POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La información forma un activo de primer orden para **TECNOLOGIA Y PERSONAS**, desde el momento en que resulta esencial para la prestación de gran parte de sus servicios, dependiendo de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Sin perjuicio de ello, las indiscutibles mejoras que aportan al tratamiento de la información vienen acompañadas de nuevos riesgos y, por lo tanto, es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependan de ella; debiendo ser administrados, estos sistemas, con la debida diligencia; tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada.

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, orientados a reducir los riesgos a los que están sometidos, hasta un nivel que resulte aceptable.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, 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 y estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo regulado por el Esquema Nacional de Seguridad.

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.

Dentro de cada organización sólo sus máximos directivos tienen las competencias necesarias para fijar dicho nivel, ordenar las actualizaciones y habilitar los medios para llevarlas a cabo.

En este sentido, establecer una política de seguridad de la información y hacer el subsiguiente reparto de tareas y responsabilidades, son actuaciones prioritarias, puesto que

son los instrumentos principales para el gobierno de la seguridad y constituyen el marco de referencia para todas las actuaciones posteriores.

El presente documento establece la política de seguridad de la información de **TECNOLOGIA Y PERSONAS** y se complementará con el desarrollo de la organización de la seguridad.

2. PREVENCIÓN, DETECCIÓN, REACCIÓN Y RECUPERACIÓN ANTE INCIDENTES

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.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido por el ENS, siendo la monitorización, especialmente relevante, cuando se establecen líneas de defensa de acuerdo con el mencionado ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

2.4. RECUPERACIÓN

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.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de **TECNOLOGIA Y PERSONAS** que dan soporte a los servicios de:

- Los Sistemas de Información que soportan los servicios de: Consultoría y Servicios de Instalación, Puesta en marcha, Garantías, Desarrollo, Comercialización y Mantenimiento de Hardware y Software.

De acuerdo la categorización del sistema vigente, que se realizan desde la Calle Princesa 25 Planta 3 28008 Madrid -

Aplica también a todos los miembros de la organización, sin excepciones.

4. MISIÓN

En **TECNOLOGIA Y PERSONAS** dentro del ámbito de los servicios que presta, anteriormente relacionados, actúa de acuerdo con los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios que contribuyen a satisfacer las necesidades y aspiraciones de sus clientes.

Por lo expuesto, en cada servicio, **TECNOLOGIA Y PERSONAS**, pone todo su empeño en prestar un servicio que se caracterice por ser funcional y seguro al mismo tiempo.

5. MARCO NORMATIVO

Como base normativa para realizar la presente guía de seguridad, se ha analizado la legislación vigente y aplicable, que afecta al desarrollo de las actividades de la organización y que implica la implantación de forma explícita de medidas de seguridad en sus sistemas de información.

El marco legal aplicable, en materia de seguridad de la información, viene establecido por la siguiente legislación:

- La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad establece, como uno de sus principios, que se debe disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos.
- Real Decreto 311/2022 del 5 de Mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

- Real Decreto 311/2022 del 3 de Mayo del 2022, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- 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-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

6. ORGANIZACIÓN DE LA SEGURIDAD

La gestión de la seguridad de la información implica la existencia de una estructura organizativa que, en consonancia con el artículo 10 del ENS defina unas responsabilidades diferenciadas en relación a requisitos de información, requisitos del servicio y requisitos de seguridad.

Esta estructura organizativa en materia de seguridad de la información de **TECNOLOGIA Y PERSONAS** queda establecida de la siguiente forma:

6.1. ROLES UNIPERSONALES

Responsable de la información:

- Determina los requisitos de seguridad de la información tratada, según los parámetros del Anexo I del ENS.
- Aprobación de los niveles de seguridad de la información. (La presente actividad es indelegable.)
- Valorar las consecuencias de un impacto negativo sobre la seguridad de la información, teniendo en cuenta la 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.

Responsable del servicio:

- Determinar los niveles de seguridad de los servicios, según los parámetros del Anexo I del ENS.
- Aprobación de los niveles de seguridad de los servicios. (La presente actividad es indelegable.)
- 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, teniendo en cuenta la 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.

Responsable de la seguridad:

- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
- Exigir, de manera objetiva, a aquellas organizaciones que les presten servicios de seguridad, que cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
- Valorar y escoger, al momento de la adquisición de productos de seguridad relacionados con las tecnologías de la información y de comunicaciones, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados; salvo en aquellos casos en que las exigencias de proporcionalidad, en cuanto a los riesgos asumidos, no lo justifiquen a juicio de éste.
- Ampliar las medidas de seguridad receptadas en el Anexo II del ENS y aquellas necesarias para garantizar el adecuado tratamiento de datos personales.
- Reemplazar las medidas de seguridad receptadas en el Anexo II del ENS siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del Real Decreto.
- Indicar en la Declaración de Aplicabilidad, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II del ENS que compensan.
- Formalizar y firmar la Declaración de Aplicabilidad.
- Analizar los informes de autoevaluación y/o los de auditoría y elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Responsable del Sistema:

- Su función principal es encargarse de la operación del sistema de información.
- Atender a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Adoptar las medidas correctoras adecuadas, en base a las conclusiones que recibe de parte del Responsable de Seguridad, dimanadas del análisis que realiza de los informes de autoevaluación y/o auditorias.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, podrá acordar la retirada de operación de alguna información, servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

Delegado de Protección de Datos:

- Asesorar respecto de la documentación necesaria para demostrar el cumplimiento con el RGPD y la LOPDGDD, incluidas, entre otras, políticas, procedimientos, contratos, plantillas y formularios y velar por que se mantengan actualizados.
- Informar y proporcionar asesoramiento experto a todo el personal con respecto a su obligación de cumplir con las disposiciones del RGPD y la LOPDGDD correspondientes con respecto al tratamiento de datos personales.
- Supervisar el cumplimiento con el RGPD y la LOPDGDD e informar a las partes interesadas dentro de la Compañía de cualquier cambio de forma rápida.

- Actuar como único punto de contacto de la autoridad de control en cuestiones relacionadas con el tratamiento de datos personales y consultar con la autoridad de control, cuando sea necesario, sobre cualquier otra cuestión relevante de datos personales.
- Actuar como el principal punto de contacto de los empleados y todos los interesados y cooperar con todos los miembros del personal en asuntos de protección de datos.
- Proporcionar asesoría y orientación sobre la Evaluación del Impacto de la Protección de Datos (EIPD), incluida la realización o supervisión del desempeño de la EIPD.
- Asistir a la persona Responsable del Sistema al momento de informar sobre las violaciones de seguridad de datos personales y en la toma de las medidas necesarias para informar a las partes interesadas pertinentes cuando sea exigible.
- Supervisar el cumplimiento de las políticas de protección de datos y cualquier otro documento interno relacionado con la protección de datos.
- Asesorar a la organización sobre las Políticas de Privacidad a entregar a los interesados en el momento de la recogida de sus datos personales.
- El resto de funciones propias y que no estén aquí expresadas, que dimanen de la legislación vigente en materia de protección de datos personales.

Responsable del Sistema de Información:

- Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Adoptar las medidas correctoras adecuadas de las conclusiones de los informes de autoevaluación y/o los informes de auditoria analizados por el Responsable de la Seguridad competente.
- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

7. GESTIÓN DE RIESGOS

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
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad en diferentes materias que aplican en la organización, tales como:

- Política de uso adecuado de los recursos de la organización.
- Política de contraseñas.
- Política de dispositivos móviles.

- Política de escritorios limpios.
- Política de pantallas limpias.
- Política de criptografía.
- Política de ingeniería social.
- Política de copias de seguridad.
- Política de acceso remoto.
- Política de teletrabajo.
- Política de eliminación de metadatos.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará 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.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros atenderán a una sesión de concienciación en materia de seguridad TIC 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 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.

10. TERCERAS PARTES

Cuando **TECNOLOGIA Y PERSONAS** preste servicios a otros organismos y/o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, estableciéndose canales para el reporte y la coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **TECNOLOGIA Y PERSONAS** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias, garantizándose que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.

Dicho informe, deberá estar aprobado por los responsables de la información y los servicios afectados antes de seguir adelante.

11. DATOS DE CARÁCTER PERSONAL

TECNOLOGIA Y PERSONAS trata datos de carácter personal en su actividad diaria, por lo cual está sujeto al cumplimiento impuesto por la normativa en vigor, individualizadas en el punto 5. MARCO NORMATIVO de la presente política.

Todos los tratamientos que se realicen sobre datos personales, se ajustarán a lo requerido por la normativa vigente, velando porque dichos datos sean tratados de manera lícita, leal y transparente en relación con el interesado; recogidos con fines determinados, explícitos y legítimos y no sean tratados ulteriormente de manera incompatible con dichos fines; adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; exactos y, si fuera necesario, actualizados, adoptándose todas las medidas razonables para que se supriman o rectifiquen sin dilación aquellos datos personales que sean inexactos con respecto a los fines para los que se traten; mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales, no pudiéndose conservar durante períodos más largos a no ser que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la normativa aplicable vigente en la materia a fin de proteger los derechos y libertades del interesado; tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Existen y están a disposición de los interesados las Políticas de Privacidad aplicables al caso en concreto, las cuales podrá solicitar, sin coste alguno, mediante solicitud por escrito dirigida al siguiente e-mail: isos.ens.lopd@tecnologiaypersonas.es

12. APROBACIÓN Y ENTRADA EN VIGOR

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración o bien, siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.