1. OFICIALIZACIÓN

Autorizó
Valentín Alonso
Director General

Validó
Basilio Barbero
Director Corporativo de TI

Realizó
Miguel Benavente
Jefe de Ciberseguridad

2. CONTROL DE VERSIONES

Documento Anterior	Versión	Documento Actual	Versión	Descripción del Cambio
N/A	N/A	PO-AV-TI-001	01.00	Documento inicial
PO-AV-TI-001	01.00	PO-AV-TI-001	01.01	Se añaden las definición de algunos principios fundamentales del ENS.
PO-AV-TI-001	01.01	PO-AV-TI-001	01.02	Se incluye el nombramiento del Responsable de Seguridad como Persona de Contacto con las Administraciones cliente (POC).

3. OBJETIVO

Exponer la Política de Seguridad de la Información de la Entidad, entendida como conjunto de principios básicos y líneas de actuación a los que la organización se compromete.

4. ALCANCE

Este documento afecta a todas las organizaciones asociadas o vinculadas a Mobility ADO incluidas en documento ***Alcance y Categorización,*** perteneciente al Sistema de Gestión de Seguridad de la Información, en el ámbito de aplicación del Real Decreto 311/2022, del 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

5. POLÍTICAS

5.1. Principios fundamentales de esta Política

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, en su transmisión, transporte, almacenamiento y hasta su borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

- **Principio de confidencialidad:** la información y los sistemas de información deberán ser accesibles únicamente para aquellas personas, órganos, entidades y/o procesos expresamente autorizados para ello. A esto se suma la obligación de secreto profesional de todo el personal que tenga acceso a la información.
- **Principio de integridad:** se deberá garantizar el mantenimiento de la integridad de la información, así como de los procesos de tratamiento de la misma, estableciéndose mecanismos para asegurar que los procesos de creación, recepción, tratamiento, almacenamiento y distribución de la información contribuyan a preservar que sea veraz y completa.
- **Principio de disponibilidad y continuidad:** se deberá garantizar un nivel de disponibilidad en los sistemas de información y se dotará de medidas necesarias para asegurar la continuidad de los servicios y su recuperación ante posibles contingencias graves.
- **Principio de trazabilidad**: se deberá mantener, en la medida de lo posible, una trazabilidad de la información y las entidades que la tratan, de forma que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

- **Principio de autenticidad**: se deberá garantizar que las entidades que tratan la información son quien dicen ser, así como la fuente de la que proceden los datos.
- **Principio de la seguridad como proceso integral**: la seguridad debe entenderse como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del SGSI estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural. Se prestará ambién 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, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.
- **Principio de líneas de defensa:** el sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita: a) 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; b) minimizar el impacto final sobre el mismo. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
- **Principio de vigilancia continua:** el sistema de información debe estar sujeto a una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.
- **Principio de reevaluación periódica:** las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario. Esta evaluación permanente del estado de la seguridad de los activos permitirá su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.
- **Principio de organización e implantación del proceso de seguridad:** la seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización. La política de seguridad deberá ser conocida y cumplida por todas las personas que formen parte de la organización.
- **Principio de gestión de personal:** El personal, propio o ajeno, relacionado con los sistemas de información deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.
- **Principio de profesionalidad:** La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento. La organización exigirá, de manera objetiva y no discriminatoria, que los proveedores que les presten servicios de seguridad cuenten con profesionales cualificados y

con unos niveles idóneos de gestión y madurez en los servicios prestados. La organización también determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

- **Principio de gestión del riesgo:** se deberá habilitar un proceso metódico, sistemático y continuo de análisis, evaluación y tratamiento de los riesgos para la seguridad de la información como mecanismo básico sobre el que debe girar la gestión de la seguridad de la información.
- **Principio de proporcionalidad en costes:** la implantación de los controles y medidas de seguridad que mitiguen los riesgos de seguridad de la información deberá realizarse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará de que los recursos para el SGSI estén disponibles.
- **Principio de concienciación y formación:** se desarrollarán iniciativas que permitan al personal involucrado en el SGSI conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De la misma forma, se fomentará la formación específica en seguridad TIC de todas aquellas personas que gestionan y administran los sistemas de información y los dispositivos de red y telecomunicaciones.
- **Principio de mínimo privilegio**: los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.
- **Principio de prevención:** se desarrollarán planes y actuaciones específicas orientadas a prevenir la ocurrencia de incidentes relacionados con la seguridad de la información.
- **Principio de detección y respuesta:** se debe monitorizar la operación del sistema continuamente para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, respondiendo eficazmente, a través de los mecanismos establecidos, a los incidentes de seguridad que ocurran.
- **Principio de mejora continua:** se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad de la información planificados anualmente y el grado de eficacia de los controles y medidas de seguridad implantadas, con el fin de adecuarlos a la evolución de los riesgos y el entorno tecnológico cambiante.
- **Principio de la seguridad de la información en el ciclo de vida de los sistemas:** las especificaciones de seguridad de la información se incluirán en todas las fases del ciclo de vida de los sistemas y servicios, a través de los correspondientes procedimientos de control.
- **Principio de autorización y control de accesos:** el acceso controlado a los sistemas de información comprendidos en el alcance deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.
- **Principio de protección de las instalaciones:** los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

- **Principios para la adquisición de productos de seguridad y contratación de servicios de seguridad:** en la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información dentro del alcance, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
- **Principio de integridad y actualización de sistemas:** la inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
- **Principio de protección de la información almacenada y en tránsito:** se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
- **Principio de prevención ante otros sistemas de información interconectados:** se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión.
- **Principio de registro de la actividad y detección de código dañino:** se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Se analizarán las comunicaciones entrantes y salientes, únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino, así como otros daños relacionados.
- **Principio de gestión de incidentes de seguridad:** la organización dispondrá de procedimientos de gestión de incidentes de seguridad acordes a los requisitos exigibles a la misma. Asimismo, dispondrá de mecanismos de detección, criterios de clasificación, 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 del sistema.

5.2. Introducción

La información es un activo que, al igual que otros activos importantes, es esencial para las actividades de la organización y, por consiguiente, necesita ser debidamente protegida. La información puede ser almacenada de muchas formas, incluyendo: formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato material (por ejemplo, papel), así como la información intangible que forma parte del conocimiento del personal.
Toda la información guardada y procesada por la organización está expuesta a ataques, errores, riesgos naturales (por ejemplo, inundaciones o incendios), etc. y está expuesta a vulnerabilidades inherentes en su uso. Por tanto, este activo debe ser adecuadamente protegido, mediante controles y medidas de seguridad, frente a las distintas amenazas que puedan afectarle, independientemente de los soportes en la que se encuentre

(papel o soporte digital), medios de transmisión, sistemas, equipos o personas que intervengan en su recogida, registro, tratamiento o supresión.
La Seguridad de la Información es la protección de este activo con la finalidad de asegurar que la información no está accesible a aquellas personas o entidades no autorizadas, que dicha información es veraz y no ha sido objeto de manipulaciones no autorizadas y que está disponible cuando se necesita.
Para ello, los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) y la vigente normativa de protección de datos personales, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
Los diferentes departamentos deben cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en la realización de los proyectos.
Los departamentos deben estar preparados para prevenir, detectar, reaccionar y conservar los datos e informaciones ante incidentes 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.
La Seguridad de la Información es un proceso que requiere de medios técnicos y humanos, en la que es fundamental la máxima implicación y colaboración de todo el personal de la organización.
La Dirección es consciente del valor de la información y está profundamente comprometida con la política descrita en el presente documento.

5.2.1. Prevención

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detección, los servicios deben monitorizar la operación de manera continua para detectar actividades o comportamientos anómalos.

La monitorización es especialmente relevante cuando se establecen líneas de defensa compuestas por múltiples capas de seguridad. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.2.3. Respuesta

Los departamentos deben:

- Establecer 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).
- Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5.2.4. Conservación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC. El sistema de información garantizará la conservación de los datos e información en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

5.3. Objetivos

El marco para establecer los objetivos anuales del SGSI es el siguiente:

- Gestionar los riesgos que existen para la seguridad de la información de una forma sistemática, completa y contrastada a nivel mundial.
- Aumentar confianza de los clientes y otras partes interesadas, en cuanto a la seguridad de la información que nos depositan, y a la que tenemos (o podríamos) tener acceso.
- Cumplir con las obligaciones contractuales contraídas con los clientes, tantos externos como internos.
- Cumplir con las disposiciones y requisitos marcados por la normativa de protección de datos personales y el resto de leyes aplicables a la organización.
- Asegurar la mejora continua del SGSI para responder a los cambios futuros.

La Dirección es la responsable de revisar este marco de objetivos y establecer un nuevo marco.

5.4. Misión de la Organización

La Dirección de **Avanza** quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas su convencimiento de que la seguridad es un factor clave para el correcto desarrollo de la organización, por lo que han de cumplir con las directrices que aquí se detallan.

Depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos asumiendo su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

5.5. Marco Normativo

Las leyes, reglamentos, y otra normativa, nacional o internacional, a la que la entidad está sujeta es la siguiente:

- 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 32/2002, 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, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Las partes interesadas y requisitos normativos y regulatorios se han definido en el documento ***Partes interesadas y Requisitos***.

5.6. Organización de la seguridad de la información

5.6.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información se constituye como órgano colegiado de la organización y está compuesto por los siguientes cargos:

- Representante de la Dirección
- Responsable de la Seguridad de la Información
- Responsable del Servicio
- Responsable de la Información
- Responsable del sistema

El Comité de Seguridad de la Información articulará la coordinación, en materia de seguridad de la información, entre todas las áreas de la organización.

Funciones:

- Atender las inquietudes de la Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto a ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto a ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- 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 diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar 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 TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver 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.

Secretaría:
El Responsable de la Seguridad de la Información es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Jerarquía:
El Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

5.6.2. Roles, funciones y responsabilidades

A continuación, se describen los roles que existen en la organización y sus responsabilidades.

5.6.2.1. Responsable de la Información

Función: Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS.
Responsabilidades:

- El Responsable de la Información tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección.

- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad, integridad, disponibilidad, trazabilidad o autenticidad.
- Determinación, junto con el Responsable del Servicio o del Comité de Seguridad de la Información, de los niveles de seguridad requeridos en cada dimensión.
- Aceptación, junto con el Responsable del Servicio, del riesgo residual resultante del Análisis de riesgos.

Figura:

Puede tratarse de una persona física singular o de un órgano colegiado, formando parte del Comité de Seguridad de la Información.

Esta responsabilidad puede ser compartida con la del Responsable del servicio.

5.6.2.2. Responsable del Servicio

Función: Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS.
Responsabilidades:

- El Responsable del Servicio tiene la potestad de determinar los niveles de seguridad de los servicios.
- Aunque la aprobación formal de los niveles de seguridad de los servicios, corresponda al Responsable del Servicio, se puede recabar una propuesta del Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

Figura:

Puede tratarse de una persona física singular o de un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información.

Esta responsabilidad puede ser compartida con la del Responsable de la información.

5.6.2.3. Responsable de la Seguridad de la Información

Función: Determina las decisiones de seguridad pertinentes para garantizar la seguridad de la información, preservando su confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, y así satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
Responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo con lo establecido en la Política de Seguridad de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información.
- Secretaría y liderazgo del Comité de Seguridad de la Información.
- Responsable del Control Documental del Sistema, en coordinación con los responsables de otros sistemas de gestión.
- Revisión de documentos implicados en el sistema.
- Aprobar aquellos documentos que no impliquen en su contenido decisiones estratégicas de alto nivel.
- Publicación de documentos.

- Supervisar la custodia y mantenimiento del archivo y los registros definidos para el procedimiento.
- Convocar y dirigir el Comité de Seguridad de la Información, elaborando las pertinentes Actas de Reunión.
- Presentación detallada de los informes de estado del Sistema a la Dirección.
- Supervisar el Inventario de Activos de la organización.
- Seguimiento de la Seguridad de la Información en la organización.
- Traslado al Comité de Seguridad de la Información de asuntos de interés en el campo de la Seguridad de la Información.
- Creación, presentación, mantenimiento y ejecución del Plan de Auditoría.
- Responsabilidad de las acciones formativas en Seguridad de la Información para el personal de la organización, en coordinación con el área de Recursos Humanos.
- Responsable de ejecución de las iniciativas de mejora de seguridad aprobadas por la Dirección.
- Llevar a cabo el seguimiento y control sobre los indicadores y registros.
- Validar los contenidos sobre seguridad en los documentos contractuales con clientes y proveedores (plantillas de ofertas, ofertas, especialmente las no sujetas a plantillas previas, pliegos, etc.) y articular la interlocución en esta materia con los correspondientes responsables de seguridad.
- Servir de Punto de Contacto (POC) para los clientes, canalizando y supervisando tanto el cumplimiento de los requisitos de seguridad del servicio prestado como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Figura:

Deberá ser una persona física, jerárquicamente independiente del Responsable del sistema.

5.6.2.4. Responsable del Sistema

Función: Se encarga, en coordinación con los equipos globales, de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad de la Información.
Responsabilidades:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles del mismo.
- Cerciorarse de que las medidas específicas de seguridad se integran adecuadamente dentro del marco general de seguridad.
- El Responsable del Sistema puede acordar la suspensión del manejo de cierta información, o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

- Elabora los procedimientos operativos de seguridad, que serán aprobados por el Responsable de la Seguridad de la Información.
- Elabora, junto con el Responsable de la Seguridad de la Información, los planes de mejora de la seguridad.
- Elabora los planes de continuidad, que serán validados por el Responsable de la Seguridad de la Información.
- Realizar ejercicios sobre los planes de continuidad elaborados para analizar su eficacia.
- Decretar, cuando así sea conveniente, la suspensión temporal del servicio.
- Elabora el ciclo de vida (especificación, arquitectura, desarrollo, operación y cambios), que será aprobado por el Responsable de Seguridad de la Información.
- Respuesta a incidentes de seguridad de la información.
- Planificar la implantación de salvaguardas en el Sistema.

Figura:
Deberá ser una persona física, esta figura puede ser compartida con el Administrador del sistema / de la seguridad del sistema.

5.6.2.5. Administrador del Sistema/de la seguridad del Sistema

Función: Coordinar y supervisar la implantación y eficacia de las medidas de seguridad establecidas, en coordinación con los equipos globales, y garantizar que el sistema de información tiene implantadas, y en perfecto estado de funcionamiento, las medidas de seguridad establecidas.
Responsabilidades:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Garantizar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Junto con los equipos globales, monitorizar el estado de la seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

- Informar a los Responsables de la Seguridad y del Sistema 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.
- Aplicar la configuración de seguridad elaborada por el Responsable de Seguridad de la Información.
- Implantar las medidas de seguridad o dar soporte cuando sea requerido en la implantación.
- Aplicar los procedimientos de seguridad operativos aprobados por el Responsable de la Seguridad de la Información.
- Monitorizar el estado de la seguridad del sistema en coordinación con los departamentos globales encargados cuando sea necesaria su implicación.
- Cooperación en la resolución y respuesta técnica a incidentes de seguridad de la información en coordinación con los equipos globales cuando sea necesaria su implicación.

Figura:
Deberá ser una persona física, esta figura puede ser compartida con el Responsable del sistema.

5.6.2.6. Delegado de Protección de Datos

Función: Asesora y supervisa el cumplimiento de la normativa de protección de datos en la organización, así como sus procesos.
Responsabilidades:

- Garantizar el cumplimiento de la normativa de protección de datos en la Organización, tanto desde el punto de vista jurídico, como desde el punto de vista de la seguridad de los datos personales.
- Promover la formación y concienciación en materia de protección de datos.

Posición:

- El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Autoridad de Control.
- El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada, y en tiempo oportuno, en todas las cuestiones relativas a la protección de datos personales.
- El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño sus funciones, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.
- El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones.
- El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio.
- Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

- En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto.
- El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.
- Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos.
- Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Funciones:

- 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 materia de protección de datos.
- Supervisar el cumplimiento de la normativa de protección de datos en la organización y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, 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, en su caso, y supervisar su aplicación.
- Cooperar con la Autoridad de Control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, en su caso.
- Intervenir y dar respuesta a las reclamaciones que hayan presentado los afectados contra la entidad con carácter previo a la presentación ante la Autoridad de Control, así como las remitidas por las propias Autoridades de Control.
- Atender a los interesados en lo que respecta a consultas relativas al tratamiento de datos personales y ejercicio de los derechos.
- Verificar, periódicamente, la eficacia de las medidas de seguridad implantadas.

Tareas:

- Coordinará, junto con el Responsable de Seguridad de la Información, la puesta en marcha y difusión de las medidas de seguridad que afecten a los datos personales y controlará el cumplimiento de las mismas.
- Analizará las incidencias registradas que afecten, o puedan afectar, a los datos personales, tomando las medidas oportunas en colaboración con el responsable del tratamiento.
- Analizará las violaciones de la seguridad que se produzcan y realizará, en su caso, la notificación de las mismas a la Autoridad de Control.

- Comprobará, periódicamente, que las copias de respaldo de los datos personales se realizan según la política y procedimientos establecidos.
- Comunicará al responsable del tratamiento cualquier cambio que se haya realizado en los sistemas de información que afecten a datos personales (como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc.), procediendo a la actualización de la documentación pertinente.
- Periódicamente realizará o promoverá la realización de una auditoría de la eficacia de las medidas de seguridad implantadas para la protección de los datos personales.

5.6.3. Procedimiento de designación

Los distintos roles serán nombrados por la Dirección y aprobados formalmente en el documento ***Designación de responsables de la seguridad de la información***. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.
Las designaciones se publicarán en el espacio de documentación del SGSI.
Con la designación se les hará entrega del documento de ***Aceptación de roles en seguridad de la información***, que debe ser firmado por la persona designada, en su caso.

5.6.4. Funciones incompatibles

En virtud de la segregación de tareas que establece una adecuada gestión de la seguridad de la información, se establecen las siguientes incompatibilidades:

Desarrollo	Configuración y mantenimiento	Supervisión / auditoría	Operación
Incompatible con Operación	Incompatible con Operación	Incompatible con Desarrollo	Incompatible con Desarrollo
Incompatible con Supervisión / auditoría	Incompatible con Supervisión / auditoría	Incompatible con Configuración y mantenimiento	Incompatible con Configuración y mantenimiento
		Incompatible con Operación	Incompatible con Supervisión / auditoría

Una misma persona no puede desempeñar dos o más funciones que sean incompatibles según la tabla anterior.

5.6.5. Coordinación y resolución de conflictos

La existencia de problemas de coordinación o conflictos entre diferentes roles se resolverá de la siguiente forma:

1. Se notificará la situación al Responsable de la Seguridad de la Información para que convoque una reunión del Comité de Seguridad de la Información a la mayor brevedad posible.
2. La situación será expuesta al Comité de Seguridad de la Información para que la analice y de una respuesta colegiada a la situación.
3. Quedarán reflejadas en un acta las conclusiones y los acuerdos alcanzados.

5.6.6. Usuarios

Cualquier persona que acceda a la información gestionada por la organización será considerada un usuario. Los usuarios son responsables de su conducta cuando accedan a información o utilicen los sistemas de información de la organización. El usuario es responsable de todas las acciones realizadas con sus identificadores o credenciales personales.
Por tanto, los usuarios tienen la obligación de:

- Conocer y cumplir la Política de Seguridad de la Información, las normas, procedimientos e instrucciones correspondientes.
- Proteger y custodiar la información de la organización, evitando la revelación, transmisión o comunicación al exterior, borrado, mal uso o destrucción (accidental o no autorizada) de la misma, independientemente del soporte en el que se encuentre o los medios por los que ha sido accedida o conocida.

5.7. Datos personales

La organización trata datos personales y se preocupa por la adecuada protección de los mismos. El tratamiento de datos personales involucra una serie de riesgos relacionados con la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de estos datos.
La gestión de riesgos de privacidad se alineará con el análisis de riesgos de la seguridad. El DPD podrá, a petición del responsable del tratamiento, proporcionar asesoramiento y herramientas específicas tanto para esta gestión de riesgos, como para la realización de evaluaciones de impacto en la privacidad para los tratamientos, cuando sea requerido por un elevado nivel de riesgo.
Los datos personales a proteger incluyen todos aquellos que son objeto de tratamiento por nuestra parte (ya sean datos de clientes, potenciales clientes, proveedores, trabajadores, contactos, colaboradores externos, etcétera).
Por ello, tanto la organización, como todo su personal, ya sea interno o externo, que esté involucrado de alguna forma en el tratamiento de datos personales, debe:

- Guardar secreto y confidencialidad de la información personal que trata.
- Proteger los datos personales que esté tratando y custodiarlos para que el personal no autorizado no tenga acceso a ellos.
- Cumplir con los principios de protección de datos (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva).
- Garantizar que los interesados puedan ejercer sus derechos (información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición y decisiones individuales automatizadas).
- Cumplir, y en su caso, hacer cumplir, los controles y las medidas de seguridad que la organización ha implantado para proteger la seguridad de los datos personales, evitando que pueda resultar comprometida la confidencialidad, integridad o disponibilidad de dichos datos.
- Comunicar inmediatamente, según los procedimientos habilitados para ello, las incidencias que puedan afectar a la seguridad de los datos personales y que puedan comprometer su confidencialidad, integridad o disponibilidad, así como el incumplimiento de los requisitos dispuestos por la normativa de protección de datos personales.
- Cumplir con todos los requisitos y obligaciones legales impuestas por la normativa de protección de datos personales.

Todos los sistemas de información se ajustarán a las medidas de seguridad que sean requeridas por la normativa según la naturaleza y finalidad de los datos personales que se traten y de acuerdo con el análisis de riesgos relativo a la protección de datos personales que se ha realizado.
La documentación relativa a la normativa de protección de datos personales, a la que tendrá acceso el Delegado de Protección de Datos, incluye el Registro de Actividades de Tratamiento y toda la documentación requerida por dicha normativa.

5.8. Evaluación de riesgos y controles

Todos los sistemas sujetos a esta Política deberán realizar 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 cambie la información manejada.
- Cuando cambien los servicios prestados o los activos que los soportan.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia de los distintos tipos de información manejados y los diferentes servicios prestados.
El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

5.9. Seguridad de la información en nuevos proyectos

El gerente de cada proyecto que se inicie en la organización, afectado por el alcance del SGSI, y de acuerdo con el Responsable de la Seguridad de la Información, debe incluir las reglas y requisitos correspondientes sobre la seguridad de la información relacionada con el proyecto en cuestión.
En particular:

a) Los objetivos de seguridad de la información deben estar incluidos en los objetivos del proyecto.

b) Hay que realizar una evaluación de riesgos de seguridad de la información en una fase temprana del proyecto para identificar controles necesarios.

c) La seguridad de la información debe formar parte de la metodología aplicada en el proyecto.

El Responsable de la Seguridad de la Información debe contemplar y revisar con regularidad las implicaciones de seguridad de la información en todos los proyectos.

5.10. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará por medio de otras políticas de seguridad que afronten aspectos específicos (también denominada normativa de seguridad). Dichas políticas de seguridad estarán a disposición de todos los miembros de la organización que necesiten conocerlas, en particular para aquellos que administren los sistemas de información y comunicaciones.
La documentación relativa a la seguridad de la información estará disponible en el apartado relativo al SGSI, compartido en Sharepoint, con accesos restringidos y compartimentados por usuarios teniendo en cuenta el principio de privilegio mínimo. El acceso al servicio de Sharepoint se realiza mediante verificación de usuario y contraseña y doble factor de autenticación mediante SMS. La documentación será gestionada por el Responsable de Seguridad según los procedimientos internos de elaboración y control documental.

5.11. Obligaciones del personal

Todos los miembros de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y el resto de políticas de seguridad (normativa de seguridad), siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.
Todos los miembros de la entidad atenderán actividades de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la entidad, en particular a los 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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

5.12. Terceras partes

Cuando la organización preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán los canales de reporte y coordinación y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando la organización utilice los servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de las políticas de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dichas políticas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerlas. Se establecerán procedimientos específicos de reporte y resolución de incidencias.
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 de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

6. PROCEDIMIENTO

No aplica

7. DIAGRAMA DE FLUJO

No aplica

8. DOCUMENTOS DE REFERENCIA

	Código	Nombre del documento
Internos	PO-AV-TI-001_R1	Partes interesadas y requisitos
	PO-AV-TI-001_R2	Designación de responsables de Seguridad de la Información

	Nombre del documento
Externos	

9. ANEXOS

Partes interesadas y requisitos del SGSI.

10. FORMATOS

	Código	Nombre del documento
Propios		

	Código	Nombre del documento
Otros	No aplica	

11. GLOSARIO

Concepto	Definición
Confidencialidad	es la propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.
Integridad	es la propiedad de la información por la cual solo es modificada por personas o entidades autorizadas y de una forma permitida, de manera que dicha información sea veraz y completa.
Disponibilidad	es la propiedad de la información de ser accesible y estar lista para su uso a demanda de una entidad autorizada.
Trazabilidad	es la propiedad o característica de la información consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
Autenticidad	es la propiedad o característica de la información consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Sistema de información	es el conjunto de aplicaciones, servicios, activos de tecnologías de la información y otros componentes que se utilizan para manejar la información.
Seguridad de la información	es la preservación de la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Concepto	Definición
Sistema de Gestión de la Seguridad de la Información (SGSI)	conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar sus objetivos de negocio.
Riesgo	estimación del nivel de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
Gestión del riesgo	actividades coordinadas para dirigir y controlar la organización con relación al riesgo.