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 4
HERRAMIENTAS PARA LA APRECIACION 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 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 fundamentales al estudio del sistema correspondiente. - 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 explotación 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, , 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 identificación de los requerimientos de seguridad del 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 el posicionamiento del procedimiento EBIOS. Contiene también una bibliografía, un glosario y 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 cuarta sección del método.

Presenta:
- una tipología de los tipos y subtipos de entidades,
- una tipología de los métodos de ataque que se describen en función de los elementos peligrosos que pueden utilizarlos,
- una base de vulnerabilidades organizada por método de ataque que incluye una lista de los tipos y subtipos de entidades involucrados.

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

2 Tipos y subtipos de entidades

2.1 MAT : Hardware

MAT: Hardware	
Tipo	MAT: Hardware
Descripción	Descripción: ---------- El tipo hardware está constituido por el conjunto de los elementos físicos de un sistema informático.

2.1.1 MAT_ACT : Soporte de procesamiento de datos (activo)

MAT_ACT: Soporte de procesamiento de datos (activo)	
Tipo	MAT_ACT: Soporte de procesamiento de datos (activo)
Descripción	Descripción: ---------- Equipo informático de tratamiento automático de datos que incluye los circuitos necesarios para su funcionamiento autónomo. Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático.
MAT_ACT.1: Hardware portátil	
Tipo	MAT_ACT.1: Hardware portátil
Descripción	Descripción: ---------- Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en lugares diferentes. Ejemplos: ---------- Microordenador portátil, PDA. Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático. MAT_ACT: Soporte de tratamiento de datos (activo) Equipo informático de tratamiento automático de datos que incluye los circuitos necesarios para su funcionamiento autónomo.
MAT_ACT.2: Hardware fijo	
Tipo	MAT_ACT.2: Hardware fijo
Descripción	Descripción: ---------- Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo. Ejemplos : ---------- Servidor, microordenador utilizado como estación de trabajo.

	Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático. MAT_ACT: Soporte de procesamiento de datos (activo) Equipo informático de tratamiento automático de datos que incluye los circuitos necesarios para su funcionamiento autónomo.
MAT_ACT.3: Periférico de procesamiento	
Tipo	MAT_ACT.3: Periférico de procesamiento
Descripción	Descripción: ---------- Hardware conectado a un ordenador mediante un puerto de comunicación (serie, paralelo, USB...) para la recepción, la transmisión o la emisión de datos. Ejemplos: ---------- Impresora, reproductor de discos extraíble. Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático. MAT_ACT: Soporte de procesamiento de datos (activo) Equipo informático de tratamiento automático de datos que incluye los circuitos necesarios para su funcionamiento autónomo.

2.1.2 MAT_PAS : Soporte de datos (pasivo)

MAT_PAS: Soporte de datos (pasivo)	
Tipo	MAT_PAS: Soporte de datos (pasivo)
Descripción	Descripción: ---------- Se trata de soportes de almacenamiento de datos o de funciones. Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático.
MAT_PAS.1: Soporte electrónico	
Tipo	MAT_PAS.1: Soporte electrónico
Descripción	Descripción: ---------- Soporte informático conectado a un ordenador o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos sin modificar su pequeño tamaño. Se utiliza a partir de equipo informático estándar. Ejemplos: ---------- Disquete, CD-ROM, cartucho para respaldo de datos, disco duro extraíble, llave de memoria, cinta magnética. Tipos y subtipos de entidades afiliadas: ---------- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un

	sistema informático. MAT_PAS: Soporte de datos (pasivo) Se trata de soportes de almacenamiento de datos o de funciones.

MAT_PAS.2: Otros soportes	
Tipo	MAT_PAS.2: Otros soportes
Descripción	Descripción: --- Soporte estático no electrónico que contiene datos. Ejemplos: --- Papel, diapositiva, transparencia, documentación, fax. Tipos y subtipos de entidades afiliadas: --- MAT: Hardware El tipo hardware está formado por el conjunto de los elementos físicos de un sistema informático. MAT_PAS: Soporte de datos (pasivo) Se trata de soportes de almacenamiento de datos o de funciones.

2.2 LOG : Software

LOG: Software	
Tipo	LOG: Software
Descripción	Descripción: ---------- El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información.

2.2.1 LOG_APP : Aplicación profesional

LOG_APP: Aplicación profesional	
Tipo	LOG_APP: Aplicación profesional
Descripción	Tipos y subtipos de entidades afiliadas: ---------- LOG: Software El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información.

LOG_APP.1: Aplicación profesional estándar	
Tipo	LOG_APP.1: Aplicación profesional estándar
Descripción	Descripción: ---------- Se trata de programas disponibles en el mercado cuya finalidad es brindar directamente a los usuarios los servicios y funciones que esperan recibir de su sistema de información en el marco de su profesión. Los ámbitos de aplicación son múltiples y, por definición, ilimitados. Ejemplos: ---------- Software de contabilidad, software controlador de máquina herramienta, software de atención al cliente, software de gestión de conocimientos técnicos del personal, software de procedimientos administrativos remotos... Tipos y subtipos de entidades afiliadas: ---------- LOG: Software El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información. LOG_APP: Aplicación profesional

LOG_APP.2 : Aplicación profesional específica	
Tipo	LOG_APP.2 : Aplicación profesional específica
Descripción	Descripción : Se trata de desarrollos específicos (lo que influye especialmente en los aspectos de soporte, mantenimiento, evoluciones…) cuya finalidad es brindar directamente a los usuarios, los servicios y funciones que esperan recibir de su sistema de información en el marco de su profesión. Los ámbitos de aplicación son múltiples y, por definición, ilimitados. Ejemplos : Gestión de facturación a clientes de un prestador de servicios de telecomunicación, aplicación de seguimiento en tiempo real de lanzamientos de cohetes. Tipos y subtipos de entidades afiliadas : LOG : Software

	El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información. LOG_APP : Aplicación profesional

2.2.2 LOG_OS : Sistema operativo

LOG_OS : Sistema operativo	
Tipo	LOG_OS : Sistema operativo
Descripción	Descripción : Esta denominación comprende todos los programas de un ordenador que constituyen la base operativa sobre la cual se ejecutarán todos los otros programas (servicios o aplicaciones). Incluye un núcleo y funciones o servicios básicos. Dependiendo de su arquitectura, un sistema operativo puede ser monolítico o puede estar formado por un micronúcleo y un conjunto de módulos del sistema. El sistema operativo abarca principalmente todos los servicios de gestión del hardware (CPU, memoria, discos, periféricos e interfaces redes), los servicios de gestión de tareas o procesos y los servicios de gestión de usuarios y de sus derechos. Ejemplos: GCOS, MVS, Solaris, Linux, Windows 95, Windows 2000, Windows XP, PalmOS, WCX, MacOS. Tipos y subtipos de entidades afiliadas : LOG : Software El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información.

2.2.3 LOG_SRV : Software de servicio, mantenimiento o gestión

LOG_SRV : Software de servicio, mantenimiento o gestión	
Tipo	LOG_SRV : Software de servicio, mantenimiento o gestión
Descripción	Descripción : Software que se caracteriza por el hecho de que completa los servicios del sistema operativo y que no está al servicio directo de los usuarios o de las aplicaciones (aunque a menudo es esencial o aún indispensable para el funcionamiento global del SI). Ejemplos: GCOS, MVS, Solaris, Linux, Windows 95, Windows 2000, Windows XP, PalmOS, WCX, MacOS. Tipos y subtipos de entidades afiliadas : LOG : Software El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información.

2.2.4 LOG_STD : Paquete de programas o software estándar

LOG_STD : Paquete de programas o software estándar	
Tipo	LOG_STD : Paquete de programas o software estándar
Descripción	Descripción : El software estándar o paquete de programas es un producto comercializado como tal (y no como desarrollo único o específico) con soporte, versión y mantenimiento. Presta un servicio « genérico » a los usuarios y a las aplicaciones pero no es personalizado o específico como la aplicación

profesional.

Ejemplos :

Software de gestión de base de datos, software de correo electrónico, software de colaboración, software de directorio, software de tipo servidor web…(Oracle, DB2, IIS, Apache, Lotus Notes, Exchange, OpenLDAP…).

Tipos y subtipos de entidades afiliadas :

LOG : Software
El tipo software está formado por el conjunto de programas que intervienen en el funcionamiento de un conjunto de procesos de tratamiento de la información.

2.3 RES : Red

RES: Red	
Tipo	RES: Red
Descripción	Descripción: El tipo red está formado por el conjunto de dispositivos de telecomunicación que permiten la interconexión de varios ordenadores o componentes de un sistema de información físicamente alejados.

2.3.1 RES_INF : Medios y soportes

RES_INF : Medios y soportes	
Tipo	RES_INF : Medios y soportes
Descripción	Descripción : Los medios o soportes de comunicación y telecomunicación pueden caracterizarse principalmente por las características físicas y técnicas del soporte (punto a punto, difusión) y por los protocolos de comunicación (enlace o red – capas 2 y 3 del modelo OSI de 7 capas). Ejemplos : RTC, Ethernet, GigabitEthernet, cable, fibra, ADSL sobre par de cobre, WiFi 802.11, BlueTooth, FireWire. Tipos y subtipos de entidades afiliadas : RES : Red El tipo red está formado por el conjunto de dispositivos de telecomunicación que permiten la interconexión de varios ordenadores o componentes de un sistema de información físicamente alejados.

2.3.2 RES_REL : Repetidor pasivo o activo

RES_REL : Repetidor pasivo o activo	
Tipo	RES_REL : Repetidor pasivo o activo
Descripción	Descripción : Este subtipo abarca todos los dispositivos que no son terminaciones lógicas de las comunicaciones (visión SI) sino intermediarios o repetidores. Dichos repetidores incluyen hardware pero también software específico. Se caracterizan por los protocolos de comunicación –red- soportados. A menudo abarcan, además del simple repetidor, funciones y servicios de encaminamiento (punto de conmutación de las comunicaciones) y/o filtrado (filtros en los enrutadores). Frecuentemente se administran en forma remota y a veces son capaces de generar trazas (registros). Ejemplos : Puente, enrutador, concentrador, switch, conmutador automático. Tipos y subtipos de entidades afiliadas : RES : Red El tipo red está formado por el conjunto de dispositivos de telecomunicación que permiten la interconexión de varios ordenadores o componentes de un sistema de información físicamente alejados.

2.3.3 RES_INT : Interfaz de comunicación

RES_INT : Interfaz de comunicación	
Tipo	RES_INT : Interfaz de comunicación

Descripción	Descripción : Las interfaces de comunicación de las unidades de tratamiento. Están vinculadas con la red, pero se caracterizan por los medios de comunicación y por los protocolos soportados, por las eventuales funciones y capacidades de filtrado, de generación de registros o de alertas y por la posibilidad y la necesidad de administración en forma remota. Ejemplos : Adaptador WiFi, GPRS, Ethernet. Tipos y subtipos de entidades afiliadas : RES : Red El tipo red está formado por el conjunto de dispositivos de telecomunicación que permiten la interconexión de varios ordenadores o componentes de un sistema de información físicamente alejados.

2.4 PER : Personal

PER: Personal	
Tipo	PER: Personal
Descripción	Descripción : El tipo personal está formado por el conjunto de grupos de individuos vinculados con el sistema de información.

2.4.1 PER_DEC : Nivel de toma de decisiones

PER_DEC : Nivel de toma de decisiones	
Tipo	PER_DEC : Nivel de toma de decisiones
Descripción	Descripción : Son los propietarios de los elementos esenciales (información y funciones) y los responsables jerárquicos en el seno de la organización o en el marco de un proyecto específico. Ejemplos : Dirección general, jefe de proyecto. Tipos y subtipos de entidades afiliadas : PER : Personal El tipo personal está formado por el conjunto de grupos de individuos vinculados con el sistema de información.

2.4.2 PER_UTI : Usuarios

PER_UTI: Usuarios	
Tipo	PER_UTI: Usuarios
Descripción	Descripción : Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas. Ejemplos : Dirección de Recursos Humanos, Dirección Financiera, gestor de riesgos. Tipos y subtipos de entidades afiliadas : PER : Personal El tipo personal está formado por el conjunto de grupos de individuos vinculados con el sistema de información.

2.4.3 PER_EXP : Operador del sistema – Mantenimiento

PER_EXP: Operador del sistema – Mantenimiento	
Tipo	PER_EXP: Operador del sistema – Mantenimiento
Descripción	Descripción: Es el personal encargado del funcionamiento y del mantenimiento del sistema de información. Dispone de privilegios particulares de acceso al sistema de información para asegurar sus tareas cotidianas. Ejemplos : Administrador del sistema, administrador de la base de datos, operador de respaldo de datos, servicio de asistencia técnica, desarrollador de aplicaciones, agentes de seguridad.

	Tipos y subtipos de entidades afiliadas :
	PER : Personal El tipo personal está formado por el conjunto de grupos de individuos vinculados con el sistema de información.

2.4.4 PER_DEV : Desarrollador

PER_DEV: Desarrollador	
Tipo	PER_DEV: Desarrollador
Descripción	Descripción : Es el personal encargado del desarrollo de las aplicaciones en el organismo. Accede a una parte del sistema de información con privilegios avanzados pero no actúa sobre los datos de producción. Ejemplos : Desarrolladores de aplicaciones profesionales. Tipos y subtipos de entidades afiliadas : PER : Personal El tipo personal está formado por el conjunto de grupos de individuos vinculados con el sistema de información.

2.5 PHY : Establecimiento

PHY: Standort	
Tipo	PHY: Establecimiento
Descripción	Descripción: ---------- El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.

2.5.1 PHY_LIE : Lugares

PHY_LIE: Lugares	
Tipo	PHY_LIE: Lugares
Descripción	Descripción : Perímetros, barreras físicas.

PHY_LIE.1 : Entorno externo	
Tipo	PHY_LIE.1 : Entorno externo
Descripción	Descripción : Se trata de todos los lugares en los cuales los medios de seguridad del organismo no pueden ser aplicados. Ejemplos : Domicilio del personal, instalaciones de otro organismo, entorno externo al establecimiento (zona urbana, zona de riesgo). Tipos y subtipos de entidades afiliadas : PHY : Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_LIE : Lugares Perímetros, barreras físicas.

PHY_LIE.2: Locales	
Tipo	PHY_LIE.2: Locales
Descripción	Descripción: ---------- Dicho lugar está delimitado por el perímetro del organismo directamente en contacto con el exterior. Puede tratarse de un perímetro de protección física que se obtiene creando barreras físicas o medios de vigilancia en torno a los edificios. Ejemplos: ---------- Establecimientos, edificios. Tipos y subtipos de entidades afiliadas: ---------- PHY: Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_LIE: Lugares Perímetros, barreras físicas.

PHY_LIE.3: Zona	
Tipo	PHY_LIE.3: Zona
Descripción	Descripción : Se trata de un perímetro de protección física que propone un cercado de las instalaciones en el organismo. Se obtiene creando barreras físicas en torno a infraestructuras de tratamiento de la información del organismo. Ejemplos : Oficinas, zona de acceso reservado, zona protegida. Tipos y subtipos de entidades afiliadas : PHY : Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_LIE : Lugares Perímetros, barreras físicas.

2.5.2 PHY_SRV : Servicio esencial

PHY_SRV: Servicio esencial	
Tipo	PHY_SRV: Servicio esencial
Descripción	Descripción: Conjunto de servicios necesarios para el funcionamiento del hardware en el organismo. Tipos y subtipos de entidades afiliadas: PHY: Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.

PHY_SRV.1 : Comunicación	
Tipo	PHY_SRV.1 : Comunicación
Descripción	Descripción : Servicios y equipo de telecomunicaciones brindados por un prestador. Ejemplos : Línea telefónica, centralita, redes telefónicas internas. Tipos y subtipos de entidades afiliadas : PHY : Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_SRV: Servicio esencial Conjunto de servicios necesarios para el funcionamiento del hardware en el organismo.

PHY_SRV.2: Energía	
Tipo	PHY_SRV.2: Energía
Descripción	Descripción: ---------- Servicios y medios (fuentes de energía y cableado) necesarios para la alimentación eléctrica del hardware y los periféricos. Ejemplos: ---------- Líneas de baja tensión, inversor, entrada de la red eléctrica.

	Tipos y subtipos de entidades afiliadas: ---------- PHY: Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_SRV: Servicio esencial Conjunto de servicios necesarios para el funcionamiento del hardware en el organismo.

PHY_SRV.3: Refrigeración - Contaminación

Tipo	PHY_SRV.3: Refrigeración - Contaminación
Descripción	Descripción: ---------- Servicios y medios (material, tubería) para refrigeración y purificación del aire. Ejemplos: ---------- Tubería de agua helada, sistemas de aire acondicionado. Tipos y subtipos de entidades afiliadas: ---------- PHY: Establecimiento El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento. PHY_SRV: Servicio esencial Conjunto de servicios necesarios para el funcionamiento del hardware en el organismo.

2.6 ORG : Organización

ORG: Organización	
Tipo	ORG: Organización
Descripción	Descripción: ---------- El tipo organización describe el marco organizacional, formado por todas las estructuras de personal afectadas a una tarea y los procedimientos que regulan dichas estructuras.

2.6.1 ORG_DEP : Organización de la cual depende el organismo

ORG_DEP: Organización de la cual depende el organismo	
Tipo	ORG_DEP: Organización de la cual depende el organismo
Descripción	Descripción: ---------- Se trata de organizaciones de las cuales depende el organismo estudiado, ya sea que esté jurídicamente vinculado con ellas o que sea externo a las mismas. El organismo estudiado está restringido, en términos de reglamentación, en cuanto a las decisiones, acciones o envío de informes. Ejemplos: ---------- Institución de tutela, sede de un organismo, Tribunal de Cuentas. Tipos y subtipos de entidades afiliadas: ---------- ORG El tipo organización describe el marco organizacional, formado por todas las estructuras de personal afectadas a una tarea y los procedimientos que regulan dichas estructuras.

2.6.2 ORG_GEN : Organización del organismo

ORG_GEN: Organización del organismo	
Tipo	ORG_GEN: Organización del organismo
Descripción	Descripción: ---------- Se trata de las distintas ramas del organismo subordinadas a su dirección, incluyendo sus actividades transversales. Ejemplos: ---------- Dirección de Recursos Humanos, Dirección Informática, Dirección de Compras, Direcciones Profesionales, Departamento de Seguridad de los Edificios, Departamento de Lucha Contra Incendios, Dirección de Auditorías. Tipos y subtipos de entidades afiliadas: ---------- ORG El tipo organización describe el marco organizacional, formado por todas las estructuras de personal afectadas a una tarea y los procedimientos que regulan dichas estructuras.

2.6.3 ORG_PRO : Organización de un proyecto o sistema

ORG_PRO: Organización de un proyecto o sistema	
Tipo	ORG_PRO: Organización de un proyecto o sistema

Descripción	Descripción: ---------- Se trata de la organización implementada para un proyecto o un servicio particular. Ejemplos: ---------- Organización del proyecto de desarrollo de una nueva aplicación, proyecto de migración del sistema de información. Tipos y subtipos de entidades afiliadas: ---------- ORG El tipo organización describe el marco organizacional, formado por todas las estructuras de personal afectadas a una tarea y los procedimientos que regulan dichas estructuras.

2.6.4 ORG_EXT : Subcontratistas - Proveedores - Industriales

ORG_EXT: Subcontratistas - Proveedores - Industriales	
Tipo	ORG_EXT: Subcontratistas - Proveedores - Industriales
Descripción	Descripción: ---------- Organización que brinda al organismo un servicio o recursos y que está vinculada a éste por contrato. Ejemplos: ---------- Empresa de gestión informática externalizada, empresa de externalización, empresa consultara. Tipos y subtipos de entidades afiliadas: ---------- ORG El tipo organización describe el marco organizacional, formado por toda la estructura del personal afectado a una tarea y los procedimientos que regulan dicha estructura.

2.7 SYS : Sistema

SYS: Sistema	
Tipo	SYS: Sistema
Descripción	Descripción: ---------- El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

2.7.1 SYS_INT : Dispositivo de acceso a Internet

SYS_INT: Dispositivo de acceso a Internet	
Tipo	SYS_INT: Dispositivo de acceso a Internet
Descripción	Descripción: ---------- Dispositivo que realiza la interconexión entre la red del organismo y la red Internet y que ofrece los servicios de acceso desde o hacia Internet. Ejemplos: ---------- Dispositivo de filtrado, DMZ, pasarelas. Tipos y subtipos de entidades afiliadas: ---------- SYS: Sistema El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

2.7.2 SYS_MES : Correo electrónico

SYS_MES: Correo electrónico	
Tipo	SYS_MES: Correo electrónico
Descripción	Descripción: ---------- Dispositivo que permite, a los usuarios habilitados, el ingreso, la consulta diferida y la transmisión de documentos informáticos o de mensajes electrónicos, a partir de ordenadores conectados en red. Ejemplos: ---------- Correo electrónico interno, correo electrónico vía web. Tipos y subtipos de entidades afiliadas: ---------- SYS: Sistema El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

2.7.3 SYS_ITR : Intranet

SYS_ITR: Intranet	
Tipo	SYS_ITR: Intranet

Descripción	Descripción: --- Datos y servicios informáticos compartidos y privados, que utilizan los protocolos y tecnologías de comunicación (por ejemplo, tecnología de Internet). Ejemplos: --- Servicio de información interna. Tipos y subtipos de entidades afiliadas: --- SYS: Sistema El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

2.7.4 SYS_ANU : Directorio de la empresa

SYS_ANU: Directorio de la empresa	
Tipo	SYS_ANU: Directorio de la empresa
Descripción	Descripción: --- Dispositivo de gestión y de acceso a una base de datos que describe al personal de la empresa y sus características. Ejemplos: --- Gestión de los derechos sobre las aplicaciones. Tipos y subtipos de entidades afiliadas: --- SYS: Sistema El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

2.7.5 SYS_WEB : Portal externo

SYS_WEB: Portal externo	
Tipo	SYS_WEB: Portal externo
Descripción	Descripción: --- Un portal externo es un punto de acceso que encontrará o utilizará un usuario cuando busque información o un servicio del organismo. Los portales brindan un gran abanico de recursos y de servicios. Ejemplos: --- Portal de información, portal para teleactividades, sitio de comercio electrónico. Tipos y subtipos de entidades afiliadas: --- SYS: Sistema El tipo sistema está formado por el conjunto de instalaciones específicas vinculadas con las tecnologías de la información, con un objetivo particular y un entorno operativo. Está compuesto por diversas entidades que pertenecen a los otros tipos arriba descritos.

3 Métodos de ataque y elementos peligrosos genéricos

El siguiente cuadro presenta los métodos de ataque con sus principales alcances sobre los criterios de seguridad. Los métodos de ataque se clasifican en función de un tema representativo (sin embargo, estos métodos podrían encontrarse al mismo tiempo en varios temas diferentes).

Métodos de ataque	Confidencialidad	Disponibilidad	Integridad
1 - Siniestros físicos			
01 - INCENDIO		X	X
02 - PERJUICIOS OCASIONADOS POR EL AGUA		X	X
03 - CONTAMINACIÓN		X	X
04 - SINIESTRO MAYOR		X	X
05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES		X	X
2 - Hechos naturales			
06 - FENÓMENO CLIMÁTICO		X	X
07 - FENÓMENO SÍSMICO		X	X
08 - FENÓMENO DE ORIGEN VOLCÁNICO		X	X
09 - FENÓMENO METEOROLÓGICO		X	X
10 - INUNDACIÓN		X	X
3 - Pérdida de servicios esenciales			
11- FALLAS EN LA CLIMATIZACIÓN		X	
12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA		X	
13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN		X	
4 - Perturbaciones provocadas por las radiaciones			
14 - EMISIONES ELECTROMAGNÉTICAS		X	X
15- RADIACIONES TÉRMICAS		X	X
16 - IMPULSOS ELECTROMAGNÉTICOS		X	X
5 - Compromiso de los datos			
17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS	X		
18 - ESPIONAJE A DISTANCIA	X	X	X
19 - ESCUCHA PASIVA	X		
20 - ROBO DE SOPORTES O DOCUMENTOS	X		
21 - ROBO DE HARDWARE	X	X	
22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	X		
23 - DIVULGACIÓN	X		
24 - INFORMACIÓN SIN GARANTÍA DEL ORIGEN		X	X
25 - SABOTAJE DEL HARDWARE	X		
26 - ALTERACIÓN DE PROGRAMAS	X	X	X
27 - GEOLOCALIZACIÓN	X		
6 - Fallas técnicas			
28 - AVERÍA DEL HARDWARE		X	
29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE		X	

30 - SATURACIÓN DEL SISTEMA INFORMÁTICO		X	
31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE		X	X
32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN		X	
7 - Acciones ilícitas			
33 - USO ILÍCITO DEL HARDWARE	X	X	X
34 - COPIA ILEGAL DE SOFTWARE	X		
35 - USO DE SOFTWARE FALSIFICADO O COPIADO		X	
36 - ALTERACIÓN DE DATOS	X		X
37 - TRATAMIENTO ILÍCITO DE LOS DATOS	X		
8 - Compromiso de las funciones			
38 - ERROR DE USO	X	X	X
39 - ABUSO DE DERECHO	X	X	X
40 - USURPACIÓN DE DERECHO	X	X	X
41 - NEGACIÓN DE ACCIONES			X
42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL		X	

Los métodos de ataque se describen en función de los elementos peligrosos que pueden utilizarlos.

Tema 1 – Siniestros físicos

01 - INCENDIO

Descripción	Tipo -------- Natural - Humano - Ambiental. Causa accidental ---------- Concentración de materiales inflamables o explosivos en un ambiente cerrado, que se prenden fuego debido a un hecho externo o un accidente interno. Ejemplos ---------- Rayo, incendio de una papelera, cortocircuito. Causa deliberada ---------- Terroristas, vándalos que acceden a los bienes para provocar directa o indirectamente (bombas incendiarias, alteración de los dispositivos de ventilación… el incendio) del material inflamable o explosivo. Ejemplos ---------- Huelguista que accede a los locales del organismo (por ejemplo, a través de las ventanas de la sala informática) para dejar allí un dispositivo incendiario. Tipo de consecuencias ---------- Destrucción del bien. Atentado contra la seguridad de las personas. Pérdidas financieras. Perturbación del funcionamiento interno.
Criterios afectados	Integridad Disponibilidad

02 - PERJUICIOS OCASIONADOS POR EL AGUA

Descripción	Tipo -------- Natural - Humano - Ambiental. Causa accidental ---------- Inundación que se debe a una pérdida o una ruptura de la tubería. Ejemplos ---------- Pérdidas de los equipos de aire acondicionado, pérdida que proviene del baño situado en el piso superior, mangueras contra incendios que se ha dejado abiertas. Causa deliberada ---------- Terroristas, vándalos que acceden al bien para provocar la inundación de los locales del organismo. Ejemplos ---------- Ruptura deliberada de la tubería, activación de sistemas de extinción o simplemente, materiales mojados.

	Tipo de consecuencias --- Destrucción o falta de disponibilidad temporaria de un bien. Pérdidas financieras. Alteración del funcionamiento interno.
Criterios afectados	Integridad Disponibilidad

03 - CONTAMINACIÓN

Descripción	Tipo --- Natural - Humano - Ambiental. Causa accidental --- Presencia de polvo, vapor, gases corrosivos o tóxicos en el aire. Ejemplos --- Gases de escape en una zona de intensa circulación. Causa deliberada --- Contaminación voluntaria del aire que altera el funcionamiento de los equipos de aire acondicionado o colocación de un foco de contaminación dentro de los locales. Ejemplos --- Acceso malicioso y colocación, en los conductos de aireación, de calefacción o de aire acondicionado, de un producto contaminante. Tipo de consecuencias --- Destrucción de un bien. Atentado contra la seguridad de las personas. Disponibilidad de personal operativo.
Criterios afectados	Integridad Disponibilidad

04 - SINIESTRO MAYOR

Descripción	Tipo --- Natural - Ambiental. Causa accidental --- Hecho externo o siniestro vinculado con el entorno natural o industrial cercano a los bienes y que puede afectarlos físicamente en forma muy importante. Ejemplos --- Explosión de establecimientos industriales situados en las cercanías, derrumbes de terreno, maremotos, caídas de aeronaves, móviles dañados o destruidos como consecuencia de una colisión. Causa deliberada --- Hecho externo o siniestro vinculado con una acción de vandalismo o de terrorismo cercana a los bienes y que puede afectarlos físicamente en forma

	muy importante. Ejemplos --- Explosión de establecimientos industriales situados en las cercanías, derrumbes de terreno, caídas de aeronaves, móviles dañados o destruidos como consecuencia de una colisión. Tipo de consecuencias --- Destrucción de un bien. Atentado contra la seguridad de las personas. Pérdidas financieras. Interrupción del funcionamiento.
Criterios afectados	Integridad Disponibilidad

05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES

Descripción	Tipo --- Humano. Causa accidental --- Negligencia o hecho accidental que provoca la destrucción de un hardware o de un soporte. Ejemplos --- Negligencia en la que se ha incurrido durante el transporte del hardware. Almacenamiento de soportes de archivo en malas condiciones ambientales. Daños causados por un animal. Derrame de alimentos o de bebidas sobre el hardware. Causa deliberada --- Persona que accede al hardware y que provoca su destrucción. Ejemplos --- Destrucción de una máquina y de sus copias de seguridad (cartucho). Tipo de consecuencias --- Pérdida de datos. Pérdidas financieras vinculadas con el valor del equipo destruido. Falta de disponibilidad del equipo.
Criterios afectados	Integridad Disponibilidad

Tema 2 – Hechos naturales

06 - FENÓMENO CLIMÁTICO

Descripción	Tipo -------- Natural. Causa accidental ---------- Condiciones climáticas particulares (cerca de los límites de funcionamiento del hardware). Ejemplos ---------- Establecimiento ubicado en una zona geográficamente sensible con condiciones extremas de calor, frío, humedad, viento y sequía. Tipo de consecuencias ---------- Destrucción de un bien o interrupción temporaria de su funcionamiento.
Criterios afectados	Integridad Disponibilidad

07 - FENÓMENO SÍSMICO

Descripción	Tipo -------- Natural. Causa accidental ---------- Sacudida sísmica o temblor que provoca vibraciones extremas o desencadena una catástrofe (maremoto). Ejemplos ---------- Establecimiento que aloja el sistema de información situado en una zona geográfica ocurren frecuentes movimientos sísmicos. Tipo de consecuencias ---------- Destrucción de un bien. Atentado contra la seguridad de las personas.
Criterios afectados	Integridad Disponibilidad

08 - FENÓMENO DE ORIGEN VOLCÁNICO

Descripción	Tipo -------- Natural. Causa accidental ---------- Erupción volcánica que provoca vibraciones o desencadena otra catástrofe (maremoto). Ejemplos ---------- Establecimiento que aloja el sistema de información situado en una zona geográfica considerada como volcánica (fenómeno intermitente, los períodos de

	actividad volcánica alternan con períodos de calma que pueden ser muy largos). Tipo de consecuencias ---------- Destrucción de un bien. Atentado contra la seguridad de las personas.
Criterios afectados	Integridad Disponibilidad

09 - FENÓMENO METEOROLÓGICO

Descripción	Tipo -------- Natural - Humano. Causa accidental ---------- Perturbación atmosférica puntual que ocasiona condiciones climáticas extremas. Ejemplos ---------- Temporales, huracanes, ciclones, granizo, rayos, avalanchas. Causa deliberada ---------- Un saboteador accede a los dispositivos de protección contra rayos. Ejemplos ---------- Desconexión de la descarga a tierra, cortocircuito en los descargadores de sobretensión, desplazamiento de los dispositivos. Tipo de consecuencias ---------- Destrucción de un bien. Atentado contra la seguridad de las personas.
Criterios afectados	Integridad Disponibilidad

10 - INUNDACIÓN

Descripción	Tipo -------- Natural. Causa accidental ---------- Río, corriente o napa subterránea que provoca una inundación de los terrenos cercanos en forma periódica o excepcionalmente. Ejemplos ---------- El establecimiento puede estar situado en una zona anegadiza y sufrir inundaciones debido a la cercanía de un río, o bien sufrir las consecuencias de dicha inundación aún encontrándose alejado (derrumbe del terreno). Tipo de consecuencias ---------- Destrucción de un bien. Atentado contra la seguridad de las personas. Pérdidas financieras.
Criterios afectados	Integridad

	Disponibilidad

Tema 3 – Pérdida de servicios esenciales

11- FALLAS EN LA CLIMATIZACIÓN

Descripción

Tipo

Humano - Ambiental.

Causa accidental

Un desperfecto, una interrupción o la insuficiencia del servicio de climatización pueden acarrear interrupciones de servicio, fallas de funcionamiento o incluso averías de los bienes que requieren refrigeración y ventilación.

Ejemplos

Falta de mantenimiento de los equipos de aire acondicionado, dimensionamiento inadecuado de dicho equipamiento, interrupción del suministro de agua por parte del proveedor.

Causa deliberada

Una persona puede sabotear los elementos necesarios para el buen funcionamiento del dispositivo de climatización (interrupción del aprovisionamiento de agua o de energía eléctrica, destrucción del dispositivo).

Ejemplos

Interrupción de la climatización, interrupción del aprovisionamiento de agua.

Tipo de consecuencias

Alteración de bienes.

Criterios afectados

Disponibilidad

12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA

Descripción

Tipo

Humano - Ambiental.

Causa accidental

Corte, interrupción o dimensionamiento inadecuado del suministro de energía de los bienes que proporcionados por el proveedor del servicio o de los dispositivos internos de distribución.

Ejemplos

Interrupción del servicio de la empresa proveedora de electricidad por huelgas, inconvenientes técnicos, trabajos en curso.
Problemas o dimensionamiento inadecuado de la central eléctrica interna o de la red eléctrica auxiliar cuando existen dichas instalaciones.
Conexión no prevista de equipos de gran potencia a la red auxiliar, lo que provoca una insuficiencia de los equipos de emergencia.
Problemas de mantenimiento o envejecimiento de las baterías del inversor.
Corte accidental de cables internos o externos.
Interrupción del aprovisionamiento de agua (problema del proveedor, anomalía interna como, por ejemplo, alguna negligencia).

Causa deliberada

	Sabotaje o perturbación de la instalación eléctrica por parte de una persona que accede a los dispositivos (entrada de línea, transformador de baja tensión, inversor...). Ejemplos --- Corte voluntario de los cables de la instalación del proveedor de energía eléctrica, interrupción voluntaria del aprovisionamiento de agua. Tipo de consecuencias --- Interrupción temporaria del servicio eléctrico, del servicio de climatización.
Criterios afectados	Disponibilidad

13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN

Descripción	Tipo --- Humano - Ambiental. Causa accidental --- Perturbación, interrupción o dimensionamiento inadecuado de los servicios de telecomunicación (teléfono, accesos a Internet, red Internet). Ejemplos --- Huelgas, hecho exterior excepcional que provoca la saturación de las comunicaciones. Causa deliberada --- Sabotaje o perturbación de la instalación de servicios de telecomunicación por parte de una persona que accede a los dispositivos de telecomunicaciones (cabecera de línea, centralita, repartidor, cables externos...). Ejemplos --- Corte voluntario de los cables de telecomunicación, destrucción de una central de telecomunicación externa, saturación voluntaria del ancho de banda del proveedor. Tipo de consecuencias --- Interrupción de corta o larga duración de los servicios de telecomunicación. Pérdidas financieras.
Criterios afectados	Disponibilidad

Tema 4 – Perturbaciones provocadas por las radiaciones

14 - EMISIONES ELECTROMAGNÉTICAS

Descripción

Tipo

Humano - Ambiental.

Causa accidental

Perturbaciones electromagnéticas vinculadas con un equipo interno o externo.

Ejemplos

Radar, antena de radio, central eléctrica, máquina de mecanizado.

Causa deliberada

Persona que utiliza las señales parásitas emitidas para interferir o saturar las comunicaciones o para perturbar el funcionamiento de los aparatos.

Ejemplos

Interferencia de comunicación WiFi.

Tipo de consecuencias

Alteración de la visualización de los monitores catódicos, interferencia en las comunicaciones.
Alteración, perturbación de funcionamiento.

Criterios afectados

Integridad
Disponibilidad

15- RADIACIONES TÉRMICAS

Descripción

Tipo

Humano - Natural - Ambiental.

Causa accidental

Efecto térmico provocado por un siniestro o por condiciones meteorológicas excepcionales.

Ejemplos

Incendio de bosque que provoca que el hardware se encuentre en condiciones ambientales que exceden sus límites de funcionamiento.

Causa deliberada

Dispositivo que provoca un efecto térmico y que acarrea fallas en el funcionamiento del hardware o su destrucción.

Ejemplos

Colocación de desechos nucleares cerca del sistema de información, explosión termonuclear.

Tipo de consecuencias

Falla de funcionamiento o destrucción del hardware.

	Atentado contra la seguridad de las personas. Pérdidas financieras.
Criterios afectados	Integridad Disponibilidad

16 - IMPULSOS ELECTROMAGNÉTICOS

Descripción	Tipo -------- Ambiental. Causa accidental ---------- Siniestro que provoca un efecto electromagnético excepcional. Ejemplos ---------- Accidente industrial cerca del establecimiento. Causa deliberada ---------- Impulsos electromagnéticos de origen nuclear. Ejemplos ---------- Bombas. Tipo de consecuencias ---------- Destrucción del bien. Pérdidas financieras.
Criterios afectados	Integridad Disponibilidad

Tema 5 – Compromiso de los datos

17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

Descripción

Tipo

Humano.

Causa deliberada

Señales parásitas de origen electromagnético emitidas por el hardware (por conducción a través de los cables de suministro eléctrico o de las conexiones a masa, o por emisión en espacios abiertos).
La captura de dichas señales depende de la distancia existente hasta el equipo al que se apunta o de la posibilidad de conectarse al cableado o a cualquier otro conductor que pase cerca (fenómeno de acoplamiento).

Ejemplos

Espía o pirata que intercepta y registra señales electromagnéticas con ayuda de sensores y de hardware electrónico a través de las tuberías.
Espía o pirata que intercepta o registra señales electromagnéticas que provienen de la emisión de video de un puesto informático.

Tipo de consecuencias

Divulgación de las comunicaciones o de los procesos.

Criterios afectados

Confidencialidad

18 - ESPIONAJE A DISTANCIA

Descripción

Tipo

Humano.

Causa deliberada

Acciones del personal que pueden ser observadas en forma remota.

Ejemplos

Observación visual con o sin medio óptico, por ejemplo, observación de un usuario que ingresa un código o una contraseña en un teclado.

Tipo de consecuencias

Intrusión.
Usurpación de identidad.

Criterios afectados

Integridad
Confidencialidad
Disponibilidad

19 - ESCUCHA PASIVA

Descripción

Tipo

Humano.

Causa deliberada

Persona conectada a los equipos o a los soportes de comunicación o ubicada dentro del perímetro de alcance de la emisión de una comunicación. Utiliza

	algunos medios, que pueden ser costosos, para escuchar, copiar y analizar la información transmitida (voz o datos). Ejemplos ---------- La interceptación puede centrarse en señales de tipo hertziano o por canales. La interceptación se realiza mediante sensores (por ejemplo, para el tipo hertziano, una antena). Ésta puede tener lugar en comunicaciones por infrarrojo. En el caso de un medio cableado, se puede utilizar un equipo ya conectado a la red (por ejemplo, estación de trabajo situada en una red local), para almacenar y analizar los datos transmitidos (por ejemplo, datos que se intercambian con un servidor). Muchos aparatos comerciales facilitan los análisis y permiten interpretar en tiempo real las tramas, cualesquiera sean los protocolos de comunicación Tipo de consecuencias ---------- Divulgación de la información que circula en un soporte de comunicación.
Criterios afectados	Confidencialidad

20 - ROBO DE SOPORTES O DOCUMENTOS

Descripción	Tipo -------- Humano. Causa deliberada ---------- Persona perteneciente o ajena al organismo que accede al soporte digital o a documentos en papel con el fin de robar y aprovechar los datos que allí se encuentran. Ejemplos ---------- Robo de disquetes, CD-ROM, cartuchos, cintas de respaldo. Robo de documentación, notas, planos, informes. Robo de impresiones dejadas momentáneamente en impresoras ubicadas en ambientes compartidos. Búsqueda en papeleros, basureros dejados en la vía pública. Tipo de consecuencias ---------- Divulgación de información (patrimonio, contraseña).
Criterios afectados	Confidencialidad

21 - ROBO DE HARDWARE

Descripción	Tipo -------- Humano. Causa deliberada ---------- Persona perteneciente o ajena al organismo que tiene acceso al hardware, ubicado en el organismo o fuera de él, con un objetivo de lucro o estratégico. Ejemplos ---------- Robo de microordenador portátil para revender el hardware, robo de un PDA (asistente personal digital) para utilizar su contenido. Tipo de consecuencias

	---------- Falta de disponibilidad de datos y/o funciones (por ejemplo, equipo portátil dedicado para el mantenimiento). Divulgación de datos almacenados por el equipo (por ejemplo: contraseña, parte del patrimonio de información). Pérdidas financieras.
Criterios afectados	Confidencialidad Disponibilidad

22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS

Descripción	Tipo -------- Humano Causa accidental ---------- Recuperación de soportes electrónicos (discos duros, disquetes, cartuchos para respaldo, llaves USB, disquetes ZIP, discos duros extraíbles...) o papel (listados impresos, impresiones incompletas, mensajes...) destinados al reciclado y que contienen datos recuperables. Ejemplo ---------- Reciclado de ordenadores cuyos discos duros no han sido formateados y que han sido destinados a otros usuarios del mismo organismo, de escuelas, de otros organismos. Reutilización de papeles como borradores dentro o fuera del organismo. Causa deliberada ---------- Recuperación de soportes electrónicos (discos duros, disquetes, cartuchos de respaldo, llaves USB, disquetes ZIP, discos duros extraíbles...) o papel (listados impresos, impresiones incompletas, mensajes...) destinados a la destrucción y que contienen datos recuperables. Ejemplo ---------- Búsqueda en papeleros, basureros dejados en la vía pública. Tipo de consecuencias ---------- Pérdida de imagen de marca. Divulgación de información.
Criterios afectados	Confidencialidad

23 - DIVULGACIÓN

Descripción	Tipo -------- Humano. Causa accidental ---------- Persona perteneciente al organismo que, por negligencia, divulga información a otras personas dentro del organismo o a terceros que tienen necesidad de conocerla (generalmente, las consecuencias son más importantes cuando la información se divulga fuera del organismo). Ejemplos ---------- Error de destinatarios durante el envío de mensajes. Respuesta a peticiones sin verificar el origen de éstas (pedido malicioso de

	contraseñas). Desconocimiento de las normas de difusión de la información que se aplican en el organismo. Negligencia cometida en la definición de las normas de control de acceso a la información compartida. Incumplimiento de las normas elementales de discreción (discusión o lectura de documentos en lugares públicos). Causa deliberada --- Persona que, concientemente, divulga información dentro del organismo o a terceros que no tienen necesidad de conocerla (generalmente, las consecuencias son más importantes cuando la información se divulga fuera del organismo). Ejemplos --- Persona que, por venganza, difunde información confidencial a través de el correo electrónico. Persona que divulga información ya que considera que la posesión de información delicada le da cierto poder sobre los demás. Difusión de información a un tercero bajo presión de chantaje. Usufructo financiero de información industrial o comercial (espionaje industrial). Tipo de consecuencias --- Violación de la privacidad de los usuarios. Divulgación del patrimonio de información. Pérdidas financieras.
Criterios afectados	Confidencialidad

24 - INFORMACIÓN SIN GARANTÍA DEL ORIGEN

Descripción	Tipo --- Humano. Causa accidental --- Recepción y uso, en el sistema de información del organismo, de datos erróneos o de hardware no adaptado que proviene de fuentes externas. Ejemplos --- Informaciones que provienen de un foro de discusión. Descarga de actualizaciones en sitios de Internet que no pertenecen al editor correspondiente. Información recibida sin identificación o autenticación de su emisor, por ejemplo, recepción de correo electrónico enviado con una identificación genérica de una empresa (soporte@empresa.com). Causa deliberada --- Persona que envía información falsa, destinada a ser incorporada al sistema de información, para desinformar al destinatario y dañar la fiabilidad del sistema o la validez de sus datos. Ejemplos --- Transmisión de bromas ("mensajes falsos en cadena") a través del correo electrónico. Persona que envía datos haciéndose pasar por la fuente legítima.

	Tipo de consecuencias --- Alteración de datos, incluso de procesos. Consumo inútil de recursos humanos. Pérdida de la imagen de marca.
Criterios afectados	Integridad Disponibilidad

25 - SABOTAJE DEL HARDWARE

Descripción	Tipo --- Humano. Causa deliberada --- Persona que accede a un soporte de comunicación o a un equipo para colocar allí un mecanismo de interceptación o de destrucción. Ejemplos --- Inserción de una tarjeta en un microordenador durante el transporte de éste. Colocación de un micrófono en un equipo. Desviación de circuitos de comunicación de voz o datos. Sabotaje de una función de un hardware de protección para inutilizarlo y llevar a cabo un ataque. Tipo de consecuencias --- Divulgación de información fuera del organismo. Destrucción del hardware durante un período crítico. Ineficacia de una función de protección.
Criterios afectados	Confidencialidad

26 - ALTERACIÓN DE PROGRAMAS

Descripción	Tipo --- Humano - Ambiental. Causa accidental --- Acción involuntaria realizada con medios lógicos desde dentro o fuera del organismo y que provocan la alteración o la destrucción de programas o datos, con el objetivo de alterar el buen funcionamiento del recurso o de ejecutar comandos en nombre de los usuarios y sin que éstos se enteren. Ejemplos --- Usuario que conecta a la red un microordenador portátil infectado con un virus, introducido durante un intercambio con otro organismo. Usuario del sistema de información que recibe un gusano desde fuera del organismo y lo propaga, sin saberlo, dentro de éste. Causa deliberada --- El agresor introduce un programa o determinados comandos para modificar el comportamiento de un software o agregar un servicio ilícito a un sistema operativo. Dicho elemento peligroso puede actuar durante las fases de diseño, preproducción, fabricación, uso, transporte o mantenimiento del sistema de información. Ejemplos

	---------- Persona que hace ejecutar a un usuario un programa que simula una acción lícita pero que contiene funciones escondidas capaces de afectar la política de seguridad (troyano). Bomba lógica que se agrega a un programa con el fin de insertar allí un comando, asociada generalmente a algo que la desencadena (fecha, hecho contextual) y que ejecuta una acción ilícita. Tipo de consecuencias ---------- Intrusión. Alteración del funcionamiento. Destrucción de datos. Alteración de programas.
Criterios afectados	Integridad Confidencialidad Disponibilidad

27 - GEOLOCALIZACIÓN

Descripción	Tipo -------- Humano. Causa deliberada ---------- Persona que tiene acceso a medios que permiten localizar a un usuario del sistema de información. Ejemplos ---------- Acceso a los registros de entrada/salida. Acceso a los pedidos de pasajes. Utilización de antenas a las cuales se conectan los teléfonos móviles cuando están en funcionamiento, con el fin de localizar a una persona. Tipo de consecuencias ---------- Uso de la información para llevar a cabo ataques orientados.
Criterios afectados	Confidencialidad

Tema 6 – Fallas técnicas

28 - AVERÍA DEL HARDWARE

Descripción	Tipo -------- Humano - Natural. Causa accidental ---------- Hecho que provoca el fallo de un hardware. Ejemplos ---------- Desgaste, envejecimiento, falta de mantenimiento o uso incorrecto (por ejemplo, dimensionamiento inadecuado, uso fuera de los límites de funcionamiento) que provoca un funcionamiento no conforme. Tipo de consecuencias ---------- Falta de disponibilidad de un equipo. Alteración o pérdida de datos.
Criterios afectados	Disponibilidad

29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE

Descripción	Tipo -------- Humano / Natural. Causa accidental ---------- Hecho lógico o físico que provoca fallas en el funcionamiento del hardware. Ejemplos ---------- Incumplimiento de los procedimientos de calificación de un equipo tras la realización de actualizaciones o modificaciones retroactivas. Degradación involuntaria de un equipo. Uso del hardware en condiciones que exceden los límites de funcionamiento propios del equipo (temperatura, humedad). Desgaste, envejecimiento del hardware. Tipo de consecuencias ---------- Interrupción del servicio de un equipo que, por efecto secundario, puede llevar a la falta de disponibilidad del sistema de información.
Criterios afectados	Disponibilidad

30 - SATURACIÓN DEL SISTEMA INFORMÁTICO

Descripción	Tipo -------- Humano. Causa accidental ---------- Recurso de tipo hardware, software o red, insuficiente para enfrentar las necesidades de los usuarios. Ejemplos ----------

	Superación de las capacidades de almacenamiento (por ejemplo: espacio para copias de seguridad, almacenamiento en buzones de correo electrónico, espacio de trabajo...), por ejemplo, saturación de un buzón de correo electrónico durante la ausencia prolongada de su propietario. Saturación vinculada con la enorme demanda de la máquina (múltiples peticiones que deben procesarse en forma simultánea). Dimensionamiento inadecuado de los equipos (inversores, canales de comunicación...). Causa deliberada --- Persona que simula una necesidad de recurso intenso provocando una interferencia intensa y continua del recurso. Ejemplos --- Ejecución de una gran cantidad de comandos simultáneos. Saturación voluntaria de los espacios destinados al almacenamiento de las trazas de actividades de los sistemas o aplicaciones con miras a enmascarar la realización de operaciones ilícitas. Tipo de consecuencias --- Interrupción que provoca la falta de disponibilidad temporaria del servicio. Pérdida de información.
Criterios afectados	Disponibilidad

31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE

Descripción	Tipo --- Humano - Ambiental. Causa accidental --- Error de diseño, error de instalación o negligencia durante una modificación que provoca un fallo del software. Ejemplos --- Error de implementación que acarrea un procesamiento inadecuado de los datos delimitados. Instalación de software que provoca efectos de límite. Incumplimiento de los procedimientos de instalación o de gestión. Negligencia cometida durante las operaciones de mantenimiento. Tipo de consecuencias --- Interrupción de servicio. Alteración de funcionamiento. Producción de datos alterados.
Criterios afectados	Integridad Disponibilidad

32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN

Descripción	Tipo --- Humano - Ambiental. Causa accidental --- Falta de control del sistema que acarrea la imposibilidad de efectuar cualquier

	modificación retroactiva o evolución, por ejemplo, para corregir una anomalía, para responder a nuevas necesidades. Ejemplos ---------- Fallo provocado por los proveedores del hardware y del software. Fallos de terceras empresas de mantenimiento de software y hardware, interrupción de contrato de prestación de servicios que provoca una falta de capacidad técnica o de medios para garantizar la evolución del sistema. Numerosas modificaciones realizadas en el sistema hacen difícil, incluso imposible, su mantenimiento sin correr el riesgo de provocar efectos secundarios tras una modificación. Causa deliberada ---------- Persona que obstaculiza, o incluso imposibilita, cualquier actualización del sistema. Ejemplos ---------- Persona que, como venganza, no deja ninguna traza ni siquiera de ayuda para el mantenimiento del sistema (volviéndolo poco transparente). Tipo de consecuencias ---------- Interrupción de servicio prolongada. Perjuicio a la seguridad de funcionamiento. Pérdidas financieras vinculadas con el cambio de materiales o de proveedores.
Criterios afectados	Disponibilidad

Tema 7 – Acciones ilícitas

33 - USO ILÍCITO DEL HARDWARE

Descripción

Tipo

Humano.

Causa deliberada

Persona perteneciente o ajena al organismo que tiene acceso al sistema de información y que utiliza uno de los servicios para introducirse en él y efectuar operaciones o robar información.

Ejemplos

Robo de datos de identificación/autenticación de un usuario autorizado a fin de arrogarse los derechos para evitar los controles de acceso.
Ingreso a zonas protegidas a partir de un acceso autorizado utilizando una falla en los mecanismos de aplicación para evitar los medios de protección.
Examen y búsqueda de información en datos residuales en soportes electrónicos (fichero de memoria escondido, fragmentos de datos residuales en discos duros, respaldos del entorno de ejecución -puntos de recuperación en caso de incidente- que contienen información sobre el estado del sistema y pueden ser consultados por un atacante informado.
Simulación del comportamiento de una máquina para engañar a un usuario legítimo y apoderarse de su nombre y de su contraseña.
Modificación o destrucción voluntaria de datos

Tipo de consecuencias

Intrusión en el sistema de información.
Divulgación de información.

Criterios afectados

Integridad
Confidencialidad
Disponibilidad

34 - COPIA ILEGAL DE SOFTWARE

Descripción

Tipo

Humano.

Causa deliberada

Persona perteneciente al organismo que realiza copias ilegales "caseras" (llamadas también copias piratas) de paquetes de programas o de software.

Ejemplos

Copia de software del organismo con un fin lúdico, de venganza (difusión vía Internet) o lucrativo (venta).

Tipo de consecuencias

Pérdidas financieras.
Daño a la imagen de marca.

Criterios afectados

Confidencialidad

35 - USO DE SOFTWARE FALSIFICADO O COPIADO

Descripción

Tipo

	-------- Humano - Ambiental. Causa accidental ---------- Pérdida o destrucción de los elementos que prueban la compra de licencias o negligencia cometida en el desarrollo del software al no pagar los derechos correspondientes. Ejemplos ---------- Siniestro que provoca la destrucción de las pruebas de la compra. Imposibilidad de conformar un inventario de las licencias utilizadas. Causa deliberada ---------- Persona perteneciente al organismo que utiliza un software copiado de manera ilícita. Ejemplos ---------- Copia de software sin licencia para realizar una tarea lícita en el organismo. Tipo de consecuencias ---------- Incumplimiento de la legislación. Daño a la imagen de marca.
Criterios afectados	Disponibilidad

36 - ALTERACIÓN DE DATOS

Descripción	Tipo -------- Humano. Causa deliberada ---------- Persona que accede a los medios de comunicación del sistema de información y altera el envío de datos (interceptación, inserción, destrucción...) o requiere esos accesos hasta encontrar uno autorizado. Ejemplos ---------- Destrucción, inserción, modificación de mensajes (modificación de la información, reacomodación de los datos dentro de los mensajes o en la respuesta de dichos mensajes). Rechazo de servicio (mensaje retrasado). Exploración desde el interior de las direcciones IP hasta encontrar una dirección accesible del sistema de información. Tipo de consecuencias ---------- Intrusión. Alteración de las comunicaciones.
Criterios afectados	Integridad Confidencialidad

37 - TRATAMIENTO ILÍCITO DE LOS DATOS

Descripción	Tipo -------- Humano.

	Causa deliberada --- Persona que realiza un procesamiento de información no autorizado por la legislación o reglamentación. Exemples --- Constitución y uso de fichero personal no declarado (gestión ilícita de trazas). Realización de operaciones prohibidas en ficheros personales declarados, como, por ejemplo, la comparación de varios ficheros. Cifrado de datos con fines de confidencialidad utilizando claves largas sin autorización previa. Manipulación ilícita de datos de un ordenador reciclado. Tipo de consecuencias --- Violación de la privacidad de los usuarios. Acciones legales y multas.
Criterios afectados	Confidencialidad

Tema 8 – Compromiso de las funciones

38 - ERROR DE USO

Descripción	Tipo -------- Humano. Causa accidental ---------- Persona que comete un error de manipulación, de ingreso de datos o de uso del hardware o del software. Ejemplos ---------- Pérdida de datos como consecuencia de un error en las operaciones de respaldo. Incumplimiento de los procedimientos de instalación o de mantenimiento. Ingreso de gran cantidad de datos cifrados mediante la consola. Negligencia cometida durante la configuración de un software de protecciónn. Error en el ingreso de la dirección del destinatario de un correo electrónico. Tipo de consecuencias ---------- Interrupción de servicio. Alteración de los datos. Falla de funcionamiento, pérdida de la eficacia de los medios de protección, introducción de fallas adicionales Divulgación involuntaria de datos.
Criterios afectados	Integridad Confidencialidad Disponibilidad

39 - ABUSO DE DERECHO

Descripción	Tipo -------- Humano. Causa accidental ---------- Persona que posee permisos especiales (administrador de redes, personal informático...) y que puede modificar las características de gestión de los recursos sin informar de ello a los usuarios. Ejemplos ---------- Creación de nuevos accesos a los sistemas sin tener en cuenta las necesidades de protección de los datos almacenados por los usuarios. Interrupción del procedimiento de respaldo sin informar de ello a los usuarios. Modificación de los parámetros de configuración en servidores, provocando efectos secundarios y fallas de funcionamiento. Causa deliberada ---------- Persona que accede al sistema para modificar, suprimir y agregar características de gestión o realizar cualquier otra operación ilícita que sea posible gracias a la atribución de dichos derechos. Ejemplos ---------- Un administrador cambia las contraseñas de los usuarios.

	Personal que realiza mantenimiento del SI modifica el comportamiento de los mecanismos de seguridad para acceder a información protegida. Supresión del registro de acontecimientos en los servidores de aplicación. Tipo de consecuencias ---------- Alteración de funcionamiento. Divulgación de información. Pérdida de información.
Criterios afectados	Integridad Confidencialidad Disponibilidad

40 - USURPACIÓN DE DERECHO

Descripción	Tipo -------- Humano. Causa deliberada ---------- Persona que se hace pasar por otra para utilizar dichos privilegios de acceso al sistema de información, desinformar al destinatario, realizar un fraude... Ejemplos ---------- Persona que se hace pasar por un usuario y solicita al administrador un nuevo acceso luego de la pérdida de su contraseña. Persona que toma el lugar de un usuario utilizando una sesión que éste ha dejado abierta. Tipo de consecuencias ---------- Intrusión.
Criterios afectados	Integridad Confidencialidad Disponibilidad

41 - NEGACIÓN DE ACCIONES

Descripción	Tipo -------- Humano. Causa deliberada ---------- Una persona o una entidad niega su participación en una comunicación con un tercero o en la realización de una operación. Ejemplos ---------- Persona que niega haber recibido o emitido un mensaje determinado, o que dice haber emitido (o recibido) un mensaje (fichero) diferente, o que pretende no haber realizado nunca determinada operación. Tipo de consecuencias ---------- Falta de pruebas.
Criterios afectados	Integridad

42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL

Descripción	Tipo

	-------- Humano - Ambiental. Causa accidental ---------- Ausencia de personal calificado o autorizado como consecuencia de un inconveniente involuntario. Ejemplos ---------- Enfermedad, fallecimiento, huelga de transporte. Causa deliberada ---------- Ausencia voluntaria de personal calificado o autorizado. Ejemplos ---------- Huelgas, feriados no advertidos por el organismo. Tipo de consecuencias ---------- Interrupción, perturbación del servicio.
Criterios afectados	Disponibilidad

4 Vulnerabilidades genericas

Las vulnerabilidades se organizan en función de los métodos de ataque y presentan los tipos y subtipos de entidades involucrados. Los subtipos de entidades heredan las vulnerabilidades del tipo de entidad al que corresponden.

4.1 INCENDIO

Ejemplar único de las licencias	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP.1: Aplicación profesional estándar
Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_APP.2: Aplicación profesional específica
Falta de hardware de repuesto	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware que utiliza materiales inflamables (por ej.: impresoras de gran capacidad que ocasionan polvo)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de respaldo de los datos contenidos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes originales	
Tipos de entidades	MAT_PAS.2: Otros soportes
Falta de cobertura de seguridad en caso de siniestro grave	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización
No asistencia al establecimiento de los servicios de emergencia (bomberos)	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales para el restablecimiento de las actividades, aplicables en caso de crisis declarada en el establecimiento del proveedor	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones de seguridad para el personal externo que trabaja dentro del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de gestión de los informes de control de los equipos de emergencia	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de estructura para combatir los incendios (descripción de los roles, responsabilidades)	

Tipos de entidades	ORG_GEN: Organización del organismo
Falta de seguimiento de los contratos de mantenimiento de los dispositivos de protección contra incendios	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de una estructura de gestión de crisis	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre la protección de los dispositivos de seguridad	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Presencia de aberturas que dan a la vía pública (ventanas)	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
Antigüedad de los locales	
Tipos de entidades	PHY_LIE.2: Locales
Falta de control de acceso al establecimiento o a los locales de éste	
Tipos de entidades	PHY_LIE.2: Locales
Falta de aislamiento antifuego	
Tipos de entidades	PHY_LIE.2: Locales
Falta de consideración, durante la fase de instalación, de los riesgos contra incendios específicos de los equipos alojados	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona
Ausencia o dimensionamiento inadecuado del dispositivo automático de extinción de incendios	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona
Falta de mantenimiento de los equipos de aire acondicionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 01 - INCENDIO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet

	SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.2 PERJUICIOS OCASIONADOS POR EL AGUA

Ejemplar único de las licencias	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP.1: Aplicación profesional estándar
Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_APP.2: Aplicación profesional específica
Falta de hardware de repuesto	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de respaldo de los datos contenidos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes originales	
Tipos de entidades	MAT_PAS.2: Otros soportes
Falta de cobertura de seguridad en caso de siniestro grave	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada del subcontratista o proveedor	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones de seguridad para el personal externo que trabaja dentro del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de gestión de los informes de control de los equipos de emergencia	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de instrucciones de alerta, de reacción, de información en caso de perjuicios ocasionados por el agua (Falta de identificación de llaves de paso,...)	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de garantía de buen funcionamiento de los detectores de presencia de agua	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de estructura de gestión de crisis	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal

Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre la protección de los dispositivos de seguridad	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Establecimiento ubicado en una zona anegadiza	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control en los accesos físicos a los locales	
Tipos de entidades	PHY_LIE.2: Locales
Aberturas no herméticas que dan al exterior	
Tipos de entidades	PHY_LIE.2: Locales
Presencia aspersores	
Tipos de entidades	PHY_LIE.2: Locales
Techos o aberturas no herméticas que dan al exterior	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona
Falta de identificación clara de las llaves de paso del agua	
Tipos de entidades	PHY_LIE.3: Zona
Acceso no protegido	
Tipos de entidades	PHY_LIE.3: Zona
Tubería de agua cerca de los equipos	
Tipos de entidades	PHY_LIE.3: Zona
Aspersores	
Tipos de entidades	PHY_LIE.3: Zona
Tubería de agua cerca de las terminales	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona
Falta de sumidero	
Tipos de entidades	PHY_LIE.3: Zona
Acceso no protegido a los locales que alojan equipos de producción o distribución de los servicios esenciales	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Cableado colocado en el suelo	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Antigüedad de los conductos de refrigeración	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Falta de mantenimiento de los equipos de aire acondicionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación

Falta de llave de paso del agua	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 02 - PERJUICIOS OCASIONADOS POR EL AGUA	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.3 CONTAMINACIÓN

Ejemplar único de las licencias	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP.1: Aplicación profesional estándar
Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_APP.2: Aplicación profesional específica
Soporte sensible a las condiciones de conservación	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de seguimiento de los contratos de mantenimiento	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de determinación de las medidas que deben adoptarse en caso de interrupción del servicio de climatización	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre la protección de los equipos de seguridad	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Proximidad de fuentes de contaminación (ruido, humo, vapor...)	
Tipos de entidades	PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Atmósfera contaminada (hangar, taller...)	
Tipos de entidades	PHY_LIE.2: Locales
Falta de mantenimiento de los equipos de aire acondicionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Falta de hardware redundante correctamente dimensionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Antigüedad de los filtros de climatización	

Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Acceso no protegido a los equipos	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 03 - CONTAMINACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.4 SINIESTRO MAYOR

Ejemplar único de las licencias	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP.1: Aplicación profesional estándar
Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_APP.2: Aplicación profesional específica
Falta de hardware de repuesto	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de respaldo de los datos contenidos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes originales	
Tipos de entidades	MAT_PAS.2: Otros soportes
Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de información actualizada a la vista con las instrucciones para llamar a los servicios de emergencia	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de cobertura de seguridad en caso de siniestro grave	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de estructura de gestión de crisis	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de procedimientos de gestión de situaciones de emergencia	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento
Posibilidades de destrucción causada por un hecho externo (colisiones, atentados)	
Tipos de entidades	PHY_LIE.1: Entorno externo
Proximidad de actividad industrial o establecimiento de riesgo	
Tipos de entidades	PHY_LIE.1: Entorno externo
Locales donde los riesgos de explosión/implosión no han sido tenidos en cuenta	
Tipos de entidades	PHY_SRV: Servicio esencial

	PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 04 - SINIESTRO MAYOR	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.5 DESTRUCCIÓN DE HARDWARE O DE SOPORTES

Ejemplar único de las licencias	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP.1: Aplicación profesional estándar
Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_APP.2: Aplicación profesional específica
Falta de hardware de repuesto	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Fragilidad del hardware	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware accesible a otras personas que no sean los propietarios (ej.: ubicado en un lugar de paso)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Soporte accesible a otras personas que no sean los propietarios	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de procedimiento de archivado	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Fragilidad de los soportes	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Ausencia de medidas de conservación de los archivos adaptadas a los plazos de conservación (antigüedad de las cintas magnéticas, desgaste del CD-ROM)	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de respaldo de los datos contenidos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes originales	
Tipos de entidades	MAT_PAS.2: Otros soportes
Falta de instrucciones para el personal externo que trabaja dentro del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de cobertura de seguridad en caso de destrucción de hardware	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
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...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema

	ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Falta de concienciación sobre la protección física de los equipos	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	
Tipos de entidades	PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Acceso físico no protegido a los locales donde hay hardware o soportes	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona
Soportes accesibles a personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Soportes bajo tierra no identificados	
Tipos de entidades	RES_INF: Medios y soportes
Equipo accesible a personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Fragilidad de los equipos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 05 - DESTRUCCIÓN DEL HARDWARE O DE SOPORTES	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares

	PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.6 FENÓMENO CLIMÁTICO

Condiciones de uso que exceden los límites de funcionamiento del hardware	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Falta de medios de ventilación o de climatización en período estival excesivo calor	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de consideración de las condiciones climáticas para la construcción de los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 06 - FENÓMENO CLIMÁTICO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo

RES_INT: Interfaz de comunicación
RES_INF: Medios y soportes
RES: Red
PHY_SRV: Servicio esencial
PHY_SRV.3: Refrigeración - Contaminación
PHY_SRV.2: Energía
PHY_SRV.1: Comunicación
PHY_LIE: Lugares
PHY_LIE.3: Zona
PHY_LIE.2: Locales
PHY_LIE.1: Entorno externo
PER_UTI: Usuarios
PER_EXP: Operador del sistema - Mantenimiento
PER_DEV: Desarrollador
PER_DEC: Nivel de toma de decisiones
PER: Personal
ORG_PRO: Organización de un proyecto o sistema
ORG_GEN: Organización del organismo
ORG_EXT: Subcontratistas - Proveedores - Industriales
ORG_DEP: Organización de la cual depende el organismo
ORG: Organización
MAT_PAS: Soporte de datos (pasivo)
MAT_PAS.2: Otros soportes
MAT_PAS.1: Soporte electrónico
MAT_ACT: Soporte de procesamiento de datos (activo)
MAT_ACT.3: Periférico de procesamiento
MAT_ACT.2: Hardware fijo
MAT_ACT.1: Hardware portátil
MAT: Hardware
LOG_STD: Paquete de programas o software estándar
LOG_SRV: Software de servicio, mantenimiento o gestión
LOG_OS: Sistema operativo
LOG_APP: Aplicación profesional
LOG_APP.2: Aplicación profesional específica
LOG_APP.1: Aplicación profesional estándar
LOG: Software

4.7 FENÓMENO SÍSMICO

Hardware sensible a las vibraciones	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Falta de consideración de los riesgos sísmicos para la construcción de edificios	
Tipos de entidades	PHY_LIE.2: Locales
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 07 - FENÓMENO SÍSMICO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales

	PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.8 FENÓMENO DE ORIGEN VOLCÁNICO

Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Establecimiento reputado como de riesgo	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de consideración de los riesgos sísmicos para la construcción de edificios	
Tipos de entidades	PHY_LIE.2: Locales
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 08 - FENÓMENO VOLCÁNICO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo

	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.9 FENÓMENO METEOROLÓGICO

Condiciones de uso que exceden los límites de funcionamiento del hardware	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Ausencia de pruebas para verificar los procedimientos de reacción y de información en caso de siniestro	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Establecimiento que sufre periódicamente fenómenos meteorológicos extremos (tempestades, huracanes, ciclones...)	
Tipos de entidades	PHY_LIE.1: Entorno externo
Ausencia de protección contra rayos	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 09 - FENÓMENO METEOROLÓGICO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

RES_REL: Repetidor pasivo o activo
RES_INT: Interfaz de comunicación
RES_INF: Medios y soportes
RES: Red
PHY_SRV: Servicio esencial
PHY_SRV.3: Refrigeración - Contaminación
PHY_SRV.2: Energía
PHY_SRV.1: Comunicación
PHY_LIE: Lugares
PHY_LIE.3: Zona
PHY_LIE.2: Locales
PHY_LIE.1: Entorno externo
PER_UTI: Usuarios
PER_EXP: Operador del sistema - Mantenimiento
PER_DEV: Desarrollador
PER_DEC: Nivel de toma de decisiones
PER: Personal
ORG_PRO: Organización de un proyecto o sistema
ORG_GEN: Organización del organismo
ORG_EXT: Subcontratistas - Proveedores - Industriales
ORG_DEP: Organización de la cual depende el organismo
ORG: Organización
MAT_PAS: Soporte de datos (pasivo)
MAT_PAS.2: Otros soportes
MAT_PAS.1: Soporte electrónico
MAT_ACT: Soporte de procesamiento de datos (activo)
MAT_ACT.3: Periférico de procesamiento
MAT_ACT.2: Hardware fijo
MAT_ACT.1: Hardware portátil
MAT: Hardware
LOG_STD: Paquete de programas o software estándar
LOG_SRV: Software de servicio, mantenimiento o gestión
LOG_OS: Sistema operativo
LOG_APP: Aplicación profesional
LOG_APP.2: Aplicación profesional específica
LOG_APP.1: Aplicación profesional estándar
LOG: Software

4.10 INUNDACIÓN

Falta de servicio de emergencia cercano al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales aplicables en caso de crisis declarada de subcontratistas o proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Establecimiento ubicado en una zona anegadiza	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de protección contra crecidas	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
Soporte o equipo no previsto para resistir a condiciones extremas (de humedad, de temperatura o de perturbaciones físicas)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 10 - INUNDACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo

	ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.11 FALLAS EN LA CLIMATIZACIÓN

Hardware que necesita climatización para funcionar	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo
Archivos que requieren climatización para ser conservados	
Tipos de entidades	MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de revisión de las necesidades de climatización en caso de modificación de los locales o de incorporación de hardware	
Tipos de entidades	PHY_LIE.3: Zona
Dispositivo que depende de un proveedor de agua helada o de energía eléctrica	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Dispositivo incorrectamente dimensionado en relación con a las necesidades	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Falta de mantenimiento de los equipos de aire acondicionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Falta de hardware redundante correctamente dimensionado	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
Acceso no protegido a los dispositivos de suministro de agua y energía eléctrica	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 11 - FALLAS EN LA CLIMATIZACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial

PHY_SRV.3: Refrigeración - Contaminación
PHY_SRV.2: Energía
PHY_SRV.1: Comunicación
PHY_LIE: Lugares
PHY_LIE.3: Zona
PHY_LIE.2: Locales
PHY_LIE.1: Entorno externo
PER_UTI: Usuarios
PER_EXP: Operador del sistema - Mantenimiento
PER_DEV: Desarrollador
PER_DEC: Nivel de toma de decisiones
PER: Personal
ORG_PRO: Organización de un proyecto o sistema
ORG_GEN: Organización del organismo
ORG_EXT: Subcontratistas - Proveedores - Industriales
ORG_DEP: Organización de la cual depende el organismo
ORG: Organización
MAT_PAS: Soporte de datos (pasivo)
MAT_PAS.2: Otros soportes
MAT_PAS.1: Soporte electrónico
MAT_ACT: Soporte de procesamiento de datos (activo)
MAT_ACT.3: Periférico de procesamiento
MAT_ACT.2: Hardware fijo
MAT_ACT.1: Hardware portátil
MAT: Hardware
LOG_STD: Paquete de programas o software estándar
LOG_SRV: Software de servicio, mantenimiento o gestión
LOG_OS: Sistema operativo
LOG_APP: Aplicación profesional
LOG_APP.2: Aplicación profesional específica
LOG_APP.1: Aplicación profesional estándar
LOG: Software

4.12 PÉRDIDA DE SUMINISTRO DE ENERGÍA

Hardware sensible a las perturbaciones eléctricas (bajas de tensión, sobretensiones, microcortes)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de información sobre las condiciones de uso de los suministros de energía auxiliares	
Tipos de entidades	PER_UTI: Usuarios
Terminal de comunicación que no dispone de alimentación auxiliar	
Tipos de entidades	PHY_SRV.1: Comunicación
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	
Tipos de entidades	PHY_SRV.2: Energía
Dimensionamiento inadecuado de los dispositivos de energía de emergencia (inversor, baterías...)	
Tipos de entidades	PHY_SRV.2: Energía
Acceso físico no protegido a los locales que alojan equipos de aprovisionamiento y distribución eléctrica	
Tipos de entidades	PHY_SRV.2: Energía
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	
Tipos de entidades	PHY_SRV.2: Energía
Los diversos revestimientos de suelos o muros no son antiestáticos	
Tipos de entidades	PHY_SRV.2: Energía
El tablero general de baja tensión no es accesible	
Tipos de entidades	PHY_SRV.2: Energía
No hay un puesto de transformación de media tensión/baja tensión instalado en el establecimiento (con acceso controlado del proveedor)	
Tipos de entidades	PHY_SRV.2: Energía
Falta de análisis de la potencia energética auxiliar, necesario en caso de incorporación de hardware	
Tipos de entidades	PHY_SRV.2: Energía
Las conexiones a masa y las conexiones a tierra no han sido realizadas conforme a la reglamentación	

vigente	
Tipos de entidades	PHY_SRV.2: Energía
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 12 - PÉRDIDA DEL SUMINISTRO DE ENERGÍA	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.13 PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN

Mantenimiento remoto de hardware utilizando medios de telecomunicación	
Tipos de entidades	RES_REL: Repetidor pasivo o activo MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de normas para la implantación de los establecimientos que pertenecen al organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales que traten sobre el plazo máximo de interrupción admitido para el suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales que traten sobre la reparación del daño en caso de interrupción del suministro de un servicio esencial	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de instrucciones (alerta, prevención, reacción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de mantenimiento de las terminales y los equipos de distribución	
Tipos de entidades	PHY_SRV.1: Comunicación
Fallas de gestión de la red telefónica interna	
Tipos de entidades	PHY_SRV.1: Comunicación
Funcionamiento incorrecto ya constatado en la provisión del servicio de telecomunicaciones	
Tipos de entidades	PHY_SRV.1: Comunicación
Acceso físico no protegido a los locales que alojan equipos de alimentación y distribución eléctrica o medios de telecomunicación	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales

	PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.14 EMISIONES ELECTROMAGNÉTICAS

Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Ausencia de cláusula contractual referida a la compatibilidad electromagnética	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 14 - EMISIONES ELECTROMAGNÉTICAS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes

	MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.15 RADIACIONES TÉRMICAS

Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 15 - RADIACIONES TÉRMICAS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento

	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.16 IMPULSOS ELECTROMAGNÉTICOS

Hardware o soporte sensible a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Proximidad de una fuente de emisiones electromagnéticas o radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
No se han considerado durante el diseño las emisiones electromagnéticas o las radiaciones térmicas	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Ninguna consideración de los riesgos vinculados con la proximidad de una fuente electromagnética	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Medios o soportes sensibles a las emisiones electromagnéticas o a las radiaciones térmicas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 16 - IMPULSOS ELECTROMAGNÉTICOS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento

	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.17 INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS

Falta de consideración de las normas de instalación	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV.2: Energía PHY_SRV.1: Comunicación MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Falta de consideración de la zonificación del hardware	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Hardware susceptible de emitir señales parásitas comprometedoras	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de reglas que impongan el cumplimento de normas	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de procedimiento de verificación del hardware antes de su compra o luego de un mantenimiento	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de una política de protección de la información	
Tipos de entidades	ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo

Falta de realización de zonificación TEMPEST	
Tipos de entidades	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo
Acceso público cerca de los edificios del organismo	
Tipos de entidades	PHY_LIE.2: Locales
Sala situada cerca de la vía pública	
Tipos de entidades	PHY_LIE.3: Zona
Soporte que facilita la captura de señales parásitas comprometedoras (cables eléctricos, tuberías...)	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Falta de protección de los accesos a los equipos	
Tipos de entidades	PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Medios y soportes susceptibles de emitir señales parásitas comprometedoras	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar

	LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.18 ESPIONAJE A DISTANCIA

Falta de protector de pantalla en caso de inactividad	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Utilización de contraseñas de acceso al sistema o a la aplicación simples de observar (forma en un teclado, contraseña corta)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Sin cambios o pocos cambios en la contraseña de acceso al sistema o a la aplicación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Pantalla observable desde el exterior	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Lectura de documentos delicados en lugares públicos (observación de documentos por parte de personas ajenas al organismo...)	
Tipos de entidades	MAT_PAS.2: Otros soportes
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas de protección para el intercambio de información de carácter confidencial	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de una política de protección de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema

Falta de identificación de las necesidades de seguridad de un proyecto	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Escasa concienciación sobre la protección de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Presencia de un lugar de observación desde fuera del establecimiento	
Tipos de entidades	PHY_LIE.1: Entorno externo
Zona que dispone de una abertura que da a la vía pública	
Tipos de entidades	PHY_LIE.3: Zona
Zona observable desde un lugar de paso	
Tipos de entidades	PHY_LIE.3: Zona
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 18 - ESPIONAJE A DISTANCIA	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo)

	MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.19 ESCUCHA PASIVA

Falta de dispositivo de control de acceso en caso de inactividad	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de agregar un software de escucha de tipo troyano	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de protección de los registros que recogen la traza de las actividades	
Tipos de entidades	SYS_WEB: Portal externo SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet LOG_STD: Paquete de programas o software estándar LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Sin cambios o pocos cambios en la contraseña de acceso al sistema o a la aplicación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de protección contra el uso de privilegios avanzados	
Tipos de entidades	LOG_OS: Sistema operativo
Pocos cambios o ningún cambio en la contraseña de acceso al software de soporte de base	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión
Acceso lógico al hardware que permite la instalación de un software de escucha	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware que dispone de una interfaz de comunicación susceptible de escucha (infrarrojos, 802.11, Bluetooth...)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas de protección para el intercambio de información de carácter confidencial	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control de la aplicación de la política de seguridad	

Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	
Tipos de entidades	ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de una política de protección de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de identificación de las necesidades de seguridad de un proyecto	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de formación sobre las medidas y herramientas de protección de las comunicaciones internas y con el exterior del organismo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Escasa concienciación sobre la protección de la confidencialidad de los intercambios de información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio para la captación de información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Posibilidad de captar las transmisiones desde fuera del establecimiento	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de protección de los accesos a las terminales de comunicación	
Tipos de entidades	PHY_SRV.1: Comunicación
Medios y soportes que poseen características que permiten la escucha pasiva (ej.: Ethernet, sistemas	

de comunicación sin cable)	
Tipos de entidades	RES_INF: Medios y soportes
Soporte o equipo de comunicación físicamente accesible que permite la instalación de dispositivos de escucha	
Tipos de entidades	RES_INF: Medios y soportes
Falta de autenticación del hardware conectado a la red	
Tipos de entidades	RES_INT: Interfaz de comunicación
Acceso físico o lógico a un repetidor que permita la instalación de un dispositivo de escucha	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Comunicación que se efectúa en modo Broadcast	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Complejidad del encaminamiento entre las subredes	
Tipos de entidades	RES_INT: Interfaz de comunicación
Interfaz que dispone de una función que permite la escucha	
Tipos de entidades	RES_INT: Interfaz de comunicación
Circulación de información sin cifrar	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Falta de aislamiento de las redes de comunicación	
Tipos de entidades	SYS_ITR: Intranet
Posibilidad de escuchar las comunicaciones con los servidores de autenticación	
Tipos de entidades	SYS_ITR: Intranet
Posibilidad de escuchar las comunicaciones con los servidores de aplicación	
Tipos de entidades	SYS_ITR: Intranet
Posibilidad de introducir en las instalaciones de los clientes un software de escucha	
Tipos de entidades	SYS_MES: Correo electrónico
Posibilidad de colocar un dispositivo de escucha lógica en las pasarelas de correo electrónico	
Tipos de entidades	SYS_MES: Correo electrónico
Lagunas en la gestión de los privilegios de acceso a las pasarelas de correo electrónico	
Tipos de entidades	SYS_MES: Correo electrónico
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 19 - ESCUCHA PASIVA	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación

	PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.20 ROBO DE SOPORTES O DOCUMENTOS

Aplicaciones únicas desarrolladas internamente	
Tipos de entidades	LOG_APP.2: Aplicación profesional específica
Falta de inventario del hardware	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware atractivo (valor mercantil, tecnológico, estratégico)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de protección del hardware contra robo (cable antirrobo)	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Disco duro fácilmente desmontable	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware de libre uso que puede ser utilizado por un grupo de personas	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Falta de protección de acceso a los equipos de respaldo de datos	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento
Presencia de impresora en los lugares de paso	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento
Los soportes son accesibles a todos	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Transmisión de soportes mediante servicios postales (proveedores externos, correo interno,...)	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de protección del almacenamiento de los soportes	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de inventario de los soportes utilizados	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de respaldo de los datos contenidos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes fácilmente transportables (ej.: disco duro extraíble, cartucho para respaldo de datos)	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soportes originales	
Tipos de entidades	MAT_PAS.2: Otros soportes
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales

Las responsabilidades de seguridad en cuanto a la clasificación de la información no han sido formalizadas ni son conocidas por todos	
Tipos de entidades	ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de estructura de gestión de los incidentes de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de los bienes delicados	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de las necesidades de seguridad de un proyecto	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Ausencia de una política de protección de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Incumplimiento de las normas vinculadas con el procesamiento de las informaciones	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre la protección de documentos de carácter confidencial que provoca una falta de cuidado	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio para la divulgación de información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de compromiso individual para la protección de documentos de carácter confidencial	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Soportes o documentos enviados o presentes fuera del establecimiento	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos	

indirectos	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 20 - ROBO DE SOPORTES O DOCUMENTOS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.21 ROBO DE HARDWARE

Falta de hardware de repuesto	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de inventario del hardware	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento MAT_ACT.1: Hardware portátil
Hardware de libre uso que puede ser utilizado por un grupo de personas	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Hardware atractivo (valor mercantil, tecnológico, estratégico)	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento MAT_ACT.1: Hardware portátil
Posible reventa del hardware (falta de marcado, utilización sin contraseña)	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Hardware fácilmente desmontable	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de estructura de gestión y tratamiento de los incidentes de seguridad vinculados con robos	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de normas de control de las entradas/salidas del hardware del organismo	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de las necesidades de seguridad de un proyecto	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Escasa concienciación sobre la protección del hardware fuera del organismo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento

	PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Incumplimiento de las normas de protección física aplicables a los equipos portátiles	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio para la reventa de algún hardware	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 21 - ROBO DE HARDWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware

	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.22 RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS

Presencia de datos residuales utilizados por el software	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Presencia de datos residuales sin que lo sepa el usuario, de hardware reasignado o desechado	
Tipos de entidades	MAT_PAS.1: Soporte electrónico MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de medios para la destrucción de los soportes	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de control de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Ausencia de política de protección de la información aplicable al reciclado y desecho	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las medidas de seguridad que deben respetar los subcontratistas y los proveedores	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Incumplimiento de las normas de destrucción de los soportes vinculadas con la clasificación de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de información y de concienciación sobre la remanencia de los datos informáticos en los soportes	

Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio para la divulgación de información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Presencia de soporte desechado fuera del establecimiento	
Tipos de entidades	PHY_LIE.1: Entorno externo
Presencia de un soporte desechado en lugares públicos	
Tipos de entidades	PHY_LIE.2: Locales
Presencia de un soporte desechado en zonas accesibles a personas que no tienen necesidad de conocer la información involucrada	
Tipos de entidades	PHY_LIE.3: Zona
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo)

	MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.23 DIVULGACIÓN

Falta de verificación de los accesos compartidos concedidos	
Tipos de entidades	MAT_ACT.2: Hardware fijo LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Procedimientos de gestión de los privilegios de acceso demasiado complicados de ejecutar	
Tipos de entidades	MAT_ACT.2: Hardware fijo LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Funciones de gestión de los derechos de acceso demasiado complicadas de utilizar y que pueden ser fuente de error	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Presencia de una red de comunicación con el exterior que permite el intercambio de información	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Soportes capaces de realizar intercambios de información de carácter delicado	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de estructura responsable de la definición, la aplicación y el control de los privilegios de acceso a la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de compromiso personal de protección de la confidencialidad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Procedimientos de gestión y de aplicación de los permisos demasiado complicados de ejecutar	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Las responsabilidades de seguridad en cuanto a la clasificación de la información no han sido formalizadas ni son conocidas por todos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema

	ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de control de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de protección de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Incumplimiento de las normas vinculadas con el procesamiento de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta concienciación sobre la protección de la información delicada	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Incumplimiento del deber de reserva	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio para la divulgación de información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de control (inclusive de trazas) del intercambio con el exterior	
Tipos de entidades	PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
Presencia de algún directorio compartido para almacenar información	
Tipos de entidades	RES_INF: Medios y soportes
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_INT: Interfaz de comunicación

Interfaz estándar que permite el intercambio de información (ej.: interfaz Bluetooth que acepte todas las comunicaciones por defecto)	
Tipos de entidades	RES_INT: Interfaz de comunicación
Posibilidad de utilizar los recursos sin generar trazas	
Tipos de entidades	RES_INT: Interfaz de comunicación
Falta de notificación de los usuarios	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Complejidad del encaminamiento entre las subredes	
Tipos de entidades	RES_INT: Interfaz de comunicación
Falta de encaminamiento estricto entre las subredes	
Tipos de entidades	RES_INT: Interfaz de comunicación
Falta de filtrado y de registro en los repetidores de comunicación entre redes	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
El sistema está conectado a redes externas	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Falta de control de acceso a los datos almacenados en el directorio	
Tipos de entidades	SYS_ANU: Directorio de la empresa
Falta de registro de los accesos	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
Falta de dispositivo de filtrado	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
Falta de gestión o dificultad para gestionar los privilegios de acceso a la información compartida (definición, implementación, control)	
Tipos de entidades	SYS_ITR: Intranet
Falta de aislamiento entre las redes de comunicación	
Tipos de entidades	SYS_ITR: Intranet
Ausencia de medidas que permitan evitar una negligencia durante el envío de información	
Tipos de entidades	SYS_MES: Correo electrónico
El sistema puede ser utilizado por todo el personal	
Tipos de entidades	SYS_MES: Correo electrónico
El sistema permite el intercambio de ficheros adjuntos	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de protección antivirus eficaz y operativa	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de gestión de los privilegios de acceso a los datos (posibilidad de alterar información pública...)	
Tipos de entidades	SYS_WEB: Portal externo
El sistema facilita la divulgación de información fuera del organismo	
Tipos de entidades	SYS_WEB: Portal externo
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 23 - DIVULGACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet

SYS_INT: Dispositivo de acceso a Internet
SYS_ANU: Directorio de la empresa
SYS: Sistema
RES_REL: Repetidor pasivo o activo
RES_INT: Interfaz de comunicación
RES_INF: Medios y soportes
RES: Red
PHY_SRV: Servicio esencial
PHY_SRV.3: Refrigeración - Contaminación
PHY_SRV.2: Energía
PHY_SRV.1: Comunicación
PHY_LIE: Lugares
PHY_LIE.3: Zona
PHY_LIE.2: Locales
PHY_LIE.1: Entorno externo
PER_UTI: Usuarios
PER_EXP: Operador del sistema - Mantenimiento
PER_DEV: Desarrollador
PER_DEC: Nivel de toma de decisiones
PER: Personal
ORG_PRO: Organización de un proyecto o sistema
ORG_GEN: Organización del organismo
ORG_EXT: Subcontratistas - Proveedores - Industriales
ORG_DEP: Organización de la cual depende el organismo
ORG: Organización
MAT_PAS: Soporte de datos (pasivo)
MAT_PAS.2: Otros soportes
MAT_PAS.1: Soporte electrónico
MAT_ACT: Soporte de procesamiento de datos (activo)
MAT_ACT.3: Periférico de procesamiento
MAT_ACT.2: Hardware fijo
MAT_ACT.1: Hardware portátil
MAT: Hardware
LOG_STD: Paquete de programas o software estándar
LOG_SRV: Software de servicio, mantenimiento o gestión
LOG_OS: Sistema operativo
LOG_APP: Aplicación profesional
LOG_APP.2: Aplicación profesional específica
LOG_APP.1: Aplicación profesional estándar
LOG: Software

4.24 INFORMACIÓN SIN GARANTÍA DEL ORIGEN

Recuperación de software desde un medio no autenticado	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de instalar correcciones, actualizaciones, parches, hotfixes...	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Ausencia de un medio seguro de identificación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de conservación de trazas de las actividades	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de medios que permitan garantizar la procedencia del hardware	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de medios que permitan garantizar la procedencia de los suministros	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de una política de conservación y de análisis de las trazas de las actividades	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de información referente a la división de responsabilidades y a los medios de garantizar la legitimidad de una petición	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de organización que permita garantizar la identificación de una persona dentro del organismo o en el marco de un proyecto	

Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre los riesgos de usurpación de identidad (uso incorrecto de los medios que garantizan la autenticación tales como las contraseñas)	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Credulidad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Desconocimiento de la importancia de la calificación de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Obtención de un beneficio gracias a la desinformación	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Falta de medios que permitan garantizar la autenticidad de los códigos	
Tipos de entidades	PER_DEV: Desarrollador
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_DEV: Desarrollador
Posibilidad de alterar una comunicación	
Tipos de entidades	RES_INF: Medios y soportes
Protocolo que no permite autenticar en forma segura al emisor de una comunicación	
Tipos de entidades	RES_INT: Interfaz de comunicación
Posibilidad de utilizar los recursos sin generar trazas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Los repetidores no identifican ni las fuentes ni los destinos (ejemplo de impacto: sistema vulnerable a los ataques basados en "spoofing")	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
Posibilidad de usurpar la función del directorio	

Tipos de entidades	SYS_ANU: Directorio de la empresa
El sistema no permite identificar al autor de una modificación	
Tipos de entidades	SYS_ANU: Directorio de la empresa
El dispositivo permite acceder a datos que no han sido autenticados (ej.: menajes en cadena)	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
El sistema no dispone de medios de conservación del registro histórico de las actividades	
Tipos de entidades	SYS_WEB: Portal externo SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet
El sistema permite el almacenamiento o la modificación de información sin autenticación de sus autores	
Tipos de entidades	SYS_ITR: Intranet
El sistema permite la emisión y la recepción de información sin autenticación de emisores ni destinatarios	
Tipos de entidades	SYS_MES: Correo electrónico
El sistema no dispone de filtros para impedir la recepción de mensajes falsos en cadena procedentes del exterior	
Tipos de entidades	SYS_MES: Correo electrónico
El sistema permite retransmisiones de mensajes	
Tipos de entidades	SYS_MES: Correo electrónico
El sistema no permite la identificación de la persona que emitió una petición	
Tipos de entidades	SYS_WEB: Portal externo
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 24 - INFORMACIÓN SIN GARANTÍA DEL ORIGEN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico

	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.25 SABOTAJE DEL HARDWARE

Posibilidad de colocar otros elementos de hardware para almacenar, enviar o alterar información (ej.: capturador de teclado físico)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Ausencia de procedimiento para el control de las intervenciones de personal externo en los equipos del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_GEN: Organización del organismo
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de procedimientos de calificación operativa	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de control de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de procedimientos de validación de los componentes de hardware durante la entrega inicial o cuando se reincorporan tras un mantenimiento	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Software no probado lo suficiente dentro de los valores límite especificados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de cuidado durante la intervención de personal de mantenimiento en un puesto de trabajo o un servidor	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Escasa concienciación sobre la protección del hardware fuera del organismo	
Tipos de entidades	PER_UTI: Usuarios

	PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio gracias a la desinformación	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	
Tipos de entidades	PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
Posibilidad de colocar una desviación de circuito	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 25 - SABOTAJE DEL HARDWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo

	MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.26 ALTERACIÓN DE PROGRAMAS

El enlace de mantenimiento remoto está permanentemente activado	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de que existan funciones escondidas introducidas durante las fases de diseño y desarrollo	
Tipos de entidades	SYS_WEB: Portal externo SYS_ANU: Directorio de la empresa LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de modificar, de alterar el software	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de protección contra el uso de privilegios avanzados	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Uso de programas no evaluados	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de implementación de normas de seguridad de base aplicables al sistema operativo y al software	
Tipos de entidades	SYS_MES: Correo electrónico LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de crear o modificar comandos de sistemas	
Tipos de entidades	SYS_WEB: Portal externo LOG_OS: Sistema operativo
Recuperación de software desde un medio no autenticado	
Tipos de entidades	LOG_OS: Sistema operativo

Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Contraseñas de conexión demasiado simples	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Posibilidad de instalar correcciones, actualizaciones, parches, hotfixes...	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Uso de un sistema operativo estándar que ya ha sufrido ataques lógicos	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Posibilidad de borrar, modificar o instalar nuevos programas	
Tipos de entidades	LOG_OS: Sistema operativo
El dispositivo SNMP está activado	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
El dispositivo SNMP está activado.: disquete, CD-ROM)	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de medios que permitan el control de inocuidad de los soportes cuando se ingresan al organismo	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de procedimiento para el control de las intervenciones de personal externo en los equipos del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales referentes a la garantía de inocuidad de los suministros entregados por el subcontratista o proveedor	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de política global de lucha contra el código malicioso	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de identificación de los bienes delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de los bienes delicados	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de política de protección de los puestos de trabajo	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de una política de conservación y de análisis de las trazas de las actividades	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de medidas de control de los desarrollos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Ausencia de medidas de protección de la integridad de los códigos en las fases de diseño, puesta en servicio y gestión	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Uso de software sin garantía de su origen	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios PER_DEC: Nivel de toma de decisiones
Falta de concienciación sobre la amenaza de los códigos maliciosos	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Desconocimiento de las reacciones reflejas necesarias en caso de detección de anomalías	
Tipos de entidades	PER_UTI: Usuarios PER_DEC: Nivel de toma de decisiones
Incumplimiento de las normas de actualización de los programas antivirus	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Obtención de un beneficio gracias a la alteración del sistema informático	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Situación conflictiva	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_DEV: Desarrollador
Falta de medios que permitan garantizar la autenticidad de los desarrollos	
Tipos de entidades	PER_DEV: Desarrollador
Operador del sistema o personal de mantenimiento que dispone de privilegios extendidos	

Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Desconocimiento de los procedimientos en caso de detección de anomalías	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Uso de hardware fuera del organismo (domicilio del personal, otro organismo...)	
Tipos de entidades	PHY_LIE.1: Entorno externo
Falta de control de acceso al establecimiento o a los locales o posibilidad de ingresar por accesos indirectos	
Tipos de entidades	PHY_SRV.1: Comunicación PHY_LIE.3: Zona PHY_LIE.2: Locales
La red facilita el uso de los recursos por parte de personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de agregar desviaciones lógicas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
La red permite modificar los recursos del sistema o actuar sobre ellos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de agregar software adicional para almacenar, enviar o alterar (ej.: capturador de teclado)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de utilizar los recursos sin generar trazas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de modificar o cambiar aplicaciones	
Tipos de entidades	SYS_WEB: Portal externo SYS_ANU: Directorio de la empresa
Posibilidad de borrar o modificar programas o ficheros de sistema	
Tipos de entidades	SYS_WEB: Portal externo SYS_ANU: Directorio de la empresa
Falta de concienciación sobre los riesgos generados por la descarga de software	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
Falta de control antivirus en los intercambios de información	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
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)	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
Presencia de un dispositivo que permite modificar o instalar aplicaciones en forma remota	
Tipos de entidades	SYS_ITR: Intranet
Uso de un espacio de almacenamiento compartido	
Tipos de entidades	SYS_ITR: Intranet
Utilización de una versión obsoleta del servidor de correo electrónico	
Tipos de entidades	SYS_MES: Correo electrónico
Utilización de una lista de difusión que incluya gran parte del personal	

Tipos de entidades	SYS_MES: Correo electrónico
Presencia de un protocolo que no dispone de función de autenticación	
Tipos de entidades	SYS_MES: Correo electrónico
El correo electrónico permite el envío automático de mensajes	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de concienciación sobre los riesgos provocados por la ejecución de ficheros adjuntos	
Tipos de entidades	SYS_MES: Correo electrónico
El correo electrónico permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: envío automático de ficheros adjuntos)	
Tipos de entidades	SYS_MES: Correo electrónico
No se realiza ninguna verificación de las aplicaciones antes de su instalación	
Tipos de entidades	SYS_MES: Correo electrónico
El correo electrónico permite instalar actualizaciones de software (ej.: parches, antivirus...)	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de medios de filtrado antivirus	
Tipos de entidades	SYS_MES: Correo electrónico
Posibilidad de instalar programas piratas	
Tipos de entidades	SYS_WEB: Portal externo
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 26 - ALTERACIÓN DE PROGRAMAS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil

	MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.27 GEOLOCALIZACIÓN

Hardware localizable (ej.: triangulación)	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Ausencia de políticas de seguridad para la protección de la información aplicables en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas de protección de la confidencialidad de la información utilizada para localizar al personal (pedido de pasajes, registro de entrada/salida...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de discreción o de cuidado	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 27 - GEOLOCALIZACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales

	ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.28 AVERÍA DEL HARDWARE

Falta de función de diagnóstico para la prevención de fallos del hardware	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo
Falta de protección contra perturbaciones eléctricas	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Malas condiciones de uso	
Tipos de entidades	RES_INF: Medios y soportes MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Problemas de mantenimiento	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Poca fiabilidad del hardware	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Envejecimiento del hardware	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Soporte no adaptado a la vida útil de los datos que se van a archivar	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Malas condiciones de almacenamiento	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de cláusula referente a los plazos de intervención y de reemplazo en caso de avería del hardware	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de estructura de seguimiento de los contratos de mantenimiento	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

Falta de seguimiento de los contratos de mantenimiento y de soporte con los proveedores	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de informes sobre los fallos (cantidad, coste de los incidentes, duración)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
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)	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de instrucciones de reacciones rápidas para la protección del hardware en caso de perjuicios ocasionados por el agua o por un incendio	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de estructura destinada al análisis de la adecuación de las capacidades de los equipos a las necesidades	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
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)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Falta de envío de informes para un análisis centralizado de los fallos	
Tipos de entidades	PER_UTI: Usuarios
Desconocimiento de las instrucciones de uso del hardware	
Tipos de entidades	PER_UTI: Usuarios
Falta de consideración del entorno específico que aumenta los riesgos de fallos (atmósfera sobrecalefaccionada, entorno industrial,...)	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Ausencia de control del buen funcionamiento de los recursos de emergencia	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Desencadenamiento manual de la solución de emergencia	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Poca fiabilidad de los soportes	
Tipos de entidades	RES_INF: Medios y soportes
Envejecimiento de los soportes de información	
Tipos de entidades	RES_INF: Medios y soportes

VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 28 – AVERÍA DEL HARDWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.29 FALLA DE FUNCIONAMIENTO DEL HARDWARE

Falta de función de diagnóstico para la prevención de fallos del hardware	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo
Falta de protección contra perturbaciones eléctricas	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Malas condiciones de uso	
Tipos de entidades	RES_INF: Medios y soportes MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Poca fiabilidad del hardware	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Posibilidad de incompatibilidad entre los distintos componentes del hardware	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Soporte no adaptado a la vida útil de los datos que se van a archivar	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Malas condiciones de almacenamiento	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de reglas que impongan el cumplimento de normas	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de cláusula referente a los plazos de intervención y de tratamiento en caso de falla de funcionamiento	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de informes sobre las fallas de funcionamiento	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

Ausencia de procedimientos de calificación operativa	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de normas referentes al entorno de uso de las infraestructuras de tratamiento de la información (temperatura, higrometría...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de estructura destinada al análisis de la adecuación de las capacidades de los equipos a las necesidades	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Desconocimiento de las instrucciones de uso del hardware	
Tipos de entidades	PER_UTI: Usuarios
Falta de envío de informes para un análisis centralizado de los fallos	
Tipos de entidades	PER_UTI: Usuarios
Falta de consideración del entorno específico que aumenta los riesgos de fallos (atmósfera sobrecalefaccionada, entorno industrial,...)	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Ausencia de control del buen funcionamiento de los recursos de emergencia	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Desencadenamiento manual de la solución de emergencia	
Tipos de entidades	PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación
Envejecimiento de los soportes de información	
Tipos de entidades	RES_INF: Medios y soportes
Posibilidad de incompatibilidad entre los soportes y otros componentes	
Tipos de entidades	RES_INF: Medios y soportes
Medios y soportes que incorporan características técnicas específicas de su localización (ej.: diferentes parámetros de configuración ADSL entre Francia y el Reino Unido)	
Tipos de entidades	RES_INF: Medios y soportes
Poca fiabilidad de los soportes	
Tipos de entidades	RES_INF: Medios y soportes
Problemas de mantenimiento	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
Interfaz que incorpora características técnicas referidas al país (ej.: conexiones telefónicas diferentes entre Francia y el reino Unido)	
Tipos de entidades	RES_INT: Interfaz de comunicación
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	
Tipos de entidades	RES_REL: Repetidor pasivo o activo

	RES_INT: Interfaz de comunicación
Envejecimiento del hardware	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de incompatibilidad entre los distintos recursos	
Tipos de entidades	RES_INT: Interfaz de comunicación
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 29 - MAL FUNCIONAMIENTO DEL HARDWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.30 SATURACIÓN DEL SISTEMA INFORMÁTICO

Falta de filtros que protejan al sistema contra saturaciones	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Consumo inútil de recursos	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Aplicación que requiere recursos informáticos que no se adaptan al hardware (ej.: falta de memoria RAM)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de consideración, en la definición de los requerimientos de un proyecto, de situaciones particulares que ponen al sistema en condiciones límite	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de calificación de los desarrollos en un contexto representativo del uso	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Dimensionamiento inadecuado de los recursos (ej.: falta de autonomía de una batería de ordenador portátil)	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware

Persistencia involuntaria de los datos en los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico

Ausencia de reglas que impongan el cumplimento de normas	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
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)	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
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	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
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	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de instrucciones referidas a los incidentes (detección, acción...)	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de decisión de redimensionamiento que considere los significativos aumentos en el uso de los recursos informáticos	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de implementación de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	
Tipos de entidades	PER_UTI: Usuarios
Obtención de un beneficio mediante la alteración del sistema informático	
Tipos de entidades	PER_UTI: Usuarios
Falta de concienciación sobre las necesidades de economizar los recursos informáticos del organismo (uso incorrecto de los espacios de almacenamiento...)	
Tipos de entidades	PER_UTI: Usuarios
Dimensionamiento inadecuado de los recursos de telecomunicación, por ejemplo, como consecuencia del uso diario de recursos destinados a la solución de emergencia	
Tipos de entidades	PHY_SRV.1: Comunicación
Dimensionamiento inadecuado de los recursos de emergencia	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía
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"...)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Dimensionamiento inadecuado (ej.: demasiados datos en relación con el ancho máximo de banda)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
Dimensionamiento inadecuado de los recursos (ej.: demasiados usuarios en relación con la capacidad máxima del directorio)	

Tipos de entidades	SYS_ANU: Directorio de la empresa
Posibilidad de someter el dispositivo a una enorme demanda que excede sus límites	
Tipos de entidades	SYS_WEB: Portal externo SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Acontecimiento puntual o período durante el cual se produce un aumento muy significativo del uso del sistema	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ANU: Directorio de la empresa
Dimensionamiento inadecuado de los recursos (ej.: demasiados usuarios en relación con la cantidad de conexiones posible y el ancho de banda)	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet
Falta de gestión de los derechos de escritura en los espacios de almacenamiento compartidos	
Tipos de entidades	SYS_ITR: Intranet
Dimensionamiento inadecuado de los recursos (ej.: espacio para almacenar o compartir ficheros demasiado limitado)	
Tipos de entidades	SYS_ITR: Intranet
Falta de aislamiento entre las redes de comunicación	
Tipos de entidades	SYS_ITR: Intranet
Utilización de una lista de difusión interna accesible a todos	
Tipos de entidades	SYS_MES: Correo electrónico
Dimensionamiento inadecuado de los espacios de almacenamiento de los mensajes recibidos	
Tipos de entidades	SYS_MES: Correo electrónico
El correo electrónico permite la emisión automática de mensajes	
Tipos de entidades	SYS_MES: Correo electrónico
Ausencia de protección contra spam	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de limitación del tamaño de los ficheros adjuntos	
Tipos de entidades	SYS_MES: Correo electrónico
Uso incorrecto del servicio de correo electrónico por parte de los usuarios (utilización de los buzones de correo electrónico como espacio de archivado)	
Tipos de entidades	SYS_MES: Correo electrónico
Acceso público al portal	
Tipos de entidades	SYS_WEB: Portal externo
Dimensionamiento inadecuado de los recursos (ej.: demasiadas conexiones simultáneas)	
Tipos de entidades	SYS_WEB: Portal externo
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial

	PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.31 FALLA DE FUNCIONAMIENTO DEL SOFTWARE

Posibles efectos secundarios vinculados con la actualización de un componente lógico	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de conservación de trazas de los procesamientos de información	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de formación en el uso y mantenimiento del nuevo software	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de mantenimiento	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de calificación antes de toda instalación o actualización	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de sincronización de los relojes	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de envío de informes para un tratamiento centralizado de las fallas de funcionamiento	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo

	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de configurar, instalar o modificar en forma incorrecta el sistema operativo	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de informes de las operaciones de mantenimiento	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
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)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de documentación actualizada	
Tipos de entidades	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
No se realiza ninguna verificación de las aplicaciones antes de su instalación	
Tipos de entidades	SYS_MES: Correo electrónico LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	
Tipos de entidades	SYS_MES: Correo electrónico LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo
Ausencia de reglas que impongan el cumplimento de normas	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallos o saturaciones (esquemas orientativos)	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales referentes a las condiciones de asistencia y servicio técnico	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
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	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de instrucciones sobre el uso correcto de los recursos informáticos a fin de evitar conductas	

riesgosas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de instrucciones referidas a los incidentes (detección, acción...)	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de homogeneidad del parque informático	
Tipos de entidades	ORG_GEN: Organización del organismo
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)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de un seguimiento de los incidentes que permita prevenir eventuales fallas de funcionamiento (esquemas orientativos)	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de formación	
Tipos de entidades	PER_DEV: Desarrollador
Ausencia de normas de seguridad durante los desarrollos	
Tipos de entidades	PER_DEV: Desarrollador
Falta de formación en el mantenimiento y uso de los nuevos equipos	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Dimensionamiento inadecuado de los recursos de gestión y mantenimiento	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Incumplimiento de los procedimientos de intervención	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	
Tipos de entidades	PER_UTI: Usuarios
Posibilidad de configurar, instalar o modificar en forma incorrecta los repetidores	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Gestión incorrecta de las versiones y configuraciones de los pilotos	
Tipos de entidades	RES_INT: Interfaz de comunicación
Efectos secundarios de las interfaces (problemas de compatibilidad entre protocolos...)	
Tipos de entidades	RES_INT: Interfaz de comunicación
Posibilidad de que el dispositivo esté sometido a peticiones o datos mal formados (ej.: buffer overflow, denegación de servicio en el servidor LDAP)	
Tipos de entidades	SYS_ITR: Intranet SYS_ANU: Directorio de la empresa
Incumplimiento de los procedimientos de instalación o de mantenimiento	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Posibilidad de someter el dispositivo a una gran demanda que excede sus límites	
Tipos de entidades	SYS_INT: Dispositivo de acceso a Internet

Incompatibilidad de software (ej.: efecto secundario de un software antivirus que filtre los mensajes...)	
Tipos de entidades	SYS_MES: Correo electrónico
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)	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico
Utilización de una versión obsoleta del servidor de correo electrónico	
Tipos de entidades	SYS_MES: Correo electrónico
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 31 – FALLA DE FUNCIONAMIENTO DEL SOFTWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.32 PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN

No se realiza ninguna verificación de las aplicaciones antes de su instalación

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de emergencia

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de vuelta atrás en caso de anomalía durante una modificación

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento de mantenimiento

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de documentación actualizada

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de informes de las operaciones de mantenimiento

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de conservación de las trazas de los procesos y modificaciones

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional

	LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Software específico	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de formación en el uso y mantenimiento del nuevo software	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Software obsoleto	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Software de configuración no escalable	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de medios para una asistencia técnica accesible desde fuera del organismo o desde un país con importante diferencia horaria	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware de configuración no escalable	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware obsoleto	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware específico	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación MAT_ACT: Soporte de procesamiento de datos (activo)

	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Modificación de los equipos, del software o de los procedimientos de respaldo de datos sin tener en cuenta anteriores respaldos o archivos	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Soporte obsoleto	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Pérdida o gestión incorrecta de los documentos originales (contratos de asistencia técnica, licencias...)	
Tipos de entidades	MAT_PAS.2: Otros soportes
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de cláusula contractual que asegure el restablecimiento de la actividad (en caso de cese de la actividad, en caso de quiebra del proveedor,...)	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de garantía referida a la continuidad del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de seguimiento de los contratos de mantenimiento y de soporte con los proveedores	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de instrucciones referidas a los incidentes (detección, acción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de manual de aseguramiento de la calidad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de estructura de protección de la documentación y de los medios de mantenimiento de los sistemas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de plan de restablecimiento de las actividades esenciales del organismo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de procedimientos de gestión de la configuración de los sistemas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de aplicación de normas o estándares durante el desarrollo del sistema de información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de plan de formación en el mantenimiento de los nuevos sistemas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Elección de tecnología sin garantía de actualización permanente	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Bajo presupuesto asignado al mantenimiento	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Existencia de componentes obsoletos en la infraestructura de tratamiento de la información (desarrollo en lenguajes más utilizados...)	

Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Incumplimiento de las normas de calidad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Ausencia de estándares o de normas	
Tipos de entidades	PER_DEV: Desarrollador
Incumplimiento de las normas de calidad	
Tipos de entidades	PER_DEV: Desarrollador
Falta de formación sobre el correcto uso de las herramientas informáticas (alteración del sistema, instalación de software incompatible...)	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento
Uso de software o de desarrollos fuera de las normas y estándares del organismo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento
Problemas de mantenimiento	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
Falta de plano del cableado	
Tipos de entidades	RES_INF: Medios y soportes
El mantenimiento o la gestión de los equipos requiere la disponibilidad de los soportes de red	
Tipos de entidades	RES_INF: Medios y soportes
El mantenimiento o la gestión del sistema se realiza por intermedio de la red	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Falta de plazos máximos de garantía para los soportes de comunicación	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Utilización de una versión obsoleta del servidor de correo electrónico	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Uso de un sistema obsoleto	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Uso de un sistema no estandarizado	
Tipos de entidades	SYS_WEB: Portal externo

	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Falta de cumplimiento de procedimientos de instalación y mantenimiento (especificaciones de configuración y parámetros)	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Falta de medios de soporte internos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 32 - SATURACIÓN DEL SISTEMA DE INFORMACIÓN	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión

	LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.33 USO ILÍCITO DEL HARDWARE

Falta de gestión de licencia, de dispositivo de registro y de activación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Uso compartido de una identificación de conexión	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	
Tipos de entidades	LOG_OS: Sistema operativo
El hardware está conectado a redes externas	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
El hardware utilizado permite un uso diferente del previsto (desarrollo de software no destinado al organismo...)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Los soportes son accesibles a todos	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de políticas de seguridad para la protección de la infraestructura de tratamiento de la información en los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de concienciación del personal sobre el riesgo de ser sancionado	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales referidas al uso del material informático	

Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de instrucciones referidas al uso del material informático	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de procedimiento de control	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de guía informática que especifique los requerimientos de uso	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador ORG_GEN: Organización del organismo
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación sobre los riesgos de sanciones	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Derechos otorgados fuera de la legítima necesidad	
Tipos de entidades	PER_UTI: Usuarios PER_DEC: Nivel de toma de decisiones
Obtención de un beneficio	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Incumplimiento de la guía informática que especifica los requerimientos de uso	
Tipos de entidades	PER_UTI: Usuarios PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Falta de control de las necesidades materiales para desarrollar una aplicación	
Tipos de entidades	PER_DEV: Desarrollador
Ausencia de normas morales o éticas	
Tipos de entidades	PER_DEV: Desarrollador
Falta de gestión del parque de hardware	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	
Tipos de entidades	PHY_LIE.3: Zona

	PHY_LIE.2: Locales
Falta de registro del ingreso de personas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de protección de las líneas y equipos de comunicación	
Tipos de entidades	PHY_SRV.1: Comunicación
Los equipos permiten utilizar los recursos del sistema desde el exterior del organismo	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Los equipos son accesibles a todos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Los equipos están conectado a redes externas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Los equipos utilizados permiten usos diferentes de los previstos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
El dispositivo utilizado permite usos diferentes de los previstos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
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)	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Ausencia de normas de acceso	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El hardware está conectado a redes externas	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

El dispositivo es accesible a todos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 33 - USO ILÍCITO DEL HARDWARE	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.34 COPIA ILEGAL DE SOFTWARE

Falta de gestión de los privilegios asociados a los perfiles (administradores, usuarios, invitados...)	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de gestión de licencia, de dispositivo de registro y de activación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Software atractivo para el "público en general"	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de copiar fácilmente software o paquetes de programas	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de copiar fácilmente las versiones de los sistemas operativos propietarios	
Tipos de entidades	LOG_OS: Sistema operativo
Sistema operativo atractivo para el "público en general"	
Tipos de entidades	LOG_OS: Sistema operativo
Hardware que permite el registro de datos en soportes (disquete, ZIP, grabadora de CD/DVD)	
Tipos de entidades	MAT_ACT.1: Hardware portátil
Hardware que permite el registro de datos en soportes (disquete, ZIP, grabadora de CD-ROM/DVD)	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Desinformación sobre las leyes y los reglamentos que se aplican al tratamiento de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de control de las licencias impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales sobre el uso de copias ilegales de software	

Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de guía informática que especifique los requerimientos de uso	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de concienciación del personal sobre el riesgo de ser sancionado	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de concienciación o de información sobre la legislación referida a los derechos de autor	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de procedimiento de control	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Incumplimiento de la guía informática que especifica los requerimientos de uso	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Falta de concienciación sobre los riesgos de sanciones	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEC: Nivel de toma de decisiones
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de registro del ingreso de personas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
No se realiza ninguna verificación del origen de las aplicaciones antes de su instalación	

Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

El dispositivo de acceso permite el almacenamiento de software

Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

El dispositivo de acceso permite la descarga de software

Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema

VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 34 - COPIA ILEGAL DE SOFTWARE

Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión

	LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.35 USO DE SOFTWARE FALSIFICADO O COPIADO

Falta de gestión de licencia, de dispositivo de registro y de activación	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de copiar fácilmente software o paquetes de programas	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Software atractivo para el "público en general"	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de que los sistemas funcionen con sistemas operativos copiados en forma ilícita o falsificados	
Tipos de entidades	LOG_OS: Sistema operativo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de control de las licencias impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales sobre la identificación y la verificación del origen del software	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de concienciación o de información sobre la legislación referida a los derechos de autor	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de control de certificación de los productos	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control del origen de los productos	
Tipos de entidades	ORG_GEN: Organización del organismo
Ausencia de guía informática que especifique los requerimientos de uso	
Tipos de entidades	ORG_GEN: Organización del organismo
La política de seguridad no hace referencia a la notificación de las obligaciones y responsabilidades de cada uno en materia civil, penal y reglamentaria	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de definición de privilegios que limiten la posibilidad de realizar instalaciones en las estaciones de trabajo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de concienciación del personal sobre el riesgo de ser sancionado	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal

Incumplimiento de la guía informática que especifica los requerimientos de uso	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Ninguna certificación de los productos	
Tipos de entidades	PER_DEV: Desarrollador
Ningún procedimiento de evaluación de los productos	
Tipos de entidades	PER_DEV: Desarrollador
Falta de procedimiento y medios de verificación del origen del software (firma del código, del binario...)	
Tipos de entidades	PER_DEV: Desarrollador
Falta de registro del ingreso de personas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
No se realiza ninguna verificación del origen de las aplicaciones antes de su instalación	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El dispositivo de acceso permite el almacenamiento de software	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El dispositivo de acceso permite la descarga de software	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico

	SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 35 - USO DE SOFTWARE FALSIFICADO O COPIADO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.36 ALTERACIÓN DE DATOS

Falta de control de la integridad de los datos

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

Falta de procedimiento y de dispositivo de autorización para la modificación de datos

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

El enlace de mantenimiento remoto está permanentemente activado

Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de restricción en los puntos de ingreso del software

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

No se realiza ninguna verificación de las aplicaciones antes de su instalación

Tipos de entidades	SYS_MES: Correo electrónico LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de implementación de normas de seguridad de base aplicables al sistema operativo y al software

Tipos de entidades	SYS_MES: Correo electrónico LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

El software permite acceder a datos (contenido del disco duro, base de datos...)

Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
El sistema operativo permite acceder a datos (base de datos...)	
Tipos de entidades	LOG_OS: Sistema operativo
Contraseñas de conexión demasiado simples	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
No se realiza ninguna verificación del sistema operativo antes de su instalación	
Tipos de entidades	LOG_OS: Sistema operativo
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
El dispositivo SNMP está activado	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Ausencia de normas de protección de datos	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
El hardware puede ser inicializado por cualquier persona a partir de un periférico (ej.: disquete, CD-ROM)	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Hardware obsoleto	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de redundancia o procedimiento de respaldo de datos	
Tipos de entidades	MAT_ACT.2: Hardware fijo
Desgaste de los soportes	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT.3: Periférico de procesamiento
Falta de medios de protección y control de la integridad de los datos	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT.3: Periférico de procesamiento
Ausencia de normas y de procedimientos sobre la autorización del personal	

Tipos de entidades	ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de gestión y de control de las autorizaciones impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de protección de la información impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de permisos de acceso a la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de seguridad de los accesos al SI (pasarelas, detección de intrusos, supervisión de los acontecimientos de seguridad,...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de cláusulas contractuales referidas a la protección del material informático	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control de la aplicación de la política de seguridad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de instrucciones referidas al uso del material informático	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de prevención y de detección de virus y otros programas maliciosos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de control de acceso a la información	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de plan de formación sobre los problemas de seguridad	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de procedimientos de control de los disquetes provenientes de fuera del organismo	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Ausencia de guía informática que especifique los requerimientos de uso	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Incumplimiento de la guía informática que especifica los requerimientos de uso	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de protección y clasificación de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento

	PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de concienciación del personal sobre el riesgo de ser sancionado	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Personal manipulable	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Situación conflictiva entre personas	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de procedimientos de control de la identidad de toda persona que ingrese en los diferentes locales o zonas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de registro del ingreso de personas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de protección de las líneas y equipos de comunicación	
Tipos de entidades	PHY_SRV.1: Comunicación
Falta de protección física y lógica (aislamiento...)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Posibilidad de actuar sobre los datos enviados utilizando los medios de comunicación	
Tipos de entidades	RES_INF: Medios y soportes

La red permite modificar los recursos del sistema o actuar sobre ellos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
La red facilita el uso de los recursos por parte de personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Falta de dispositivo sólido de control de acceso	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
Falta de procedimiento respaldo de datos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_ANU: Directorio de la empresa
El dispositivo permite borrar, modificar o instalar programas en forma remota	
Tipos de entidades	SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet
El dispositivo permite introducir programas hostiles tales como troyanos, virus, gusanos, bombas lógicas...	
Tipos de entidades	SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet
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)	
Tipos de entidades	SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet
Falta de aislamiento entre las redes de comunicación	
Tipos de entidades	SYS_ITR: Intranet
El correo electrónico permite gestionar el funcionamiento asíncrono de ciertas partes o comandos del sistema operativo (ej.: envío automático de ficheros adjuntos)	
Tipos de entidades	SYS_MES: Correo electrónico
Falta de auditorías o de supervisión de los accesos	
Tipos de entidades	SYS_WEB: Portal externo
Ausencia de normas de acceso	
Tipos de entidades	SYS_WEB: Portal externo
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 36 - ALTERACIÓN DE LOS DATOS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo

	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.37 TRATAMIENTO ILÍCITO DE LOS DATOS

Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de dispositivo de cifrado	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de utilizar un acceso oculto (puerta falsa) o un troyano en el sistema operativo	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión
Falta de protección física	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento
Falta de medio de identificación de la sensibilidad de los datos que contienen los soportes	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Los soportes son accesibles a todos	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Soportes atractivos (valor mercantil, tecnológico, estratégico)	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Soportes móviles o fácilmente transportables (ej.: disquete, ZIP, disco duro extraíble)	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de medio de cifrado	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de procedimiento y medio de destrucción	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Desinformación sobre las leyes y los reglamentos que se aplican al tratamiento de la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

	ORG_DEP: Organización de la cual depende el organismo
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política de protección de la información impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusula contractual de confidencialidad	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de dispositivo de control y de sanción	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de instrucciones referidas a los incidentes (detección, acción...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de control de acceso a la información	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de concienciación sobre las responsabilidades individuales	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de designación de un responsable de la protección de datos e informaciones vinculadas con los individuos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
La política de seguridad no se aplica, particularmente en lo que se refiere al tratamiento de los datos personales	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de concienciación del personal	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de protección y de auditorías de acceso a los datos delicados	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de concienciación del personal sobre el riesgo de ser sancionado	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de formación que especifique las condiciones de uso lícito de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de protección y clasificación de la información	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal

Desconocimiento de las medidas de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Presencia de un acceso de escucha ilícito	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
Falta de identificación de los niveles de protección de los sistemas	
Tipos de entidades	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Falta de control del contenido	
Tipos de entidades	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Falta de auditorías o de supervisión de los accesos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Falta de gestión de autorización de los accesos	
Tipos de entidades	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
El dispositivo facilita la divulgación de información fuera del organismo	
Tipos de entidades	SYS_MES: Correo electrónico SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
El dispositivo está conectado a redes externas	
Tipos de entidades	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 37 - TRATAMIENTO ILÍCITO DE LOS DATOS	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares

	PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.38 ERROR DE USO

Falta de documentación explícita sobre las aplicaciones	
Tipos de entidades	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Conocimientos técnicos insuficientes del usuario	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_INT: Interfaz de comunicación MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de procedimientos de prueba y de recepción conforme a las especificaciones	
Tipos de entidades	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de validación de los datos de entrada (de ingreso)	
Tipos de entidades	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de responsabilidad	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Aplicación de uso complejo	
Tipos de entidades	LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar

Falta de asistencia al usuario accesible	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet

	SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Uso no intuitivo del software	
Tipos de entidades	LOG_OS: Sistema operativo
Conocimientos técnicos insuficientes	
Tipos de entidades	LOG_OS: Sistema operativo
Falta de asistencia accesible	
Tipos de entidades	LOG_OS: Sistema operativo
Falta de formación en el uso y mantenimiento del nuevo software	
Tipos de entidades	LOG_OS: Sistema operativo
Software de uso complejo	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión
Hardware de uso complejo o poco ergonómico	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Malas condiciones de uso	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware
Posibilidad de que cierto hardware provoque perjuicios al personal usuario (trabajo frente a un monitor, ondas...)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de etiquetado de los soportes	

Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Soportes de uso complejo o poco ergonómico	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de un control de los procesos críticos por parte del organismo central	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de doble control de los procesos críticos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de formación referida al hardware o software utilizado	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Desconocimiento de las responsabilidades	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de formalización de las responsabilidades conocidas por todos	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Condiciones de trabajo desfavorables	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Falta de profesionalismo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Incumplimiento de las instrucciones	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Personal usuario que ha recibido poca formación o formación de mala calidad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de documentación sobre el uso de las aplicaciones existentes	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Falta de motivación para los trabajos vinculados con el ingreso de datos	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Personal poco acostumbrado al ingreso de datos	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador

Entorno de trabajo desfavorable (locales demasiado pequeños, falta de espacio para ubicar los elementos de trabajo...)	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de etiquetado de los cables o falta de plano del cableado	
Tipos de entidades	PHY_SRV.1: Comunicación
Espacio insuficiente en los locales técnicos	
Tipos de entidades	PHY_SRV.1: Comunicación
Falta de procedimiento de uso	
Tipos de entidades	PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía
Falta de etiquetado y de esquema de diseño actualizado	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
Falta de plano del cableado	
Tipos de entidades	RES_INF: Medios y soportes
Interfaz que incorpora características técnicas referidas al país (ej.: conexiones telefónicas diferentes entre Francia y el Reino Unido)	
Tipos de entidades	RES_INT: Interfaz de comunicación
Medios y soportes que incorporan características técnicas específicas de su localización (ej.: diferentes parámetros de configuración ADSL entre Francia y el Reino Unido)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
Falta de medidas de protección (sólo lectura...)	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
Falta de herramientas de supervisión	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 38 - ERROR DE USO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales

	PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.39 ABUSO DE DERECHO

Ausencia de una política de auditorías	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de respaldo de los registros de acontecimientos	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de registro de los acontecimientos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Contraseñas de conexión demasiado simples	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	
Tipos de entidades	LOG_OS: Sistema operativo
La base de contraseñas del sistema operativo puede descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
El dispositivo SNMP está activado	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo
El enlace de mantenimiento remoto está permanentemente activado	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota	

Tipos de entidades	LOG_OS: Sistema operativo
Los logs o registros del sistema operativo pueden ser modificados por todos	
Tipos de entidades	LOG_OS: Sistema operativo
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo no actualiza los registros o los acontecimientos del sistema	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite realizar conexiones anónimas	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite abrir una sesión sin ingresar la contraseña	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	
Tipos de entidades	LOG_OS: Sistema operativo
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	
Tipos de entidades	LOG_OS: Sistema operativo
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	
Tipos de entidades	LOG_OS: Sistema operativo
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión
Falta de protección física	
Tipos de entidades	MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de dispositivo sólido de control de acceso	
Tipos de entidades	MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de auditorías de los procedimientos de control de acceso físico	
Tipos de entidades	MAT_PAS.2: Otros soportes
Ausencia de una política de gestión y de control de las autorizaciones impuesta a los establecimientos del organismo	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de cláusulas contractuales que limiten las responsabilidades de ambas partes	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de definición del derecho de conocer la información	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

Falta de dispositivo de control y de sanción	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de un reglamento que defina los derechos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Las atribuciones de los usuarios no están claramente definidas	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de control de las atribuciones de los derechos de los usuarios	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Preeminencia de la categoría de personal	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Para el personal, no está definida la noción de derecho	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de protección física y lógica	
Tipos de entidades	RES_INF: Medios y soportes
No se aplica el principio del menor privilegio	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo

	RES_INT: Interfaz de comunicación
Posibilidad de utilizar los recursos sin generar trazas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
El dispositivo es accesible a todos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 39 - ABUSO DE DERECHO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.40 USURPACIÓN DE DERECHO

Ausencia de una política de auditorías	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de respaldo de los registros de acontecimientos	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de registro de los acontecimientos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Los logs o registros del sistema operativo pueden ser modificados por todos	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite abrir una sesión sin ingresar la contraseña	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite realizar conexiones anónimas	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo no actualiza los registros o los acontecimientos del sistema	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	
Tipos de entidades	LOG_OS: Sistema operativo
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	
Tipos de entidades	LOG_OS: Sistema operativo
La base de contraseñas del sistema operativo puede descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
El dispositivo SNMP está activado	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación

	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
El enlace de mantenimiento remoto está permanentemente activado	
Tipos de entidades	SYS_MES: Correo electrónico RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación LOG_OS: Sistema operativo
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
Contraseñas de conexión demasiado simples	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	
Tipos de entidades	SYS_MES: Correo electrónico LOG_OS: Sistema operativo
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión
El hardware está conectado a redes externas	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de dispositivo sólido de control de acceso	
Tipos de entidades	RES_REL: Repetidor pasivo o activo MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de aislamiento de los equipos	
Tipos de entidades	MAT_ACT.3: Periférico de procesamiento
Falta de protección de los soportes	
Tipos de entidades	MAT_PAS.1: Soporte electrónico
Falta de auditorías de los procedimientos de control de acceso físico	
Tipos de entidades	MAT_PAS.2: Otros soportes
Los responsables no tienen contacto con los servicios de expertos o de vigilancia tecnológica	

Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de normas y de procedimientos sobre la autorización del personal	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de concienciación sobre los riesgos de sanciones	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de procedimiento de control	
Tipos de entidades	ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de protección de los espacios dedicados a intercambiar o a compartir información	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de procedimiento de autorización del personal	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de un clima de confianza entre los individuos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_EXT: Subcontratistas - Proveedores - Industriales
Las responsabilidades de seguridad en cuanto a la gestión de los permisos no han sido formalizadas	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de comunicación y de información de los procedimientos de autorización del personal	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de procedimiento de envío de informe en caso de detección de anomalías	
Tipos de entidades	ORG_GEN: Organización del organismo
La política de seguridad no se aplica	
Tipos de entidades	ORG_GEN: Organización del organismo
Organización no adaptada	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Derechos otorgados fuera de la legítima necesidad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Situación conflictiva entre personas	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones

	PER: Personal
Ausencia de normas morales o éticas	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Existen operaciones muy delicadas que sólo debe poder realizar una sola persona	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Misiones poco adaptadas al personal	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Falta de procedimientos de control de los permisos del personal que accede al establecimiento o a los locales	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Falta de protección física y lógica (aislamiento...)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red
Falta de aislamiento de la red	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
Las interfaces están conectadas a redes externas	
Tipos de entidades	RES_INF: Medios y soportes
Los soportes y los medios están conectados a redes externas	
Tipos de entidades	RES_INF: Medios y soportes
Posibilidad de modificar características técnicas (ej.: dirección MAC de una tarjeta Ethernet)	
Tipos de entidades	RES_INF: Medios y soportes
Falta de protección física	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
La red permite modificar los recursos del sistema o actuar sobre ellos	

Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Presencia de un protocolo que no dispone de función de autenticación	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Las interfaces son accesibles a todos	
Tipos de entidades	RES_INT: Interfaz de comunicación
La red facilita el uso de los recursos por parte de personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
Los repetidores no identifican ni las fuentes ni los destinos (ejemplo de impacto: sistema vulnerable a los ataques basados en "spoofing")	
Tipos de entidades	RES_REL: Repetidor pasivo o activo
El dispositivo es accesible a todos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
Posibilidad de que el dispositivo esté sometido a peticiones o datos mal formados (ej.: buffer overflow)	
Tipos de entidades	SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa
No se realiza ningún control de las aplicaciones antes de su instalación	
Tipos de entidades	SYS_MES: Correo electrónico
Se puede acceder al dispositivo de correo electrónico desde Internet	
Tipos de entidades	SYS_MES: Correo electrónico
Utilización de una versión obsoleta del servidor de correo electrónico	
Tipos de entidades	SYS_MES: Correo electrónico
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 40 - USURPACIÓN DE DERECHO	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal

	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.41 NEGACIÓN DE ACCIONES

Ausencia de una política de auditorías	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software
Falta de respaldo de los registros de acontecimientos	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
Falta de registro de los acontecimientos	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar
El sistema operativo no actualiza los registros o los acontecimientos del sistema	
Tipos de entidades	LOG_OS: Sistema operativo
El dispositivo SNMP está activado	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota con herramientas de gestión no cifradas	
Tipos de entidades	LOG_OS: Sistema operativo
Ficheros de imputación complejos o poco ergonómicos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes LOG_OS: Sistema operativo
Contraseñas de conexión demasiado simples	
Tipos de entidades	LOG_OS: Sistema operativo
Las contraseñas ingresadas para acceder al sistema operativo pueden descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
La base de contraseñas del sistema operativo puede descifrarse fácilmente	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite realizar conexiones anónimas	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de que el sistema operativo esté sometido a peticiones o datos mal formados (ej.: buffer	

overflow)	
Tipos de entidades	LOG_STD: Paquete de programas o software estándar LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota desde cualquier puesto	
Tipos de entidades	LOG_OS: Sistema operativo
Uso de una versión obsoleta del sistema operativo o de las aplicaciones	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo es accesible y puede ser utilizado por todos (ej.: conexión a la cuenta "invitado")	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de gestionar el sistema en forma remota	
Tipos de entidades	LOG_OS: Sistema operativo
Los logs o registros del sistema operativo pueden ser modificados por todos	
Tipos de entidades	LOG_OS: Sistema operativo
Posibilidad de inicializar varios sistemas operativos en la misma máquina (ej.: acceso a las particiones NTFS vía Linux)	
Tipos de entidades	LOG_OS: Sistema operativo
El sistema operativo permite abrir una sesión sin ingresar la contraseña	
Tipos de entidades	LOG_OS: Sistema operativo
El enlace de mantenimiento remoto está permanentemente activado	
Tipos de entidades	LOG_OS: Sistema operativo
Los recursos compartidos facilitan el uso del sistema por parte de personas no autorizadas	
Tipos de entidades	LOG_OS: Sistema operativo
Software que puede ser utilizado por todos (ej.: falta de contraseña requerida para la gestión remota de un puesto)	
Tipos de entidades	LOG_SRV: Software de servicio, mantenimiento o gestión
Falta de dispositivo de trazas y de auditoría	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
El hardware es accesible y puede ser utilizado por todos	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Los soportes son accesibles a todos	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Falta de procedimiento de acceso a la información clasificada	
Tipos de entidades	MAT_PAS.2: Otros soportes
Cambio de política o de estrategia de organización	
Tipos de entidades	PER_UTI: Usuarios PER_DEC: Nivel de toma de decisiones ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de definición de las responsabilidades	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo

	ORG_DEP: Organización de la cual depende el organismo
Falta de definición referida a las responsabilidades de seguridad de los sistemas de información en el reglamento interno	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de procedimientos disciplinarios	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Presencia de un interés político-económico	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Ausencia de una política global de gestión y de archivado de las trazas y otros elementos de prueba	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Falta de cláusula contractual referida a la definición de los procedimientos de comunicación e intercambio de información	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de control mutuo de códigos	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Presencia de cláusula de multa o sanción desmesurada o no adaptada al contexto	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Ausencia de un mecanismo de seguimiento de actividad, de registros de acontecimientos y de alertas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Posibilidad de utilizar los recursos del organismo sin control (hardware de libre uso...)	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de estructura jerárquica y procedimientos de informes	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Ausencia de funciones de auditoría separadas de las funciones de seguimiento	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de apoyo por parte de la dirección a la aplicación de la política de seguridad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal
Obtención de un beneficio	
Tipos de entidades	PER_UTI: Usuarios PER_DEC: Nivel de toma de decisiones
Falta de confianza en la organización	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
No se conoce la responsabilidad de cada uno	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Situación conflictiva entre personas	
Tipos de entidades	PER_UTI: Usuarios

	PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones
Falta de registro histórico de las entradas y salidas de personas	
Tipos de entidades	PHY_LIE.3: Zona PHY_LIE.2: Locales
Los repetidores son accesibles a todos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
El soporte de comunicación permite utilizar los servicios del sistema desde el exterior del organismo	
Tipos de entidades	RES_INF: Medios y soportes
Los soportes y medios son accesibles a todos y están activos por defecto (ej.: conjunto de conectores RJ45 fijos)	
Tipos de entidades	RES_INF: Medios y soportes
La red facilita el uso de los recursos por parte de personas no autorizadas	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
El protocolo no permite la identificación segura del emisor	
Tipos de entidades	RES_INT: Interfaz de comunicación
La red permite modificar los recursos del sistema o actuar sobre ellos	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación
El protocolo no permite el envío de acuses de recibo	
Tipos de entidades	RES_INT: Interfaz de comunicación
Posibilidad de utilizar los recursos sin generar trazas	
Tipos de entidades	RES_INT: Interfaz de comunicación
El dispositivo de acceso no registra las trazas provenientes de su uso	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El acceso al dispositivo de trazas no está protegido	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El dispositivo es accesible a todos (ej.: dispositivo que no autentica las estaciones de trabajo de clientes ni los usuarios)	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
El dispositivo está conectado a redes externas	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet

	SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 41 - NEGACIÓN DE ACCIONES	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

4.42 DAÑO A LA DISPONIBILIDAD DEL PERSONAL

Posibilidad de que cierto hardware provoque perjuicios al personal usuario (trabajo frente a un monitor, ondas...)	
Tipos de entidades	MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil
Falta de procedimiento de archivado	
Tipos de entidades	MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico
Presencia de un clima social desfavorable	
Tipos de entidades	ORG_DEP: Organización de la cual depende el organismo
Presencia de un conflicto político-económico entre el país de origen de la organización y el país que la acoge	
Tipos de entidades	ORG_GEN: Organización del organismo ORG_DEP: Organización de la cual depende el organismo
Falta de cláusulas o procedimientos de transferencia de los conocimientos	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de continuidad financiera o tecnológica del organismo	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de cláusula de continuidad de provisión del servicio	
Tipos de entidades	ORG_EXT: Subcontratistas - Proveedores - Industriales
Falta de elementos para la protección del personal	
Tipos de entidades	ORG_GEN: Organización del organismo
Presencia de una epidemia viral local	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de procedimientos de transferencia de conocimientos	
Tipos de entidades	PER_UTI: Usuarios ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Presencia, en la organización, de un clima social desfavorable para la actividad	
Tipos de entidades	ORG_GEN: Organización del organismo
Falta de plan de concienciación y de formación sobre los procedimientos de contingencia para las actividades profesionales	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo
Falta de procesos de gestión de la continuidad de las actividades profesionales del organismo	
Tipos de entidades	ORG_GEN: Organización del organismo
Subdimensionamiento de la organización	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de suplentes del personal estratégico	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de estructura redundante de las funciones delicadas	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de procesos de gestión de la continuidad de las actividades profesionales del equipo de proyecto	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema

Ausencia de base documental de las normas y procedimientos	
Tipos de entidades	ORG_PRO: Organización de un proyecto o sistema
Falta de disponibilidad provocada por una actitud competitiva	
Tipos de entidades	PER_DEC: Nivel de toma de decisiones
Falta de disponibilidad por causa de enfermedad	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Falta de disponibilidad debida al ausentismo	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Falta de disponibilidad provocada (agresión física, toma de rehenes...)	
Tipos de entidades	PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Problemas sociales	
Tipos de entidades	PER_EXP: Operador del sistema - Mantenimiento PER_DEV: Desarrollador
Clima social conflictivo	
Tipos de entidades	PER_UTI: Usuarios
Clima social complicado que puede provocar huelgas de transporte	
Tipos de entidades	PHY_LIE.1: Entorno externo
Personal especializado alojado en locales remotos	
Tipos de entidades	PHY_LIE.2: Locales
Personal que reside lejos de los locales del organismo	
Tipos de entidades	PHY_LIE.2: Locales
Posibilidad de consecuencias nocivas para el personal usuario (transmisión por vía hertziana, ondas...)	
Tipos de entidades	RES_REL: Repetidor pasivo o activo RES_INF: Medios y soportes
VULNERABILIDADES VINCULADAS CON EL MÉTODO DE ATAQUE 42 - PERJUICIOS A LA DISPONIBILIDAD DEL PERSONAL	
Tipos de entidades	SYS_WEB: Portal externo SYS_MES: Correo electrónico SYS_ITR: Intranet SYS_INT: Dispositivo de acceso a Internet SYS_ANU: Directorio de la empresa SYS: Sistema RES_REL: Repetidor pasivo o activo RES_INT: Interfaz de comunicación RES_INF: Medios y soportes RES: Red PHY_SRV: Servicio esencial PHY_SRV.3: Refrigeración - Contaminación PHY_SRV.2: Energía PHY_SRV.1: Comunicación PHY_LIE: Lugares PHY_LIE.3: Zona PHY_LIE.2: Locales PHY_LIE.1: Entorno externo PER_UTI: Usuarios PER_EXP: Operador del sistema - Mantenimiento

	PER_DEV: Desarrollador PER_DEC: Nivel de toma de decisiones PER: Personal ORG_PRO: Organización de un proyecto o sistema ORG_GEN: Organización del organismo ORG_EXT: Subcontratistas - Proveedores - Industriales ORG_DEP: Organización de la cual depende el organismo ORG: Organización MAT_PAS: Soporte de datos (pasivo) MAT_PAS.2: Otros soportes MAT_PAS.1: Soporte electrónico MAT_ACT: Soporte de procesamiento de datos (activo) MAT_ACT.3: Periférico de procesamiento MAT_ACT.2: Hardware fijo MAT_ACT.1: Hardware portátil MAT: Hardware LOG_STD: Paquete de programas o software estándar LOG_SRV: Software de servicio, mantenimiento o gestión LOG_OS: Sistema operativo LOG_APP: Aplicación profesional LOG_APP.2: Aplicación profesional específica LOG_APP.1: Aplicación profesional estándar LOG: Software

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