


POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



Elaborado por: Consultor, EstudNET Fecha: 15/03/2021	Revisado por: Comité de Seguridad Fecha: 29/03/2021	Aprobado por: Director General  Firma: Aitor Deleyto Fecha: 29/03/2021
--	---	---

Historial de modificaciones

Fecha	Versión	Descripción de la modificación
29/03/2021	1.0	Creación del documento

USO PÚBLICO

El presente documento, propiedad de **ATM Grupo Maggioli SL**, está clasificado como de **USO PÚBLICO**. Su contenido podrá ser objeto de repro total o parcial, tratamiento informático o transmisión por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera ot

Índice

1.	DECLARACIÓN	3
2.	MISIÓN DE ATM GRUPO MAGGIOLI	4
3.	PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	4
4.	ALCANCE	5
5.	MARCO NORMATIVO	5
6.	ORGANIZACIÓN DE LA SEGURIDAD	6
6.1.	COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	6
6.2.	RESPONSABILIDADES	7
7.	DATOS DE CARÁCTER PERSONAL	10
8.	GESTIÓN DE LOS RIESGOS	10
9.	OBLIGACIONES DEL PERSONAL	11
10.	CONCIENCIACIÓN Y FORMACIÓN	11
11.	TERCERAS PARTES	11
12.	DESARROLLO Y ESTRUCTURA NORMATIVA	12
13.	AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN	12
14.	REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD	12

1. DECLARACIÓN

ATM GRUPO MAGGIOLI prioriza la seguridad y privacidad de la información, de conformidad con los requisitos del 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, como estrategia clave para la competitividad del negocio y el cumplimiento normativo.

ATM GRUPO MAGGIOLI dispone de un Sistema de Gestión de Seguridad de la Información, adoptando como marco la norma UNE ISO/IEC 27001:2014 “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información”, para la consecución de los objetivos siguientes:

- ✓ Gestionar los riesgos de la seguridad y privacidad de la información.
- ✓ Proteger los servicios y la información ante riesgos y amenazas.
- ✓ Concienciar y formar a empleados y colaboradores.
- ✓ Gestionar las incidencias de la seguridad de la información
- ✓ Cumplir con la legislación de protección de datos personales y cualquier otra de aplicación
- ✓ Garantizar la continuidad ante eventos que afecten a la disponibilidad de los servicios.
- ✓ Medir los indicadores de eficacia y eficiencia de la seguridad de la información
- ✓ Optimizar los procesos de gestión y los controles en modo mejora continua.
- ✓ ATM GRUPO MAGGIOLI ha establecido una organización de la seguridad y privacidad de la información, caracterizada por los rasgos siguientes:
 - ✓ Constitución del Comité de seguridad y privacidad de la información, como órgano con autoridad y competencias, presidido por la Dirección General.
 - ✓ Designación de las personas responsables del Servicio, de la Información, de la Seguridad de la información y del Sistema de información.
 - ✓ Designación de una persona que ejerce las funciones de Delegado de Protección de Datos
 - ✓ Asignación de recursos personales y materiales para satisfacer los requisitos de seguridad y privacidad de la información.
 - ✓ Colaboración con los socios tecnológicos y de negocio, así como proveedores con el fin de asegurar la seguridad a lo largo de la cadena logística.
 - ✓ Monitorización de los procesos de gestión de seguridad de la información, implantando las mejoras correctivas preventivas o de mejora, en función de los resultados y objetivos establecidos.

Aitor Deleyto, Director General

ATM GRUPO MAGGIOLI

2. MISIÓN DE ATM GRUPO MAGGIOLI

ATM GRUPO MAGGIOLI tiene como misión diseñar, desarrollar, mantener y soportar soluciones tecnológicas de última generación, a través de los servicios en la nube o “SaaS”, que den respuesta a las necesidades de las Entidades Públicas Locales, que simplifiquen la complejidad de la gestión local, faciliten el cumplimiento normativo y contribuyan a mejorar la relación con la ciudadanía.

3. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los sistemas de información y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de ATM GRUPO MAGGIOLI.

Principio de seguridad TIC en el ciclo de vida de los sistemas de información: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

4. ALCANCE

La presente política es de obligado cumplimiento a los sistemas de información en el ámbito objetivo del ENS, así como, a todo persona o colaborador de ATM GRUPO MAGGIOLI.

5. MARCO NORMATIVO

La Política de Seguridad de la Información da respuesta a los ordenamientos legales siguientes:

Administración pública

- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Ley 39/2015, de 1 de Octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Administración electrónica:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Protección de datos y seguridad de la 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 y por el que se deroga la Directiva 95/46/CE (RGPD)
- Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPDGDD)

Contratación pública:

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014

Propiedad Intelectual e Industrial

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizado, aclarando y armonizando las disposiciones legales vigentes sobre la materia
- Real Decreto de 3 de septiembre de 1880 por el que se aprueba el Reglamento para la ejecución de la Ley de 10 de enero de 1879 sobre propiedad intelectual.
- Ley 24/2015, de 24 de julio, de Patentes
- Real Decreto 316/2017, de 31 de marzo, por el que se aprueba el Reglamento para la ejecución de la Ley 24/2015, de 24 de julio, de Patentes.

6. ORGANIZACIÓN DE LA SEGURIDAD

La Política de Seguridad y Privacidad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar los responsables de su cumplimiento, así como ser conocida por todos los miembros y colaboradores de ATM GRUPO MAGGIOLI.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones, la componen:

- Comité de Seguridad y Privacidad de la información
- Responsable de la Información y del Servicio
- Responsable de Seguridad
- Responsable del Sistema
- Administrador de Seguridad
- Delegado de Protección de Datos

6.1. COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Comité de Seguridad y Privacidad de la Información, como órgano de gobierno la seguridad y privacidad de la información de ATM GRUPO MAGGIOLI, está integrado por los responsables siguientes:

- Presidente: Director General
- Responsable de la información y del Servicio
- Responsable y Administrador del Sistemas de información
- Responsable de Seguridad de la información, que actuará además como secretario del Comité
- Delegado de Protección de Datos

El Comité de Seguridad tendrá las siguientes funciones:

- a) Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- b) Elaborar la estrategia y posicionamiento en relación con la seguridad y privacidad de la información.
- c) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad y privacidad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- d) Elaborar y revisar regularmente la Política para su aprobación por el Director General.
- e) Aprobar la normativa de seguridad de la información.
- f) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- g) Supervisar y aceptar, en su caso, los riesgos residuales y recomendar posibles acciones de eliminación o mitigación.
- h) Supervisar el desempeño de la gestión de incidentes de seguridad y emprender posibles actuaciones de mejora.

- i) Promover las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
- j) Aprobar los planes de mejora de la seguridad y privacidad de la información.
- k) Asignar y priorizar los recursos en materia de seguridad.
- l) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos tecnológicos desde su concepción inicial hasta su puesta en producción.
- m) Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- n) Informar regularmente del estado de la seguridad de la información al Consejo de Administración.

El Responsable de Seguridad actuará como Secretario del Comité con las funciones:

- a) Convocar las reuniones del Comité de Seguridad de la Información.
- b) Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- c) Elaborar el acta de las reuniones.
- d) Ejecutar directa o de forma delegada de las decisiones del Comité.

El Delegado de Protección de Datos asesorará en aquellos aspectos que afecten a la seguridad de los datos personales y violaciones de seguridad de los datos personales.

El Comité se deberá reunir con carácter ordinario, al menos, una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

El Comité quedará constituido cuando asista la mitad más uno de sus miembros y para que sus acuerdos sean válidos, deberán ser adoptados por mayoría simple de votos de las personas presentes. En caso de empate el voto de calidad lo tiene el Presidente, o en quien haya delegado.

El Comité podrá recabar del personal técnico la información o asesoramiento pertinente para el ejercicio de sus funciones. En caso necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de asesores, con voz, pero sin voto.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la seguridad y privacidad, prevalecerá la decisión adoptada por el Comité.

6.2. RESPONSABILIDADES

Responsable del Servicio y de la Información

El Responsable de la Información y del Servicio, conforme con los artículos 10 y 44 del ENS, establece las necesidades de seguridad de la información, determina los requisitos de seguridad de los servicios prestados y efectúan las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

Tiene, además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS).

Son funciones del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

- a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 44 del ENS).
- b) Determinar la categoría de los sistemas de información, según lo descrito en el Anexo I del ENS.

Es, asimismo, responsable de aceptar los riesgos residuales calculados en el análisis de riesgos y de realizar su seguimiento y control.

Responsable de Seguridad

El Responsable de Seguridad, conforme al artículo 10 del ENS, es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Serán funciones del Responsable de Seguridad de ATM GRUPO MAGGIOLI las siguientes:

- a) Procurar que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.
- b) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- c) Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación al Esquema Nacional de Seguridad.
- d) Realizar los análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo, elevando un informe anual al Comité.
- e) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones para que adopten las medidas correctoras adecuadas.
- f) Coordinar el proceso de Gestión de la Seguridad.
- g) Firmar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema (artº. 27 y Anexo II.2 del ENS).
- h) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período.
- i) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- j) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

Responsable del Sistema

El Responsable del Sistema de información, conforme con el artículo 10 del ENS, es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Serán funciones del Responsable del Sistema de Información, las siguientes:

- a) Desarrollar, operar y mantener los sistemas de Información durante todo su ciclo de vida, así como aprobar y/o ejecutar los cambios que afecten a la seguridad del modo de operación del sistema.
- b) Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad.
- c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- d) Suspender el manejo de una determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.
- e) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- f) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- g) La gestión de las autorizaciones concedidas a los usuarios las personas usuarias del sistema.
- h) La aplicación de los procedimientos de seguridad.
- i) Ejecutar los cambios de configuración del sistema de información.
- j) Asegurar el cumplimiento de los controles de seguridad y privacidad establecidos.
- k) Supervisar la instalación de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- l) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- m) Informar al Responsable de Seguridad de la información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

Administrador de Seguridad

El Administrador de Seguridad, dependiendo del Responsable del Sistema, es quien se encarga de implementar la seguridad de acuerdo con las directrices del Responsable de Seguridad de las TIC

Serán funciones del Administrador de Seguridad, las siguientes:

- a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- b) La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- c) La gestión de las autorizaciones concedidas a los usuarios las personas usuarias del sistema.
- d) La aplicación de los procedimientos de seguridad.

- e) Aprobar los cambios de configuración del sistema de información.
- f) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- h) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- i) Informar a los Responsables de Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- j) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7. DATOS DE CARÁCTER PERSONAL

ATM GRUPO MAGGIOLI dispone de un proceso de análisis de riesgos para la gestión de los riesgos de los tratamientos de datos de carácter personal.

Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal.

En caso de conflicto con la normativa de seguridad indicada en el artículo 15 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

8. GESTIÓN DE LOS RIESGOS

La gestión de riesgos deberá realizarse de conformidad con los principios de gestión de la seguridad basada en los riesgos (artículo 6 del ENS) y reevaluación periódica (artículo 9 del ENS).

El proceso de gestión de riesgos comprende la identificación y categorización de los sistemas y subsistemas de información, el análisis de amenazas, el cálculo de los riesgos y la selección de medidas de seguridad, que deberán ser proporcionales y justificadas.

El Responsable de Seguridad de ATM GRUPO MAGGIOLI es el responsable de realizar los análisis de riesgos y seleccionar las medidas de seguridad o salvaguardas a implantar, elevando un informe al Comité de Seguridad y Privacidad de la Información para su aprobación.

El análisis de los riesgos y su tratamiento, según lo establecido en el Artículo 9 del ENS, se desarrollarán según lo siguiente:

- Al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada y/o en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad y/o cuando se reporten vulnerabilidades graves.

El análisis de riesgos deberá contemplar los requisitos establecidos por el Artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 para decidir y establecer las medidas técnicas y organizativas que corresponda implantar y así atender los riesgos generados por el tratamiento.

9. OBLIGACIONES DEL PERSONAL

Todo el personal de ATM GRUPO MAGGIOLI tiene obligación de conocer y cumplir con lo dispuesto en la Política de Seguridad y Privacidad de la información y la normativa de seguridad complementaria a partir de ella, siendo responsabilidad del Comité de Seguridad dispone los medios necesarios para que la información llegue a los afectados.

10. CONCIENCIACIÓN Y FORMACIÓN

Todos los empleados de ATM GRUPO MAGGIOLI atenderán a una acción de concienciación en materia de seguridad de la información y protección de datos, al menos, una vez al año. Se establecerá un programa de formación y de concienciación, en particular a las nuevas incorporaciones.

Las personas con responsabilidades en el ámbito de la presente Política serán objeto de acciones especializadas de cualificación, teniendo en consideración la necesaria actualización de conocimientos.

11. TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de la presente Política, 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, asimismo, se les solicitará la aceptación de la presente Política, quedando sujeta a las obligaciones establecidas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y privacidad, 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, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos, sometiéndose a la aprobación de los responsables de la información y los servicios y del sistema de información.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por ATM GRUPO MAGGIOLI y formalizar su relación como encargados de tratamientos.

12. DESARROLLO Y ESTRUCTURA NORMATIVA

La documentación de seguridad que desarrolla la presente Política es la siguiente:

2º Nivel:

Normativa que establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. Es de carácter obligatorio.

Procedimientos que determinan las acciones a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución.

3º Nivel:

Instrucciones Técnicas de Seguridad que describen las tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.).

Guías o buenas prácticas con carácter formativo o de ayuda a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos.

13. AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad y privacidad de la Información y los sistemas de información de ATM GRUPO MAGGIOLI, serán objeto, al menos, anualmente, de una auditoría regular ordinaria, interna o externa, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, asimismo, deberá auditarse siempre que se produzcan cambios o situaciones que puedan repercutir en el cumplimiento de las medidas de seguridad establecidas.

Los informes de auditoría se elevarán, para su aprobación, al Comité de Seguridad y Privacidad, decidiéndose las acciones a emprender, ya sean preventivas o correctivas.

14. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política será revisada por el Comité de Seguridad de la Información y la Privacidad, al menos, con periodicidad anual o, bien, siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por Comité de Seguridad de la Información y la Privacidad, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.