ENS – ORG 1
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Propuesto por	EY	Fecha:29/01/2024
Revisado por:	Rodrigo Figueroa	Fecha:07/03/2024
Aprobado por:	Rodrigo Figueroa	Fecha:07/03/2024
Alcance:	Política de seguridad de la información de ALEATICA	
Clasificación del documento	Uso interno	

Control de cambios

Revisión	Sección	Descripción breve del cambio
01	4	Añadidas "Otras materias"
	7.3.3, 7.3.5, 7.3.6, 7.3.7	Añadidas funciones adicionales del rol ENS
	14	Añadido "Obligaciones del personal"

Documentación relacionada y aplicable

Código	Nombre del documento
ENS - 01	Alcance del ENS

ÍNDICE

1. INTRODUCCIÓN

1.1. Introducción

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El artículo 12 del citado Real Decreto exige que se contará con una política de seguridad formalmente aprobada por el órgano competente. El mismo Real Decreto enuncia los principios básicos en materia de seguridad de la información recogidos en el capítulo II de la propia ley (seguridad como proceso integral, gestión de la seguridad basada en riesgos, prevención, detección, respuesta y conservación, líneas de defensa, vigilancia continua, reevaluación periódica y diferenciación de responsabilidades) y establece el marco regulatorio de la Política de Seguridad de la Información (en adelante, PSI), que se plasmará en un documento, accesible y comprensible para todos los miembros de la organización, que definirá lo que significa seguridad de la información en una organización determinada y que regirá la forma en que una organización gestiona y protege la información y los servicios que considera críticos, disponiendo que:

a) Cada Organización que aplique el ENS contará con una política de seguridad formalmente aprobada por el órgano competente.
b) La seguridad deberá comprometer a todos los miembros de la organización. La PSI deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.
c) El contenido mínimo de la PSI debe precisar de forma clara los objetivos o misión de la organización, el marco legal y regulatorio en que desarrolla sus actividades, los roles o funciones de seguridad, definiendo para cada uno sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, la estructura del comité para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, sus miembros y su relación con otros elementos de la organización, y las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
d) Además, la PSI debe ser coherente con lo establecido en el 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 en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La PSI proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran para garantizar la seguridad de la información, cumpliendo el marco legal de aplicación y las directivas, políticas específicas y procedimientos definidos.

Estas actuaciones son seleccionadas e implantadas en base a un análisis de riesgos realizado y el equilibrio entre riesgo aceptable y coste de las medidas.

El Responsable de Seguridad debe definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, de modo que los procesos más importantes y/o sensibles recibirán mayor protección.
Es responsabilidad del Comité de Seguridad de la Información (en adelante CSI), promover y apoyar la implantación de las medidas técnicas y organizativas necesarias para minimizar los riesgos potenciales a los que se encuentra expuesta la información en la consecución de los objetivos estratégicos del negocio.
El objeto de esta Política es alcanzar una protección adecuada de la información de la Organización, preservando los siguientes principios de la seguridad:

- **Confidencialidad:** garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.
- **Integridad:** garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** garantizar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- **Autenticidad:** garantizar que una entidad es quien dice ser o que se garantiza la fuente de los datos.
- **Trazabilidad:** garantizar que las actuaciones de una entidad (persona o proceso) puede ser trazado de forma indiscutible.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de la Organización o fuera de ellas.

1.2. Prevención

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, Aleatica, 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, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.
Para garantizar el cumplimiento de la política, Aleatica:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo el análisis de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente.

1.3. Detección

Aleatica, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

1.4. Respuesta

Aleatica establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con 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).

1.5. Recuperación

Para garantizar la disponibilidad de los servicios, Aleatica, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

2. OBJETIVO

El objeto de la PSI es garantizar la seguridad homogénea e integral que tiene por finalidad proteger los activos (conjunto de instalaciones y/o sistemas de su propiedad o gestión), así como establecer el marco organizativo de la misma.

3. ALCANCE

La presente Política es aplicable a todos los activos de información incluyendo instalaciones, sistemas, servicios, software, bases de datos y toda la información almacenada o procesada en los sistemas informáticos.
Asimismo, deberán cumplir con la Política de Seguridad todas las personas que tengan acceso a la información objeto de alcance del Sistema de Gestión de Seguridad de la Información, y/o presten servicios para la Organización, incluso en el supuesto de que su relación no tenga carácter laboral.
Se aplicarán los principios básicos y los requisitos mínimos que se establecen en el ENS de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, que permita una protección adecuada de la información y los servicios.

4. MARCO NORMATIVO

Dentro del marco legal relativo a la seguridad de la información merecen especial mención las siguientes normas, regulaciones y estándares que serán objeto de verificación de su cumplimiento de forma periódica:

- En materia de sistemas de información:
  - ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  - ✓ Guías CCN-STIC del CCN-CERT.
- En materia de protección de datos de carácter personal:
  - ✓ 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 - RGPD).
  - ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
  - ✓ Guías de la AEPD.
- Otras materias:
  - ✓ Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
  - ✓ Real Decreto Legislativo 1/1996 (Ley de Propiedad Intelectual).
  - ✓ Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
  - ✓ Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

5. PRINCIPIOS Y REQUISITOS MÍNIMOS DE LA SEGURIDAD DE LA INFORMACIÓN

5.1. Principios básicos

5.1.1. Alcance estratégico

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de Aleatica para conformar un todo coherente y eficaz.

5.1.2. Diferenciación de responsabilidades

En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad del ciclo de vida del sistema; el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad; y el administrador de seguridad que será el encargado de la implementación y mantenimiento de las medidas de seguridad sobre los elementos o activos tecnológicos y operativos de su ámbito de competencia.

5.1.3. La seguridad como un proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

Aleatica presta la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia o la ausencia de conocimiento, la falta de organización y de

coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

5.1.4. Gestión de la seguridad basada en los riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá realizarse de manera continua y permanentemente actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos para reducirlos a niveles aceptables. La reducción de los riesgos a estos niveles aceptables se realizará mediante una apropiada aplicación de medidas de seguridad de manera equilibrada y proporcionada a la naturaleza de la información tratada de los servicios a prestar y de los riesgos a los que estén expuestos.

Los responsables de la información y del servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente y, por tanto, los responsables de asumir los riesgos asociados al tratamiento de la información y prestación de los servicios.

Aleatica realiza su propia gestión de riesgos por medio de una metodología propia, basada en estándares reconocidos internacionalmente, de análisis y tratamiento de los riesgos a los que están expuestos los sistemas.

5.1.5. Prevención, detección, respuesta y conservación

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciber incidente.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

5.1.6. Existencia de líneas de defensa

Los sistemas han de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas sea comprometida, permita:

- Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

5.1.7. Proporcionalidad

El establecimiento de medidas de protección, prevención, detección, respuesta y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

5.1.8. Vigilancia continua y reevaluación periódica

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.
La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

5.1.9. Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

5.1.10. Protección de datos de carácter personal

Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal, con especial mención al artículo 32 del Reglamento (UE) 679/2016 General de Protección de Datos (RGPD), por el que se establece que el Responsable y el Encargado del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluirán, entre otros, la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento y la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

5.2. Requisitos mínimos de seguridad de la información

5.2.1. Profesionalidad

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado de Aleatica, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

5.2.2. Adquisición de productos

Se tendrá en cuenta en la adquisición de productos la categoría del sistema y nivel de seguridad determinado. Se aceptarán aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

5.2.3. Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento de los objetivos de la seguridad de la información, 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, 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.

5.2.4. Seguridad de la información en la gestión de proyectos

Se integrará la seguridad de la información en los procesos de gestión de proyectos para asegurar que los riesgos se identifican y se contemplan de forma que los objetivos de seguridad estén incluidos dentro de los objetivos del proyecto, se realice una evaluación de riesgos en una fase temprana, y la seguridad de la información forme parte de todas las fases de la metodología aplicada en el propio desarrollo del proyecto.

6. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Aleatica, establece como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestión de activos de información: Los activos de información de la cada una de las concesionarias se encontrarán inventariados y categorizados y estarán asociados a un responsable.
- Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación de los usuarios respecto a la seguridad de la información.
- Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

- Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
- Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
- Garantizar la prestación continuada de los servicios: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.
- Protección de datos: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento para cumplir la legislación de seguridad y privacidad.
- Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. Criterios utilizados para la organización de la seguridad de la información

Aleatica teniendo en cuenta lo establecido en el antedicho Real Decreto 311/2022, por el que se regula el ENS y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS", para organizar la seguridad de la información emprenderá las siguientes acciones:

a) Designará roles de seguridad: Responsables de los Servicios, Responsables de la Información, Responsable de la Seguridad, Responsable del Sistema y Delegado de Protección de Datos.
b) Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2. Roles y Órganos de la seguridad de la información

Aleatica, en el marco del ENS, determina que los roles y órganos de la Seguridad de la Información que se establecerán serán los siguientes:

- Responsables de los Servicios y Responsables de la Información.
- Responsable de Seguridad de la Información.
- Responsable del Sistema.
- Comité de Seguridad TIC (CSI):
  - Presidencia.
  - Vocales.
  - Secretario/a del CSI.

7.3. Responsabilidades de los roles asociados al ENS

7.3.1. Responsable de la información y de los Servicios

Serán funciones de los Responsables de la Información y de los Servicios:

Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.

Dictaminar respecto a los derechos de acceso a la información y los servicios.

Aceptar los niveles de riesgo residual que afectan a la información y los servicios.

Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios e información que se efectuarán, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

7.3.2. Responsable de Seguridad

Serán funciones del Responsable 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 TIC.
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.
Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

7.3.3. Responsable del sistema

Serán funciones del Responsable del Sistema:
Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad 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.
Llevar a cabo, en su caso, 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 lo 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.

Informar al Responsable de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar 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. De igual modo, también podrá delegar en otra/s funciones concretas de las responsabilidades que se le atribuyen.

7.3.4. Delegado de Protección de Datos

Serán funciones del Delegado de Protección de Datos:
Informar y asesorar a Aleatica y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de Aleatica en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisará su aplicación.
Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
El Delegado de Protección de Datos desempeñará sus funciones prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
Recabar información para determinar las actividades de tratamiento.
Analizar y comprobar la conformidad de las actividades de tratamiento.
Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
Recabar información para supervisar el registro de las operaciones de tratamiento.
Asesorar en el principio de la protección de datos por diseño y por defecto.
Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
Priorizar actividades en base a los riesgos.
Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

7.3.5. Comité de Seguridad TIC

Serán funciones del Comité de Seguridad TIC:
Atender las inquietudes de la Dirección de la unidad de negocio y de las diferentes áreas.

Informar regularmente del estado de la seguridad de la información a la Dirección de la unidad de negocio.
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.

Estar permanentemente informado de la normativa que regula la Certificación de Conformidad con el ENS, incluyendo sus normas de acreditación, certificación, guías, manuales, procedimientos e instrucciones técnicas.
Proponer directrices y recomendaciones, que serán recogidas en las correspondientes actas de las reuniones del Comité, a las que su presidente, deberá dar cumplida respuesta.
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.
Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información
Revisar la Política de Seguridad de la Información previa aprobación.
Aprobar la Normativa de Uso de Medios electrónicos para todo el personal.
Aprobar el Mapa de Normativa con la lista de Normativa y Procedimientos de seguridad para la implantación del ENS.
Asesorar en materia de seguridad de la información, siempre y cuando le sea requerido.
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
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
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.

8. GESTIÓN DE RIESGOS

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.
Como metodología base para la realización de los análisis de riesgos se utilizará MAGERIT, siendo esta metodología la más recomendable.
El análisis se realizará:

- Regularmente, una vez al año.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

De acuerdo con la escala de riesgos de la metodología MAGERIT, el nivel de riesgo deberá situarse por debajo de nivel MEDIO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser BAJO). Valores de riesgo residual mayores a BAJO deberán ser aceptados explícitamente por el CSI, previa justificación de la conveniencia de su aceptación.
Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

9. DATOS DE CARÁCTER PERSONAL

Aleatica solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos.

10.ESTRUCTURA DE LA NORMATIVA INTERNA DE SEGURIDAD

El desarrollo de la presente PSI responde al contenido de la guía de seguridad CCN-STIC-805. Asimismo, se establece la obligación de consultar, analizar y atender a lo recogido en las distintas normas técnicas, comprendiendo las reglas generales CCN-STIC en el desarrollo de cada uno de los procedimientos e instrucciones técnicas donde proceda.
El cuerpo normativo sobre seguridad integral es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior.
Dichos niveles de desarrollo normativo son los siguientes:

- Primer nivel normativo: Política de Seguridad de Aleatica.
  El Responsable de Seguridad será el responsable de su elaboración y propuesta.
- Segundo nivel normativo: Todas las normas de seguridad y otros documentos marco. Las mismas desarrollan y detallan la Política de Seguridad Integral, y se centrarán en un área o aspecto determinado de la seguridad de la información.
  El Responsable de Seguridad será el responsable de su elaboración y propuesta.
- Tercer nivel normativo: Procedimientos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la PSI.

El Responsable de Sistemas será el responsable de su elaboración y propuesta.
Además de los documentos citados, la documentación de seguridad del sistema podrá contar con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

11.DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política de Seguridad se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.
La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad se encontrará a disposición de todo el personal de Aleatica que necesite conocerla y, en particular, el personal que opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por Aleatica.

12.NOTIFICACIÓN DE INCIDENTES

De conformidad con los dispuesto en el artículo 33 del RD 311/2022, Aleatica notificara al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogida en el Anexo I de dicho cuerpo legal.

13.MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.
Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización.
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

14.OBLIGACIONES DEL PERSONAL

Todo el personal de Aleatica, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información 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.

Para que conste a los efectos oportunos, firma la presente política de seguridad de la información:

Dirección ALEATICA	
Nombre:	Rodrigo Figueroa Firmado digitalmente por Rodrigo Figueroa Fecha: 2024.03.08 10:59:58 -06'00'
Fecha:	