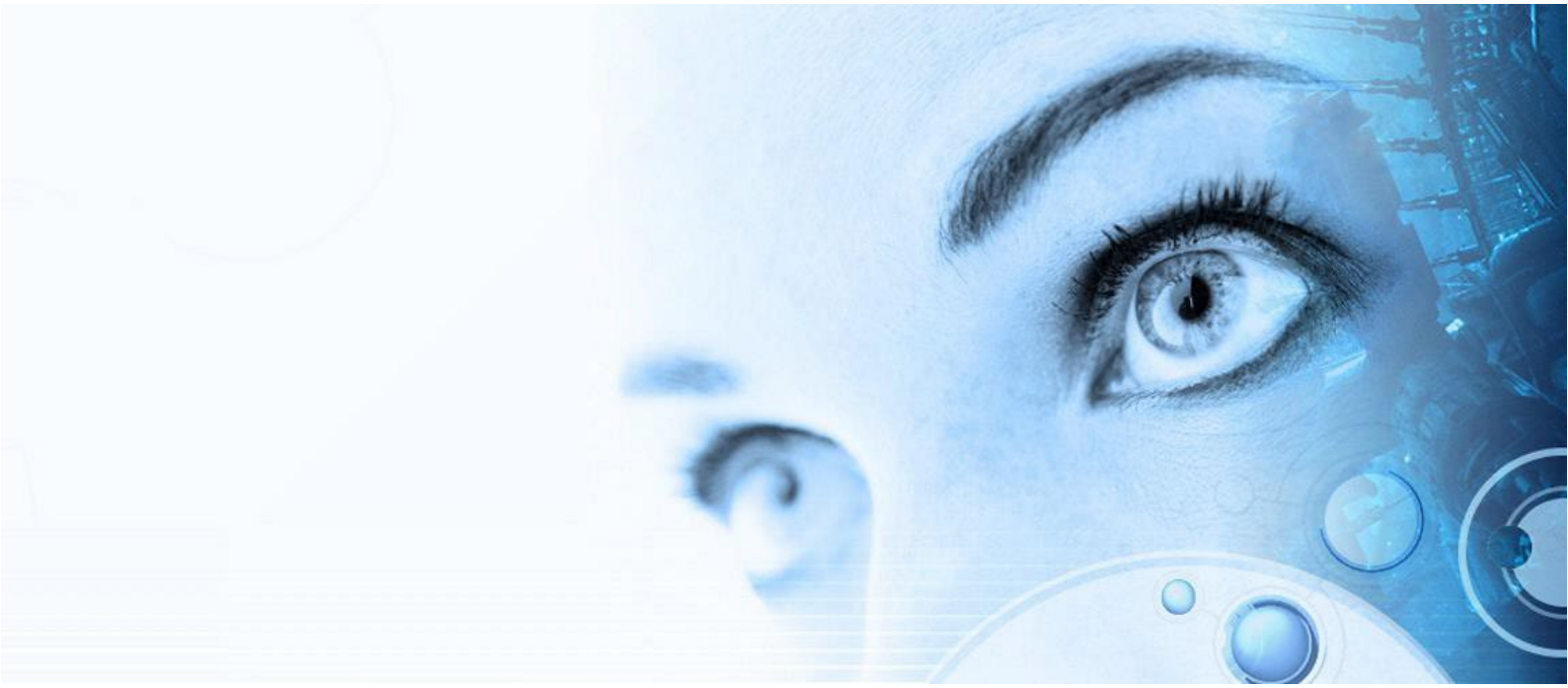
Salzillo servicios



SI_POL_001 POLITICA DE SEGURIDAD

Fecha: 07/08/2023

CONTROL DE FIRMAS

	FECHA
ELABORADO POR Responsable de Seguridad	07/08/2023

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	07/08/23	Responsable de Seguridad	Versión inicial del documento

APROBACIÓN Y ENTRADA EN VIGOR

El presente Documento ha sido aprobado por el Comité de Seguridad de SALZILLO SERVICIOS INTEGRALES, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que SALZILLO SERVICIOS INTEGRALES pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de SALZILLO SERVICIOS INTEGRALES.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de este documento.

ÍNDICE

1. Introducción

La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo, determina la política de seguridad que debe aplicarse en la utilización de los medios electrónicos.

El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por la organización para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestiones en el ejercicio de sus competencias.

El Esquema Nacional de Seguridad (ENS), y SALZILLO SERVICIOS INTEGRALES (en adelante, la organización), persigue los siguientes objetivos:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 39/2015, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que deben guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan varias entidades.
- Facilitar un tratamiento continuado de la seguridad.

En el Esquema Nacional de Seguridad se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas, pero deficientemente ensambladas.

El aspecto principal del ENS es, sin duda, que todas las organizaciones deberán disponer de

su política de seguridad que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos.

La adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones:

- Preparar y aprobar la política de seguridad, incluyendo la definición de roles y la asignación de responsabilidades.
- Categorizar los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el análisis de riesgos, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar y aprobar la Declaración de aplicabilidad de las medidas del anexo II del ENS.
- Elaborar un plan de adecuación para la mejora de la seguridad, en base a las insuficiencias detectadas, incluyendo plazos estimados de ejecución.
- Implantar operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente.
- Auditar la seguridad.
- Informar sobre el estado de la seguridad

2. Objeto y Ámbito de aplicación

Constituye el objeto de este documento fijar la Política de Seguridad de la Información (en adelante, PSI) de la organización, así como el establecimiento del marco organizativo y tecnológico de la misma.

La PSI será de obligado cumplimiento para todas las personas responsables de la organización; como también será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la misma información que sea gestionada por cada área, con independencia de cuál sea su destino, adscripción o relación con el área.

Con la aprobación de la PSI, la organización establece un marco de gestión de la seguridad de la información adecuado al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como activos estratégicos la información y los sistemas que la soportan.

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el de establecer las bases sobre las que el conjunto de empleados y los clientes puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

La PSI protege la información de un amplio abanico de amenazas, con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización

La gestión de la seguridad de la información debe garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos.

Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

Contribuir desde la gestión de la seguridad de la información al cumplimiento de la misión y objetivos establecidos por de la organización

Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo que se refiere a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.

Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento, ante amenazas, internas o externas, deliberadas o accidentales, con la finalidad de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y fiabilidad de la información.

3. Alcance

Esta política será de aplicación y de obligado cumplimiento para todas las áreas y servicios de la organización y los entes instrumentales que dependan de ella y también afectará a todos sus recursos y a los procesos incluidos en el Real Decreto 311/2022, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

En concreto, esta Política se aplicará a todos los medios técnicos y humanos de SALZILLO SERVICIOS INTEGRALES relacionado con los Sistemas de Información que soportan la Gestión de las actividades relacionadas con los siguientes servicios:

- Servicios y asistencia técnica de auxiliares generales de atención al público o atención telefónica, gestión administrativa, ordenanzas, gestión de reclamaciones, control y gestión documental y controladores de acceso, entre otros.
- Servicios para el funcionamiento y mantenimiento de representaciones y actividades

en centros culturales, deportivas, auditorios, espacios escénicos y otros habilitados para esos fines.

- Gestión de la formación de actividades de ocio, deportivas y tiempo libre en centros públicos y privados.
- Servicio de ayuda a domicilio.
- Guía de museos
- Atención al público y atención y coordinación telefónica de emergencias.

4. Revisión de la política

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con la finalidad de asegurar que ésta se adecua a la estrategia y necesidades de la organización.

La PSI será propuesta, revisada y difundida por el Comité de Seguridad; mediante el Responsable del Sistema, que velará activamente por su conservación, actualización y difusión hacia todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta política, el Comité de Seguridad será el órgano competente para su resolución.

5. Alcance del SGSI

Con objeto de establecer el alcance del Sistema de Gestión de la Seguridad de la Información a la que afecta la presente Política y todo el cuerpo normativo de Seguridad de la Información que recae bajo el paraguas de la misma, se establecen los siguientes alcances:

ENS 311/2022

Los Sistemas de Información que soportan la Gestión de las actividades relacionadas con los siguientes servicios:

- Servicios y asistencia técnica de auxiliares generales de atención al público o atención telefónica, gestión administrativa, ordenanzas, gestión de reclamaciones, control y gestión documental y controladores de acceso, entre otros.
- Servicios para el funcionamiento y mantenimiento de representaciones y actividades

en centros culturales, deportivas, auditorios, espacios escénicos y otros habilitados para esos fines.

- Gestión de la formación de actividades de ocio, deportivas y tiempo libre en centros públicos y privados.
- Servicio de ayuda a domicilio.
- Guía de museos
- Atención al público y atención y coordinación telefónica de emergencias.

6. Marco normativo

Se tomó como referencia básica en materia de Seguridad de la Información el Código de Derecho de la Ciberseguridad publicado en el BOE[1] compuesta, entre otra, por la siguiente normativa:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (Reglamento General de Protección de Datos).
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto refundido de la Ley de Propiedad Intelectual.

[1] https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Decreto 8/2021, de 9 de febrero, sobre la transparencia y el derecho de acceso a la información pública
- Política de firma electrónica de la organización.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la organización, derivadas de las anteriores y comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad de la organización, el cual dispone de un procedimiento de identificación de la legislación aplicable, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el Artículo 29. "Instrucciones técnicas de seguridad y guías de seguridad".

Asimismo, la organización, también será responsable de identificar las guías de seguridad del CCN, referenciadas en el citado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

7. Principios y Directrices

La organización, para conseguir el cumplimiento de las previsiones recogidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en la organización estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de manera que garanticen la seguridad por defecto, de la manera siguiente:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles para las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultades.
c) 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.
d) El uso ordinario del sistema debe ser sencillo y seguro, de manera que una utilización insegura requiera de un acto consciente por parte del usuario.

Revaluación periódica (artículo 10) e integridad y actualización del sistema (Artículo 21)

La organización, ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la 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. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Asimismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 15) y profesionalidad (artículo 16)

Todos los miembros de la organización, dentro del ámbito de la ENS, atenderán una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria 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.

Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando pase un incidente grave de seguridad o se detecten vulnerabilidades graves.

El responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 25), prevención, reacción y recuperación (artículo 8)

La organización, ha implementado un proceso integral de detección, reacción y recuperación frente a código dañinos mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la organización, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

La organización, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).
- Para garantizar la disponibilidad de los servicios, la organización, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 9) y prevención frente a otros sistemas interconectados (artículo 23)

La organización, ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal manera que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada ante los incidentes que no se han podido evitar.

- Reducir la probabilidad de que el sistema esté comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección debe proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)

La organización, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 17)

La organización, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 18)

La organización, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19)

Para la adquisición de productos, la organización, tendrá en cuenta que estos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tráfico (artículo 22) y continuidad de la actividad (artículo 26)

La organización, ha implementado mecanismos para proteger la información almacenada o en tráfico, especialmente cuando ésta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias de la organización. Del mismo modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 24)

La organización ha habilitado registros de la actividad 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. Todo ello con la finalidad exclusiva de alcanzar el cumplimiento del objeto del presente Real Decreto, 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, de función pública o laboral, y demás disposiciones que resulten de aplicación.

8. Estructura documental

La Organización ha desarrollado una Política de gestión y conservación de documentos electrónicos que ha sido implementada mediante normas internas, procedimientos e instrucciones técnicas.

Asimismo, señalar que se dispone de un gestor documental, regido por una norma interna de gestión de la documentación en cuanto a elaboración, aprobación, conservación, estructura, acceso, etc., de los documentos del sistema de gestión de la seguridad aplicado sobre los sistemas de información.

9. Estructura organizativa

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todas y cada una de las personas usuarias de los sistemas de información de la organización son responsables de la seguridad de los activos de información, por lo que deben hacer siempre un uso correcto de los mismos, de acuerdo con sus atribuciones profesionales y académicas.

Para una mejor respuesta a incidentes de seguridad, la organización mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios de informáticos o de comunicación, así como a organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, de acuerdo con lo señalado a continuación.

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito en esta PSI de la organización está compuesta por los órganos y agentes siguientes:

9.1. Composición y funciones del Comité de Seguridad de la Información

El Comité de Seguridad de la Información está compuesto por

El/la responsable de la Información: Isabel Alarcón Martinez

El/la responsable del servicio: Isabel Alarcón Martinez

El/la responsable de seguridad: Miguel Angel Sabater

El/la responsable del sistema: Angel Pardo Moreno

El/la responsable de administración de la seguridad del sistema: Técnico Informático

Con carácter opcional, otros miembros de la organización, podrán incorporarse a las tareas del Comité, incluidos grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información llevará a cabo sus sesiones, con periodicidad

trimestral, previa convocatoria al efecto realizada por la Presidencia de dicho Comité.

En materia de seguridad de la información, el CSI de la organización tiene las funciones siguientes:

- Aprobar la Política de Seguridad de la Información de la organización y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento de los Esquemas Nacionales de Seguridad.
- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por parte de la Alcaldía u órgano en quien delegue.
- Proponer al órgano competente la aprobación de las Directrices de seguridad de la información , en base a la propuesta formulada por el Responsable del Seguridad o del Sistema.
- Aprobar las normativas propuestas por el Responsable de Seguridad que garanticen una implantación efectiva de la Política de Seguridad y de las Directrices.
- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar por que la Seguridad de la Información se tenga en cuenta en todos los proyectos 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.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Proponer programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

- Promover la realización de las auditorías periódicas sobre el ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Organización en materia de seguridad de la Información.

9.2. Responsable de Seguridad

De acuerdo con el artículo 10 del ENS, el/la Responsable de Seguridad es la persona o conjunto de personas que determinan las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

El ámbito de actuación del responsable de seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa de la organización.

En el caso de aplicaciones y portales que otras organizaciones ponen al alcance de los trabajadores/as de nuestra organización, el comité de seguridad velará por garantizar una correcta comunicación con los sistemas remotos, pero nunca de la seguridad de las aplicaciones en sí mismas.

Serán funciones del Responsable de Seguridad, dentro del ámbito de actuación enunciado en el punto anterior, las siguientes:

- Aprobar los procedimientos de seguridad.
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación del sistema.
- Elevar al Comité de Seguridad la propuesta de modificación de la Política de Seguridad, así como la aprobación de cambios y otros requisitos del sistema.

9.3. Responsable del Sistema

El responsable del sistema tiene el encargo de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

Serán funciones del responsable del sistema, dentro del ámbito de actuación enunciado en el punto anterior, las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Elaborar los procedimientos de seguridad.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Velar por que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad de la Información y/o al Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Supervisar las funciones del administrador de la seguridad del sistema:
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con el autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- 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.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar a los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. Del mismo modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

9.4. El Administrador de la seguridad del sistema

El Administrador de la seguridad del sistema es un Técnico Informático, miembro del Servicio de Sistemas de Información y designado por el Responsable del Sistema.

Sus responsabilidades serán las siguientes:

- La elaboración, cuando así lo determine el Responsable del Sistema, aplicación y gestión de los procedimientos operativos de seguridad.
- La gestión, configuración y actualización, si procede, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema.
- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema.
- Informar a los responsables de Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados por manejo del sistema.
- Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo frecuentemente, de acuerdo con la Política de Seguridad establecida por la Organización.
- Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas.
- Iniciar el proceso de respuesta ante incidentes que se produzcan en el Sistema bajo su responsabilidad, informando y colaborando con el responsable de seguridad en la investigación de los mismos.

9.5. Responsable de la Información

El/la Responsable de la Información es la persona que determina los niveles de seguridad de la información, y tiene la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de la información. Si esta información incluye datos de carácter personal, además deben tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

El Responsable de la Información dispondrá del apoyo de cada uno de los jefes de área responsables de los ámbitos correspondientes a cada activo de información incluido en el alcance de esta Política.

La identificación del responsable de cada información se recoge en el Anexo I Categorización de los Sistemas, que complementa esta Política y que forma parte del SGSI.

Los/as responsables de las áreas de la organización tienen la obligación de solicitar al/la Responsable de la Información que indique el nivel de seguridad de la información que tratarán en cada caso, con el fin de garantizar una correcta definición de los niveles de seguridad de la información.

Aunque la aprobación formal de los niveles corresponde al responsable de la información, éste podrá solicitar una propuesta al Responsable del Sistema antes de establecer la definición del nivel de seguridad.

9.6. Responsable del Servicio

El/la Responsable del Servicio es la persona que determina los niveles de seguridad de cada servicio, y tiene la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad de los servicios. Si esta información incluye datos de carácter personal, además deben tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

Aunque la aprobación formal de los niveles corresponde al Responsable del Servicio, éste podrá solicitar una propuesta al Responsable del Sistema antes de establecer la definición del nivel de seguridad.

El ámbito de actuación del Responsable del Servicio son los sistemas de información y servicios que abarcan esta Política.

9.7. Delegado de Protección de Datos

De acuerdo con lo previsto en el artículo 39 del RGPD, las funciones del Delegado de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los estados miembros y de las políticas de responsable o del encargado del tratamiento en materia de protección de datos

personales, incluida la asignación de responsabilidades, la concienciación y formación de personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

- Ofrecer el asesoramiento que se le pida sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control por cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Ejercerá 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.

9.8. Procedimiento de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política se lleva a cabo por aceptación de las partes afectadas.

Los miembros del Comité, así como los roles de seguridad, serán revisados cada cinco años o con ocasión de vacante de la persona ocupante del puesto de trabajo que tiene asignadas cada una de las funciones de responsabilidad previstas.

9.9. Resolución de conflictos

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

10. Datos de carácter personal

Tan solo se recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstas se encuentren en relación con el ámbito y las finalidades para las que se hayan obtenido. Del mismo modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del 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 cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española. con la Ley Orgánica 3/2018,

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas: el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien ejerza las funciones de Delegado de Protección de Datos.

Todos los sistemas de información de la organización se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de protección de datos de carácter personal, identificado en el apartado 5. Marco Normativo, de esta Política de Seguridad de la Información.

11. Gestión de riesgos

Todos los sistemas sujetos a esta PSI deben someterse a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.

Aunque se necesita un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando se reporten vulnerabilidades graves
- Cuando tenga lugar un incidente grave de seguridad.
- Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información que se dispone y delos diferentes servicios prestados.

El Comité de Seguridad de la Información velará por la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos.

12. Documentación de seguridad del sistema

La documentación que debe prepararse y debe estar disponible para las personas que tienen responsabilidades sobre la operación del sistema y responsabilidades de auditoría sobre el mismo es la siguiente:

- La Política de Seguridad, que será objeto de un documento específico.
- El Análisis de riesgos, que será elaborado por el Responsable del Sistema, que podrá encargar o delegar la función, aprobando el resultado final. El Responsable de Seguridad debe validar el documento, y puede solicitar mejoras en el mismo. El documento estará a disposición de los auditores.
- La Declaración de Aplicabilidad, que será elaborada por el Responsable del Sistema, que podrá encargar o delegar la función, aprobando el resultado final. El Responsable de Seguridad debe validar el documento, y puede solicitar la inclusión de medidas adicionales. El documento estará a disposición de los auditores.
- La arquitectura de seguridad, que será elaborada por el Responsable del Sistema, que podrá encargar o delegar la función, aprobando el resultado final. El Responsable de Seguridad debe validar el documento, y puede solicitar mejoras en el mismo. El documento estará a disposición de los auditores.
- La normativa y los procedimientos de seguridad se irán elaborando bajo la denominación de Procedimientos de Seguridad. Éstos serán elaborados por el Responsable del Sistema o en quien éste delegue. Serán aprobados y validados por el Responsable de Seguridad. Esta documentación estará a disposición de los auditores y se comunicará a las personas afectadas, que deberán explicitar su conocimiento y compromiso de cumplimiento de lo establecido.

13.Desarrollo de la Política de Seguridad de la Información

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponente, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del Comité de Seguridad de la organización.

Esta Política de Seguridad de la Información se desarrolla por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad está a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Las normas y procedimientos contemplarán, al menos, los siguientes aspectos:

- Protección de datos de carácter personal: se implantarán medidas técnicas y organizativas que permitan cumplir los requisitos normativos en esta materia.
- Gestión de activos de información: los activos de información se encontrarán inventariados, categorizados y estarán asociados a un responsable.
- Seguridad ligada a los recursos humanos: la seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios, para lo que se implantarán los mecanismos que permitan a los usuarios conocer sus responsabilidades y cómo cumplir con ellas.
- Seguridad física: las instalaciones de la organización mantendrán una correcta seguridad física para evitar los accesos no autorizados, así como cualquier otro tipo de daño o interferencia externa.
- Seguridad lógica: se establecen medidas organizativas y técnicas para el control de accesos, la protección frente a códigos nocivos, la seguridad de las comunicaciones, la realización de copias de seguridad …
- Gestión de incidentes de seguridad: se deben establecer responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los acontecimientos en materia de seguridad

En todo caso, las directrices para la estructuración de la documentación se encuentran desarrolladas en “NOR_003 Normativa de Gestión de la Documentación”.

14. Formación y concienciación

Todos los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la organización asistirán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizarla. La formación será obligatoria 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.

15. Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información puede conllevar el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

16. Confidencialidad

Todo el personal de la organización, dentro del alcance de esta Política, asumen el compromiso de no difundir información a la que se ha tenido acceso a través del desempeño de sus funciones, derivado de la ejecución de un proyecto o de una relación de servicios, laboral o profesional con el mismo.

Se entiende por difusión, cualquier forma de transmisión de información: verbal, escrita, o por cualquier otro medio físico o telemático, a cualesquiera personas, empresas, instituciones u organizaciones. También se considerará difusión, permitir o facilitar el acceso de forma dolosa o imprudente a la información a la que se hubiera tenido acceso en virtud de una relación de carácter empresarial, laboral o profesional.

El deber de confidencialidad corresponde a cualquier tipo de información, en cualquier formato, contenida en cualquier documento o soporte, que contenga información. También es de aplicación a aquella información que la organización pueda mantener sobre entidades colaboradoras y terceros en general.

Este Deber de Confidencialidad tiene una duración indefinida, exigible tanto durante la vigencia de la relación profesional, laboral o formativa con la organización, como después de su conclusión.

17. Terceras partes

Las empresas y organizaciones externas que con ocasión de su colaboración con la organización para la prestación de un servicio, accedan o gestionen activos de información de la organización o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos de la organización, de manera que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados a la Organización sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad de la organización que traten por razón de la prestación de servicio.

- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados a la Organización. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo de la organización a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la misma entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso en los sistemas de la organización. Específicamente, cualquier equipo conectado a la red corporativa de la organización debe disponer de un antivirus actualizado preferiblemente de forma automática.
- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas de la organización desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no fiables.

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 del servicio afectados antes de seguir adelante.

En todo caso, la organización se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

18. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información ha sido aprobada por acuerdo del Comité de Seguridad en fecha 07 de agosto de 2023 y es efectiva desde esa fecha y hasta que sea sustituida por una nueva versión.