MAS.2.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BOS_SAT.1.1 BOS_SAT.1.2 BOS_SAT.1.3 BOS_SAT.1.4 BOS_SAT.1.5 BOS_SAT.2.1 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 CEI_ABS.1.1 CET_EGT.2.3 CGS_CSR.1.3 CGS_GDH.1.1 CGS_GDH.1.2 CGS_GDH.1.3 CGS_GDH.1.4 CGS_GDH.1.5 CGS_GDH.1.6 CGS_GDH.1.7 CGS_GDH.1.8 CGS_GDH.1.9 CGS_GMA.4.1 CGS_PAI.1.2 CGS_PAI.1.3 CGS_PDI.1.1 CGS_PEP.1.1 CGS_PPS.3.2 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_31	
Cobertura	CEI_ABS.1.6 CEI_ABS.1.7 CRH_PDP.1.1
ORG_32	
Cobertura	BPS_PSI.2.2 BPS_PSI.2.4 CEI_ABS.1.1 CEI_ABS.1.2 CEI_ABS.1.3 CEI_ABS.1.4 CEI_ABS.1.5
ORG_33	
Cobertura	BCO_RPS.1.1 BCO_RPS.1.2 BDM_SSA.1.1 BDM_SSA.4.1 BGC_PRE.4.1 BMA_EMA.1.1 BMA_GAU.2.1 BMA_MAA.1.1 BMA_MAA.2.1 BMA_MAR.1.1 BMA_MAR.6.1 BMA_MAR.7.1 BMA_MAS.1.1 BMA_MAS.3.1 BMA_MAS.5.1 BMA_REU.2.1 BOS_SAT.1.2 BOS_SAT.1.5 BPE_SEM.1.1 BPE_SEM.3.1 BPE_SEM.3.2

	BPE_ZOS.1.1 BPE_ZOS.2.1 BPE_ZOS.3.1 BPE_ZOS.4.1 BPE_ZOS.5.1 BSP_SPR.3.1 CET_EGT.1.3 CET_PLD.1.2 CGS_GLI.2.1 CGS_OES.1.2 CGS_OES.1.3 CGS_PAI.2.1 CGS_PAI.2.2 CGS_PAI.2.3 CGS_PDI.1.1 CGS_PPS.2.5 FPT_PHP.1/2.1 FPT_PHP.2.3 FPT_PHP.3.1
ORG_34	
Cobertura	BOS_ISI.5.1 BOS_ISI.5.2 BOS_ISI.5.3 BOS_ISI.6.1 BOS_ISI.6.2 BOS_ISI.6.3
ORG_35	
Cobertura	BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1
ORG_36	
Cobertura	CGS_GDH.1.3 CGS_PAI.1.4
ORG_37	
Cobertura	BCO_CEL.1.1 BCO_CEL.4.1 BCO_CEL.7.1 BCO_CEL.7.2 BDM_SSA.1.1 BDM_SSA.4.1 BMA_MAS.3.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 BOS_SAT.1.3 BOS_SAT.2.1 BSP_RIS.5.1 BSP_RIS.5.2 BSP_SPR.1.1 BSP_SPR.3.1 BSP_SPR.4.1 CCC_CLR.1.1
ORG_38	
Cobertura	BDM_SED.4.1 BDM_SED.5.1 BGC_PRE.6.1 BOS_ISI.4.1 BOS_ISI.7.1

	BOS_SOT.1.1 BOS_SOT.1.2 CCC_CLR.1.2 CGS_GPC.1.1 CGS_GPC.1.2 CGS_PPS.2.3 CRI_MOF.1.1 CRI_MOF.2.1
ORG_39	
Cobertura	BDM_COC.2.1 BDM_COC.4.1 BGC_INT.2.1 BMA_SAS.1.1 BMA_SAS.2.1 BMA_SAS.3.1 CGS_GDA.1.4 FAU_SAA.2.1 FAU_SAA.2.2 FAU_SAA.2.3 FAU_SAA.3.1 FAU_SAA.3.2 FAU_SAA.3.3 FAU_STG.1/2.1 FAU_STG.1/2.2 FAU_STG.2.3 FAU_STG.3.1 FAU_STG.4.1
ORG_40	
Cobertura	BCO_CEL.1.1 BCO_CEL.2.1 BCO_CEL.4.1 BCO_CEL.5.1 BPS_PSI.1.3
ORG_41	
Cobertura	BGC_PRE.1.1 BMA_GAU.1.1 BPS_PSI.1.3 BSP_FOU.1.1 CDO_APP.1.1 CDO_APP.1.2
ORG_42	
Cobertura	BDM_ESS.1.1 BDM_SFS.1.1 BGC_PRS.2.1 BMA_GAU.2.1 CGS_REC.1.1 FCO_NRO.1.1
ORG_43	
Cobertura	CGS_GPC.2.1 CGS_GPC.2.2 CGS_GPC.2.3 CGS_GPC.2.4
ORG_44	
Cobertura	CRR_ETU.1.1 CRR_ETU.1.2 CRR_ETU.2.2

ORG_45	
Cobertura	CRH_CDT.1.1 CRH_CDT.1.2 CRH_PDP.1.1

Formulario de recogida de comentarios

Este formulario puede enviarse a la siguiente dirección:

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identificación del aporte
Nombre y organismo (facultativo): .....
Dirección de correo electrónico: .....
Fecha: .....

Observaciones generales sobre este documento
¿El documento responde a sus necesidades? Si □ No □

En caso afirmativo:

¿Piensa que puede mejorarse su contenido? Si □ No □

En caso afirmativo:

¿Qué otros temas hubiera deseado que tratáramos?
.....
.....

¿Qué partes del documento le parecen inútiles o inadecuadas?
.....
.....

¿Piensa que puede mejorarse su formato? Si □ No □

En caso afirmativo:

¿En qué aspecto podríamos mejorarlo?
- legibilidad, comprensión □
- presentación □
- otro □

Indique sus preferencias en cuanto al formato:
.....
.....

En caso negativo:

Indique el aspecto que no le resulta conveniente y defina lo que le hubiera resultado conveniente:
.....
.....

¿Qué otros temas desearía que se trataran?
.....
.....

Observaciones específicas sobre este documento

Puede formular comentarios detallados utilizando el siguiente cuadro.

"N°" indica un número de orden.

El "tipo" está compuesto por dos letras:

La primera letra indica la categoría de la observación:

- O Error de ortografía o de gramática
- E Falta de explicaciones o de aclaración en un punto existente
- I Texto incompleto o faltante
- R Error

La segunda letra indica su carácter:

- m menor
- M Mayor

La "referencia" indica la ubicación precisa en el texto (número de párrafo, línea...).

El "enunciado de la observación" permite formalizar el comentario.

La "solución propuesta" permite presentar la forma de resolver el reto enunciado.

N°	Tipo	Referencia	Enunciado de la observación	Solución propuesta
1				
2				
3				
4				
5				

Gracias por su colaboración