AMSTRO

POLÍTICA DE SEGURIDAD CORPORATIVA DE AMSTRO

AMSTRO

DATOS SOBRE LA PRESENTA EDICIÓN

Nº DE VERSIÓN	FECHA	RESUMEN DE CAMBIOS / COMENTARIOS
2	15/09/2022	Adaptación política AMSTRO
2	04/10/2022	Modificación apartado 8
3	25/05/2023	Adaptación ISO 27001/2022
4	21/03/2024	Revisión y actualización anual; adaptación a otras partes interesadas, nueva clasificación documento a pública
5	15/05/2025	Se añade la figura de DPD
5	10/04/2026	Revisión anual

	ELABORADO	APROBADO
NOMBRE	CISO EXTERNO/Responsable Seguridad	Comité de Seguridad
FECHA	14 de septiembre de 2022	15 de septiembre de 2022

AMSTRO

Contenido

AMSTRO

AMSTRO

1. Introducción

Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, uso previsto y valor de la información tratada o los servicios prestados.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que se deban aplicar las medidas mínimas de seguridad exigidas por la legislación de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Esta Política de Seguridad de la Información se integrará a la normativa básica de AMSTRO, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

2. Objetivo

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Es esencial dar a conocer y concienciar a todo el personal, tanto interno como externo, que preste sus servicios en AMSTRO sobre la estrategia de seguridad de la organización y definir las líneas estratégicas generales de actuación para evitar amenazas y reaccionar ante incidentes de seguridad.

La Política de Seguridad establece los principios básicos y requisitos mínimos de seguridad necesarios para proteger la información, así como la tecnología utilizada para su procesamiento, estableciendo las directrices para la implantación de medidas organizativas, técnicas y legales y define los responsables de su desarrollo, implantación y gestión.

La implantación de dichas medidas se realizará de forma preventiva, reactiva, dinámica y mediante mecanismos de detección, que garanticen en todo momento la preservación de la información, y el cumplimento de las leyes en vigor que afecten a su uso y tratamiento.

3. Alcance

El alcance de la Política de Seguridad se centra en la información y los recursos de procesamiento de la información de todos los Sistemas de Información que usa, administra, o custodia AMSTRO.

Asimismo, la Política de Seguridad cumple con las especificaciones de las normas UNE-ISO/IEC 27001 y el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

4. Destinatarios

La presente Política de Seguridad de la Información de AMSTRO será de aplicación y de obligado cumplimiento para todo el personal de AMSTRO o terceros, que presten servicios en el mismo independiente de la forma de contratación y vinculación con el mismo, de manera permanente o eventual, que en el desempeño de sus funciones o parte de ellas desarrolle su trabajo fuera de sus instalaciones, en adelante los usuarios.

Será el Comité de Seguridad el encargado de la custodia y divulgación de la versión aprobada de este documento.

5. Contenido de la Política de Seguridad

El contenido de la presente Política trata de identificar, en primer lugar, a los responsables encargados de velar por la seguridad de la información y protección de datos de carácter personal de AMSTRO. Así mismo, en esta Política se contiene:

- Los objetivos en materia de seguridad que persigue AMSTRO.
- El marco legal en el que se desarrolla su actividad.
- La estructura del Comité de Seguridad de la Información y Protección de Datos de Carácter Personal, desarrollando su ámbito de responsabilidades, los miembros y la relación con otros elementos de AMSTRO.

- Definición de las funciones de seguridad, definiendo por cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

6. Marco legal y regulatorio

En este apartado se recogen las normas más significativas correspondientes al ámbito de la seguridad de la información y la protección de datos:

- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Leyes y normativa aplicables a las diferentes líneas de negocio de AMSTRO.

7. Organización de la seguridad en AMSTRO

La estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información de AMSTRO, estará compuesta por:

7.1 Definición de Roles

La Política de Seguridad, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. Se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información:

7.1.1 Responsable de la Información y del Servicio

Se ha designado responsable de la Información a Albert Borràs, Director General de AMSTRO, u órgano en quien delegue, a quien le corresponden las siguientes funciones:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los tratamientos de datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Determinará los niveles de seguridad en cada dimensión dentro del marco establecido en la Norma UNE-ISO/IEC 27001)
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

7.1.2 Responsable de Seguridad de la Información

Se ha designado como responsable de Seguridad de la Información a Cristina Hidalgo, Compliance Officer, a quien le corresponderán las siguientes funciones:

- Coordinará y controlará las medidas definidas en el Registro de actividades del tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

7.1.3 Delegado de Protección de Datos

Se ha designado como Delegada de Protección de Datos a **Cristina Hidalgo Cerrato, Responsable de Compliance**. Las funciones de la Delegada de Protección de Datos se encuentran especificadas en el artículo 39 del RGPD, siendo las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

La delegada de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

7.2 Comité de Seguridad de la Información

El Comité de Seguridad de la Información y Protección de Datos de Carácter Personal (en adelante, el Comité) es un órgano colegiado, cuya competencia será velar por e impulsar la seguridad de la información y protección de los datos de carácter personal de AMSTRO.

7.2.1 Ambito de responsabilidad

El Comité se responsabiliza de alinear todas las actividades de AMSTRO en materia de seguridad de la información y protección de datos de carácter personal. En concreto:

- Coordina las actividades relacionadas con los sistemas de información y comunicaciones de AMSTRO.
- Es responsable de la redacción de la Política de Seguridad de la Información de AMSTRO.
- Es responsable de la creación y aprobación de las normas que emanan del uso de los sistemas de información de AMSTRO.
- Aprueba los procedimientos de actuación y calificación en lo relativo al uso de los sistemas de información.

- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).

7.2.2 Funciones del Comité

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Puesto que el Comité de Seguridad de la Información no es un comité técnico, deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

- Grupos de trabajo especializados, internos, externos o mixtos, o bien a través de asesoría externa.
- Asesoría externa.

7.2.3 Composición del Comité:

El Comité estará conformado por:

a) **Presidente**: cargo que será ocupado por un miembro de la **Gerencia de AMSTRO** quien asumirá las siguientes competencias: Se propone al **Director General: Albert Borràs**

- Convocar las reuniones periódicas del Comité.
- Dirigir el Comité, proponiendo los distintos puntos a tratar en las reuniones periódicas.
- Realizar el seguimiento de los distintos proyectos y equipos de trabajo que hayan surgido como respuesta a objetivos estratégicos y tácticos.
- Comunicar al resto de comités de la AMSTRO las directrices claras a tener en cuenta en relación a los proyectos en curso y requisitos de seguridad que les puedan afectar.
- Nombrar, a propuesta del Secretario, al resto de los miembros del Comité.

b) **Secretario:** es el Responsable de Seguridad: **Se propone a Cristina Hidalgo como persona indicada para el puesto.**

- Convocar las reuniones periódicas, así como las extraordinarias del Comité.
- Preparar los temas a tratar en las reuniones del comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Ser responsable de la ejecución directa o delegada de las decisiones del Comité.

Importante: no actuará en el Comité bajo la denominación de delegado de protección de datos, sino como Responsable de Seguridad, para que exista un solapamiento de funciones que puedan generar controversia.

c) **Vocales:**

- Director IT: Antoni Batlle
- Directora RRHH: Marta Bertrán

(Podrán delegar en el equipo técnico necesario propio de su gerencia).

7.2.4 Delegación de funciones

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el Comité, a propuesta del responsable de seguridad, podrá designar responsables de seguridad delegados, en el número que considere necesario, que tendrán dependencia funcional directa del responsable de seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

7.2.5 Funcionamiento

El Comité se reunirá como mínimo, una vez al trimestre (cuatro veces al año), y de forma extraordinaria, siempre que el Presidente lo considere pertinente, así como de forma inmediata tras un incidente de seguridad que afecte a la seguridad de la información de AMSTRO, o a los datos de carácter personal custodiados por el mismo.

AMSTRO

ELABORACIÓN DEL ACTA

Los temas que se adopten en las reuniones deberán estar alineados con la definición de los objetivos de seguridad que se traten de alcanzar dentro de cada plan de mejora de acciones correctivas y preventivas, así como los objetivos por los cuales se constituye el Comité y las competencias que ostenta.

Después de cada reunión el Secretario levantará acta, que deberá ser firmado en todo caso, por el Presidente.

Las actas contendrán:

1. Detalles de la Reunión: asistentes, convocatoria, fecha, convocante.
2. Lugar de reunión y asunto a tratar.
3. Resultado de las auditorias o revisiones de análisis de riesgos.
4. Estado de los planes de acciones correctivas, preventivas y en materia de formación.
5. Definición y asignación de los objetivos, concretos y cuantificables, en materia de seguridad de la información y protección de datos, así como análisis de su cumplimiento.
6. Técnicas y procedimientos implantados para mejorar la eficacia de la Seguridad.
7. Vulnerabilidad o amenazas no abordadas en el análisis de riesgos.
8. Resultados de las mediciones de eficacia.
9. Acciones de seguimiento de las revisiones anteriores.
10. Cambios que pudieran afectar a la gestión de seguridad de la información de AMSTRO.
11. Recomendaciones de mejora.

8. Procedimientos de designación de personas

La Dirección de la Organización nombrará formalmente:

- Al Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- A los Responsables del Servicio; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
- Al Responsable de la Seguridad, que debe reportar directamente al Comité de Seguridad de la Información.
- Al Responsable del Sistema, que debe reportar directamente al Comité de Seguridad de la Información.

La Dirección de la Organización designa al Administrador de Seguridad del Sistema a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

9. Datos de carácter personal

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes, así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

De acuerdo con el Reglamento General de Protección de Datos, AMSTRO tanto en calidad de Responsable del tratamiento, como de Encargado del tratamiento, cuándo proceda debido a la prestación de servicios proporcionada a sus clientes, cumplirá en todo momento con los principios exigidos al tratar datos personales:

- Principio de "licitud, transparencia y lealtad", que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de "finalidad" que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.

- Principio de "minimización de datos", es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.
- Principio de "exactitud", que obliga a los responsables a disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- Principio de "limitación del plazo de conservación" que constituye una de las materializaciones del principio de minimización. La conservación de esos datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.
- Principio de "seguridad" que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.
- Principio de "responsabilidad activa" o "responsabilidad demostrada" que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

10.Directrices de Seguridad de la Información

Las directrices de la Política de Seguridad serán desarrolladas de acuerdo con la normativa en materia de protección de datos.

a) **Organización e implantación del proceso de seguridad**

La seguridad de la información y protección de los datos de carácter personal deberá comprometer a todos los miembros de AMSTRO. En el presente documento se identifican a los responsables de velar por el cumplimiento de la presente Política y ponerla en conocimiento de todos los miembros de la organización administrativa.

b) **Análisis y Gestión de riesgos**

Este proceso comprende las fases de categorización de los sistemas y servicios, identificación de los activos, responsables, análisis de los riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas. De ser necesario, se elaborará un Plan de Tratamiento de Riesgos.

Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambien los sistemas y/o servicios prestados.
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves.

Será el Comité de Seguridad el encargado de que se lleve a cabo el preceptivo análisis de riesgos. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, las cuales serán reevaluadas y actualizadas periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

c) **Gestión de Personal**

Todos los miembros de AMSTRO deberán ser formados e informados de sus deberes y obligaciones en materia de seguridad y protección de datos de carácter personal. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

Su formación y concienciación será necesaria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema se concretará y plasmará en las normas internas de seguridad de AMSTRO.

Será el Comité de Seguridad el encargado de fomentar la concienciación de los usuarios de los sistemas para alcanzar un grado de madurez en la formación seguridad de la información, por lo que deberá disponer de los medios necesarios para que la información llegue a los afectados.

Con la periodicidad establecida por el Comité y, al menos, una vez al año, se llevarán a cabo formaciones en aquellos temas que se haya detectado que se encuentran en mayor situación de olvido, o que por la criticidad de la información, es necesario incidir en la importancia de adoptar buenas prácticas en su tratamiento y custodia. Se establecerá un programa de concienciación continua para atender a todos los miembros de AMSTRO, en particular a los de nueva incorporación.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de AMSTRO y a todas las actividades, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Así mismo, se definirán las exigencias de confidencialidad y no divulgación de datos para todos los miembros de AMSTRO, esta exigencia se definirá formalmente y todo el personal deberá firmar como prueba de recepción.

d) **Profesionalidad**

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal de AMSTRO recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de AMSTRO.

Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad al AMSTRO cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) **Autorización y control de los accesos**

El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

f) **Protección de las instalaciones**

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Por ello, en primer lugar, se ha de establecer un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

El acceso a los locales, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos, estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar si disponen de autorización para su acceso.

Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia y formalizarlas en instrucciones de acceso a los locales, que deberán ser comunicadas a todo el personal.

g) **Adquisición de productos de seguridad**

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por AMSTRO se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

La certificación indicada deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

h) **Seguridad por defecto**

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

i) **Integridad y actualización del sistema**

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

j) **Protección de la información almacenada y en transito**

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los siguientes

dispositivos: equipos portátiles, tabletas, dispositivos periféricos, soportes de información (pen-drive, disco duro) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por AMSTRO en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

k) **Prevención ante otros sistemas de información interconectados**

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, o a través de redes, con otros sistemas, y se controlará su punto de unión.

l) **Registro de actividad**

Con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

m) **Incidentes de seguridad**

Deben registrarse los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema, y detección de vulnerabilidades.

Se establecerá un sistema de detección y reacción frente a código dañino.

n) **Gestión de la continuidad del negocio**

La definición de planes de continuidad del negocio es indispensable para proteger los procesos y actividades críticas del negocio de contingencias o desastres, y para garantizar el restablecimiento del normal funcionamiento en plazos aceptables en términos de negocio.

El establecimiento de un plan de continuidad pasa por el análisis de cuáles son los requisitos de disponibilidad de los procesos del negocio y qué es el riesgo al cual están sometidos, a través de la determinación de cuál sería el impacto en caso de que se materializara un desastre, incidente de seguridad, pérdida de servicio o pérdida de disponibilidad, integridad y/o confidencialidad.

El análisis de impacto permite definir cuáles son los activos de información a proteger en función de su criticidad en términos de disponibilidad por el negocio, así como qué son los tiempos aceptables de recuperación. El plan de continuidad tendrá que tener en cuenta estos aspectos, así como la definición de la actuación esperada por parte de todas las personas implicadas, su formación, y la realización de como mínimo una prueba anual.

Hay que garantizar la actualización periódica del plan de continuidad, así como que esté disponible en situación de crisis o emergencia.

o) **~~Mejora continua del proceso de seguridad~~**

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

p) **Clasificación y Categoría de la información:**

~~Confidencialidad~~

En la tabla que se adjunta a continuación se especifican los criterios/directrices a seguir por parte de los empleados y colaboradores externos, con el objeto de marcar y clasificar la información en función de su nivel de confidencialidad, teniendo en cuenta el impacto que supondría su publicación, alteración o pérdida:

AMSTRO

Nivel	Descripción	Impacto	Tratamiento
Nivel 4 **SECRETA**	Información altamente restringida, concebida para el conocimiento de un grupo muy reducido de personas, de importancia estratégica para la compañía.	Elevadas pérdidas económicas Incumplimientos legales graves Desprestigio o perjuicio grave para la Compañía Toma de decisiones estratégicas erróneas	La documentación irá asociada a una lista de distribución.
Nivel 3 **CONFIDENCIAL**	Información accesible solamente a un grupo concreto de personas, áreas concretas o parte de ellas. Es el caso de: • Datos de carácter personal • Información generada o manejada por la Dirección de la Empresa de naturaleza reservada • Datos para procesos de autenticación, tanto de clientes como empleados: Números secretos, claves, PINs, etc.	Pérdidas económicas moderadas Incumplimientos legales Desprestigio o perjuicio para la Compañía Toma decisiones no estratégicas erróneas	Información de proyectos estratégicos de la Empresa. Sólo ha de ser accedida por un grupo restringido de personas.
Nivel 2 **INTERNA**	Información disponible de forma general para todo o gran parte del personal, aunque no puede ser divulgada públicamente, ya	Pérdidas económicas leves Incumplimientos legales leves Los procesos pueden depender levemente de su exactitud	Conocida y utilizada por todos los empleados de la Organización y personas externas debidamente autorizadas, la información la deben

Nivel	Descripción	Impacto	Tratamiento
	que se pretende que se de uso interno. Por defecto, cualquier información no clasificada en ninguno de los otros niveles se considerará interna.		conocer sólo quienes la necesitan para su trabajo, con autorización.
Nivel 1 **PÚBLICA**	Toda información no incluida en ninguno de los grupos anteriores y que no requiere de ninguna medida especial de protección. Información de uso interno y externo cuya pérdida o acceso no autorizado no tiene impacto negativo en la Compañía.	No causaría ningún prejuicio a la compañía Ningún proceso depende de su exactitud.	En este sentido, se trata de información sin restricciones de acceso que puede ser conocida y consultada por cualquier persona.

~~Disponibilidad~~

En la tabla que se adjunta a continuación se especifican los criterios/directrices a seguir por parte de los empleados y colaboradores externos, con el objeto de marcar y clasificar la información en función del tiempo en que se requerirá su disponibilidad.

Nivel	Descripción
Nivel 1 **(Alta Disponibilidad)**	Cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la Organización o a terceros.
Nivel 2 **(Media Disponibilidad)**	Cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la Organización o a terceros.
Nivel 3 y 4 **(Baja Disponibilidad)**	Cuya inaccesibilidad no afecta la operativa de la Organización.

~~Integridad~~

En la tabla que se adjunta a continuación se especifican los criterios/directrices a seguir por parte de los empleados y colaboradores externos, con el objeto de marcar y clasificar la información en función de la importancia de la integridad de la información.

Nivel	Descripción
Nivel 1 (Alta Integridad)	• Información para la que, debido a sus características o naturaleza (importancia para el negocio en términos económicos, de imagen, etc.), se debe garantizar la imposibilidad de modificación de la misma por parte de personal no autorizados o a través de métodos alternativos a su procesamiento habitual • Cuya **modificación no autorizada no podría repararse, ocasionando pérdidas graves** a la Organización o a terceros, con posibles repercusiones económicas y/o legales.
Nivel 2 (Media Integridad)	• Información de importancia para el negocio de la Compañía para la que deben establecer mecanismos o controles que impidan o detecten la modificación no autorizada de dicha información • Cuya **modificación no autorizada es difícil de reparar y podría ocasionar pérdidas significativas** para la Organización o a terceros, con posibles repercusiones significativas legales y/o económicas.
Nivel 3 (Baja Integridad)	• Dentro de este grupo se incluiría aquella información para la que, si bien sería recomendable la inclusión de controles que impidan o detecten su modificación no autorizada, su condición hace que dichos controles no sean imprescindibles. • Cuya **modificación no autorizada puede repararse fácilmente** o no afecta a la operativa de la Organización, **sin repercusiones** significativas legales y/o económicas.

11. Cuerpo Normativo: Estructuración de la documentación de seguridad del sistema, gestión y acceso

Las directrices de seguridad de la información indicadas en la presente Política de Seguridad se desarrollarán en un conjunto de documentos entre los que destacan, Políticas, Normativas, Guías, Procedimientos Operativos de Seguridad e Instrucciones de Trabajo.

La documentación sigue la siguiente estructura:

- El presente documento de Política de Seguridad del que emana el resto de documentos.
- Un documento de normativas que especifica los principios básicos y los requisitos mínimos de seguridad explicitados en la Norma ISO 27001 y enumera la relación de guías que es preciso desarrollar para lograr el cumplimiento de los citados principios básicos y requisitos mínimos de seguridad.
- Varios documentos guía donde se describe las actuaciones a desarrollar para implantar las medidas de seguridad enumeradas en la Norma ISO 27001.
- Varios documentos de procedimientos operativos de seguridad, registros, instrucciones de trabajo, manuales, etc., que se desarrollan como consecuencia de aplicar las guías.

12. Proceso de revisión

La Política de Seguridad deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de administración electrónica, a la evolución tecnológica y al desarrollo de la información.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Política, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad de AMSTRO.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

El Comité de Seguridad de AMSTRO se asegurará de que los documentos vigentes estén disponibles en AMSTRO para todo aquel que lo necesite.

Para evitar el uso no intencionado de documentos obsoletos, el Responsable de Seguridad de la Información mantendrá actualizada una carpeta informática identificada como "Obsoleto", separada del resto de documentación, a la cual no tendrá acceso el resto de personal, siendo restringido el uso al Responsable del Seguridad de la Información.

13. Terceros

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

14. Procedimiento Disciplinario

No se contempla un sistema disciplinario específico distinto al disponible en la empresa para cualquier conflicto laboral con los trabajadores o en los redactados en los contratos firmados con terceros. Estos se fundamentan en la normativa laboral vigente y en el Convenio Colectivo de oficinas y despachos de Catalunya y el Estatuto de los Trabajadores, y en caso de conflictos con terceros, conforme la legislación mercantil vigente,

El inicio de un proceso disciplinario o sancionador por motivos de Seguridad de la Información será incoado exclusivamente por la Dirección de AMSTRO y puede venir motivado por el incumplimiento de las medidas de uso adecuado de los sistemas.

15.Procedimiento de eliminación o expurgo de la información

Se adjunta como anexo I

16. Anexo. Glosario de términos

Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes: Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información: Caso concreto de un cierto tipo de información.

Política de seguridad: Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad: Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información: Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad: El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio: Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema: Persona que se encarga de la explotación del sistema de información.

Servicio: Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

AMSTRO

Auditoría de la seguridad: Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Categoría de un sistema: es un nivel, dentro de la escala básica-media-alta, con el que se clasifica un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. la categoría del sistema recoge la visión del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Barcelona 21 de Marzo 2024

Comité de Seguridad

AMSTRO

1. ANEXO I

PROCEDIMIENTO DE ELIMINACIÓN DE LA INFORMACIÓN O EXPURGO

AMSTRO

ÍNDICE DEL DOCUMENTO

2. Objeto

El objeto del presente documento es la definición del procedimiento de Eliminación de información empleado en AMSTRO de forma que se vele por la confidencialidad de los datos dando así cumplimiento a la legislación vigente.

Se ha implantado el siguiente procedimiento atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de AMSTRO.

3. Ambito de aplicación

Este procedimiento es de aplicación a todo el ámbito de actuación de AMSTRO, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de AMSTRO.

El presente procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en AMSTRO, especialmente a los usuarios como principales actores en sus respectivas competencias, de la generación y custodia de la información, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los sistemas tanto de información como no de AMSTRO.

En el ámbito del presente procedimiento, se entiende por usuario cualquier empleado público perteneciente o ajeno al AMSTRO, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con AMSTRO y que utilice o posea acceso a sus Sistemas de Información.

4. Actualización del documento

Cuando se produzca un cambio significativo en la estructura o en la operativa de AMSTRO que afecte a este procedimiento, deberá producirse una modificación y actualización del mismo.

Se levantará acta de los cambios y modificaciones identificados, y éstos serán incluidos en una nueva versión del documento, así como en el apartado de control de cambios,

como evidencia del proceso de actualización realizado y para mantener la trazabilidad entre distintas versiones.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. Referencias

Las referencias tenidas en cuenta para la redacción de este procedimiento han sido:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPDUE).
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

6. Descripción

La eliminación de los documentos constituye la fase final del ciclo de vida de un registro.

Los registros que contienen información privada o confidencial (por ejemplo, números de documento de identidad, tarjetas de crédito, información financiera personal, información académica de los estudiantes, información de salud, etc.) requieren procedimientos de destrucción segura, que resguarden la privacidad y protejan contra el robo de identidad. Entre estos procedimientos se recomienda la eliminación utilizando equipamiento de destrucción de documentos.

La eliminación segura de la información crítica, ya sea que resida en un medio digital o en papel, impide obtener información mediante trashing, que es la práctica de recuperar información técnica o confidencial a partir de material descartado, y suele ser la manera de obtener datos para posteriormente cometer otros delitos (robo, intrusión en los sistemas de información u otros incidentes).

6.1 Inventario de la información

No destruir de manera correcta los datos es un riesgo evidente para la seguridad y la privacidad, tanto o mas riesgo implica destruir dicha información por equivocación o negligencia. Para ello es fundamental llevar un inventario de la información que se gestiona que recoja, al menos:

- Clasificación.
- Responsable.
- Tiempo que se ha de conservar.
- Legislación que le aplica.

Consultar el Registro de actividades de tratamiento.

6.2 Eliminación segura de documentos en papel

La eliminación segura de documentos en papel consistirá en el uso de las trituradoras habilitadas a tal fin o la inserción de la documentación en los recipientes sellados para su recogida por la empresa contratada para la destrucción de documentos.

6.3 Gestión de soportes

Realizar un seguimiento de los dispositivos que están en uso, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.

Llevar a cabo el control, gestión y registro de los dispositivos que almacenan las copias de seguridad de estos datos (por ejemplo las cintas de los robots de backups).

Controlar cualquier operación realizada sobre un dispositivo: mantenimiento, reparación, sustitución, eliminación, etc...

En los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la empresa, asegurar que se cumple la cadena de custodia de los mismos, para evitar fugas de información.

6.4 Métodos de destrucción de la información

El método de borrado más adecuado para cada organización depende de factores tales como:

- Modelo de negocio.
- Volumen de datos que se gestionan.
- Tipo de datos que manejan.
- Recursos disponibles.

6.5 Eliminación segura de información en soportes ópticos.

Dispositivos capaces de guardar datos utilizando un rayo láser. La información queda grabada en la superficie de manera física por medio de ranuras microscópicas, es por esto que las ralladuras pueden ocasionar la pérdida de los datos.

La eliminación segura de información en soportes ópticos es solo posible destruyendo el soporte de almacenamiento. Los DVDs y CDs serán depositados en los recipientes sellados para su recogida por la empresa contratada para su destrucción.

6.6 Eliminación segura de información en soportes magnéticos.

Estos dispositivos se basan en la aplicación de campos magnéticos que causan una reacción de partículas, lo que a su vez hace que cambien de posición, la cual se mantiene una vez que se deja de aplicar el campo magnético.

La eliminación segura de información en este tipo de soportes se realiza aplicando un campo magnético que invalida los datos existentes. Los discos duros (internos o externos) y las cintas magnéticas podrán ser reutilizadas o eliminadas dependiendo del tipo de campo magnético aplicado.

6.7 Eliminación de configuraciones en hardware

Muchos equipos conservan información de configuración que puede aportar información valiosa. Particularmente los equipos de red como switches y routers pueden aportar información valiosísima para una persona malintencionada.

A la hora de retirar equipos de red y hardware en general se seguirán estos pasos previos a la retirada:

- Ejecutar las opciones y comandos especificados por el fabricante para el borrado explícito de la configuración (en el caso de que fuese posible).
- Ejecutar las opciones y comandos especificados por el fabricante para aplicar la configuración "Default" de tal forma que se sobrescriba cualquier información residual del paso anterior.

6.8 Registro de las operaciones de borrado realizadas

Al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado

En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente