Portal de
Transparencia

Política de seguridad de la información-ens

PLANIFICA
MADRID

Edición: 2.0
Fecha: 05/03/2025

Clasificación: uso público

Contenido

1. Introducción 2
2. Objeto y alcance 3
3. Objetivos de Planifica Madrid 3
4. Marco normativo 4
5. Principios de la seguridad de la información 5
6. Organización de la Seguridad 6
6.1.- Estructura documental del sistema de gestión 7
6.2.- Roles, funciones y responsabilidades 7
6.2.1.- Responsable de la Información 8
6.2.2.- Responsable del servicio 8
6.2.3.- Responsable de seguridad 8
6.2.4.-Responsable del sistema 9
6.2.5.- Comité de Seguridad TIC 9
7. Medidas o políticas de la seguridad de la información. 10
7.1.- Análisis y gestión de los riesgos 10
7.2.- Protección de datos de carácter personal 11
7.3.- Profesionalidad, concienciación y formación 11
7.4.- Seguridad ligada a las personas 11
7.5.- Gestión de activos de información 12
7.6.- Gestión de los Recursos Humanos 12
7.7.- Gestión de terceros 13
7.8.- Autorización y control de accesos a los sistemas de información 13
7.9.- Adquisición, desarrollo y mantenimiento de sistemas de información 13
7.10.- Registro de actividad 14
7.11.- Gestión de incidentes de seguridad 14
7.12- Protección física de las instalaciones 14
7.13.- Integridad y actualización del sistema 15
7.14.- Prevención de sistemas de información interconectados 15
7.15.- Protección de la información almacenada y en tránsito 15
7.16.- Continuidad de la actividad 15
7.17.- Mejora continua del proceso de seguridad 16

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN-ENS

1. Introducción

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece la obligación de las Administraciones Públicas y de todo su sector público de relacionarse a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2025, de 1 de octubre, regula el Esquema Nacional de Seguridad (ENS).

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

El ENS, de aplicación a todo el Sector Público, así como a las entidades del sector privado cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público, 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 necesarios para una protección adecuada de la información tratada y los servicios prestados por estas entidades, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

Desde su primera regulación por el RD 3/2010, el ENS ha estado en constante evolución, no sólo por la necesidad de mantener la conformidad con la diferente normativa europea que ha fijado el marco de actuación en los ordenamientos nacionales, sino también para garantizar una mejor respuesta a las tendencias de ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad, ajustándolos a la realidad y contexto actual de riesgos, y mejorando las capacidades de prevención, detección y respuesta ante incidentes.

La actual regulación del ENS prevista en el RD 311/2022, de 3 de mayo, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

El objetivo último de la seguridad de la información es garantizar que una organización, en este caso Planifica Madrid, pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias garantizando adecuadamente la seguridad de la información tratada y los servicios prestados.

El fundamento jurídico del presente documento se encuentra en el artículo 12 del citado RD 311/2022, que establece que, cada órgano o entidad con personalidad jurídica propia comprendido en su ámbito subjetivo de aplicación, deberá contar con una política de seguridad formalmente aprobada por el órgano competente y ésta deberá establecerse de acuerdo con los principios básicos señalados en el artículo 5: Seguridad como proceso integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua; reevaluación periódica y diferenciación de responsabilidades.

2. Objeto y alcance

Es objeto del presente documento la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el marco organizativo y tecnológico de Planifica Madrid, documento que constituye el conjunto de directrices que rige la forma en que la entidad gestiona y protege la información que trata y los servicios que presta y que, conforme a lo previsto en el artículo 12 del RD 311/2022, incluye los objetivos de Planifica Madrid, el marco regulatorio en que se desarrollan sus actividades, los diferentes roles de seguridad con la definición de sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, la estructura y composición del Comité de Seguridad, que es el órgano colegiado encargado de la gestión y coordinación de la seguridad, las directrices de estructuración de la documentación de la seguridad, y los riesgos derivados del tratamiento de datos personales.

La presente PSI es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la entidad en el desarrollo de sus funciones.

La seguridad de los sistemas de información debe comprometer a todos los miembros de la entidad, por lo que tanto la PSI como las Normas de Uso de los Sistemas de Información, desarrolladas en un documento anexo, deberán ser conocidas y aplicadas por todas las personas que forman parte de Planifica Madrid, en función del puesto que desempeñan y su nivel de acceso a la información, en aplicación del principio de diferenciación de responsabilidades.

Todas estas personas serán consideradas *usuarios* a los efectos del presente documento.

3. Objetivos de Planifica Madrid

La Dirección de Planifica Madrid asume el compromiso de garantizar la seguridad de la información tratada en el desarrollo de su actividad corporativa adecuando sus sistemas TIC (Tecnologías de Información y Comunicaciones) a los principios básicos y requisitos mínimos previstos en el RD

311/2022, de 3 de mayo, creando las condiciones necesarias de seguridad en el uso de los medios electrónicos.

Para ello adoptará las medidas concretas que permitan que la información tratada en el desarrollo de los servicios prestados esté protegida durante todo su ciclo de vida, desde su creación o recepción, su procesamiento, comunicación, almacenamiento, difusión y hasta su eventual borrado o destrucción.

La adecuada protección de la información tratada implica asegurar el acceso, la disponibilidad (garantía de que los recursos del sistema se encontrarán operativos cuando se necesiten, especialmente los correspondientes a la información crítica), la integridad (disponibilidad de la información tal y como se almacenó por el usuario autorizado), la confidencialidad (disponibilidad de la información sólo para los usuarios autorizados), autenticidad (seguridad en la identidad u origen de la información) y trazabilidad (seguridad para ciertos datos de quién hizo qué y en qué momento).

Con el objetivo de garantizar la seguridad y la calidad de la información, así como la prestación continuada de los servicios, Planifica Madrid, mediante el oportuno análisis de riesgos ha de adoptar medidas tanto preventivas que sean proporcionadas a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estos estén expuestos, minimizando los mismos a niveles aceptables, como medidas de detección de amenazas y medidas correctivas, que supongan una respuesta rápida y efectiva ante posibles incidentes, de modo que estos no afecten gravemente a la información tratada, y orientadas al mismo tiempo a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Estas medidas serán sometidas a supervisión y reevaluación continua adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, lo que permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

4. Marco normativo

El marco legal relativo a la seguridad de la información cuyo cumplimiento deberá ser objeto de verificación de manera periódica es el siguiente:

- En materia de sistemas de información:
  - Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad.
  - Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
  - Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
  - Ley 9/2017, de 8 de noviembre de Contratos del Sector Público.

- En materia de seguridad de las redes y sistemas de información:

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el RDL 12/2018.
- Guías CCN-STIC

- 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.

5. Principios de la seguridad de la información

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información, y acorde con lo establecido en el RD 311/2022, de 3 de mayo y en las guías de seguridad de las tecnologías de la información y comunicación (guías CCN-STIC), se establecen los siguientes principios básicos:

- 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 iniciativas estratégicas de Planifica Madrid para conformar un todo coherente y eficaz.
- Responsabilidad diferenciada: en los sistemas de información se diferenciará la persona responsable de la información, la persona responsable del servicio, la persona responsable del sistema, y la persona responsable de la seguridad. En los supuestos de tratamiento de datos personales se identificará además a la persona o unidad responsable de tratamientos.
- Seguridad integral: la seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema de información, 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.

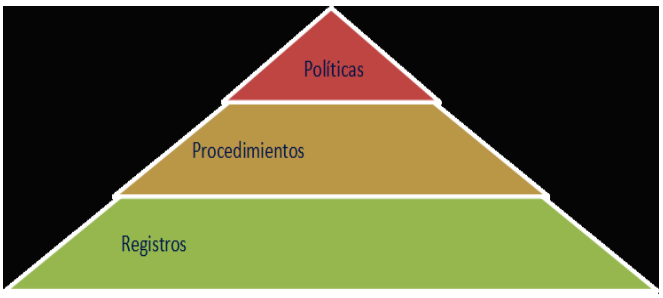
- Gestión de los riesgos: el análisis y gestión de los riesgos será parte esencial del proceso de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos, y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y con dichas competencias entre sus funciones.
- Seguridad desde el diseño y por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Planifica Madrid considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y trasversal.
- Vigilancia continua: de forma que la evaluación permanente del estado de la seguridad de los activos permita medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

6. Organización de la Seguridad

La gestión de la seguridad de los sistemas de información en las organizaciones - definición, implantación y mantenimiento - exige establecer una Organización de la Seguridad. Tal organización debe determinar con precisión los diferentes actores que la conforman, sus funciones y responsabilidades, así como la implantación de una estructura que las soporte.

6.1.- Estructura documental del sistema de gestión

La estructura de nuestro sistema de gestión es la siguiente:



Donde:

Política: Es la declaración formal de intenciones que establece las directrices generales y los objetivos de seguridad de una organización. Define los roles y responsabilidades, así como los principios que guiarán la toma de decisiones en materia de seguridad.

Procedimiento: Es el conjunto de pasos detallados que describen cómo llevar a cabo una tarea específica relacionada con la seguridad de la información.

Registro: Es el documento que proporciona evidencia de que se han llevado a cabo las actividades de seguridad según lo establecido en las políticas y procedimientos.

La estructura documental del sistema de seguridad de la información de Planifica Madrid se compone de una Política de Seguridad, que es el presente documento, que establece los principios y objetivos generales, Procedimientos detallados para la implementación de las medidas de seguridad, y Registros que documentan el cumplimiento de dichos procedimientos. Esta estructura garantiza la coherencia y la trazabilidad de las actividades de seguridad, facilitando el cumplimiento de los requisitos legales y normativos.

La gestión de nuestro sistema es responsabilidad del Responsable del Sistema y estará disponible en un repositorio dentro del sistema de información al que se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de accesos.

6.2.- Roles, funciones y responsabilidades

La seguridad de los sistemas de información debe comprometer a todos los usuarios, y la PSI debe ser conocida por todas las personas que forman parte de Planifica Madrid, si bien la responsabilidad esencial en materia de organización de la seguridad de la información corresponde a la Dirección de la empresa. Es el Consejero Delegado de Planifica Madrid quien ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad,

incluyendo las de seguridad de la información, siendo el máximo responsable de la implantación el ENS. Es el encargado de definir los diferentes roles, asignar las distintas responsabilidades y facilitar los recursos adecuados a los usuarios para conseguir cumplir los objetivos dentro del marco de la ENS.

Acorde con el principio de diferenciación de responsabilidades previsto en el ENS, se definen los siguientes roles, responsables de velar por el cumplimiento de seguridad, que tendrán las siguientes funciones (siempre en el marco de la ENS):

En un primer nivel de gobierno, se encuentra el responsable de la información y el responsable del servicio.
En un segundo nivel de supervisión se encuentra el responsable de seguridad
En un tercer nivel operativo se encuentra el responsable del sistema

6.2.1.- Responsable de la Información

Información es la materia prima de la que se nutre la actividad de una organización, en este caso Planifica Madrid, y puede tener su origen en la propia entidad, en los ciudadanos y en terceras entidades, ya sean públicas o privadas (contratistas, proveedores, etc.).

El responsable de la Información, es la persona/órgano que determina los requisitos de seguridad de la información tratada, o, en terminología del ENS, la persona que determina los niveles de seguridad de la información, valorando las diferentes consecuencias de un impacto negativo. Esta valoración se efectuará atendiendo al grado de repercusión que este impacto negativo pueda tener en la capacidad de la empresa 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.

6.2.2.- Responsable del servicio

Es la persona/órgano que determina los requisitos de seguridad de los servicios prestados. Establece las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, a los que suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

6.2.3.- Responsable de seguridad

Es la persona que determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Las funciones esenciales del responsable de la seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo a lo establecido en la PSI de Planifica Madrid, estableciendo los controles y medidas técnicas y organizativas para asegurar los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Validar la implantación de los requisitos de seguridad necesarios
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Reportar sobre todas las cuestiones anteriores.

6.2.4.-Responsable del sistema

Es la persona que se encarga, por sí o a través de recursos propios o contratados, de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Sus principales funciones son:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación uy verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el maraco general de seguridad.

6.2.5.- Comité de Seguridad TIC

Órgano colegiado que coordina las funciones y esfuerzos de las diferentes áreas en materia de seguridad de la información en la entidad, para asegurar que las medidas adoptadas están alineadas con la estrategia decidida en la materia, evitando duplicidades.

Asimismo, es el órgano encargado de:

- Elaborar la estrategia de evolución de la organización en materia de seguridad de la información.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar y revisar regularmente la PSI para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la Información.
- Coordinar todas las funciones de seguridad de la organización.

- Implementar los medios y canales necesarios para que el responsable de seguridad maneje informes de incidentes y anomalías del sistema.
- En caso de incidentes, supervisará la investigación y promoverá su resolución.

- 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.

Este Comité estará formado por:

- El responsable de la Información.
- El responsable del servicio.
- El responsable de seguridad.
- El responsable del sistema
- El Delegado de Protección de Datos.

Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección de la empresa.

7. Medidas o políticas de la seguridad de la información.

Las directrices fundamentales de seguridad se concretan en un conjunto de medidas y políticas específicas que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones de Planifica Madrid en dicha materia:

7.1.- Análisis y gestión de los riesgos

El análisis y gestión de riesgos es parte esencial del proceso de seguridad y debe realizarse de manera continua y permanentemente actualizada.
El análisis de los riesgos es el estudio de los riesgos existentes y la valoración de las consecuencias de los mismos sobre los activos de información, considerándose un “activo” a estos efectos cualquier recurso crítico de Planifica necesario para cumplir con las obligaciones corrientes de la entidad y que es objeto de protección (personal, información, sistemas, instalaciones).
Todos estos activos son objeto de análisis, evaluándose las posibles amenazas a las que están expuestos. Este análisis permite determinar diferentes niveles de riesgo a partir de los cuales se adoptan las medidas adecuadas para el mantenimiento de un entorno controlado, minimizándolos para reducirlos a niveles aceptables.

Este análisis será objeto de revisión:

- Regularmente, al menos una vez al año.
- Cuando cambie la información maneada y/o los servicios prestados.

- Cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades graves.

Planifica utiliza la metodología MAGERIT para analizar los riesgos, realizando un análisis detallado de los que afecten a los activos recogidos en el inventario de activos, que queda recogido en un Documento de Análisis de Riesgos.

El Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados y asignará recursos para atender a las necesidades de seguridad de los diferentes sistemas de acuerdo con el análisis efectuado.

7.2.- Protección de datos de carácter personal

Cuando un sistema de información trate datos personales 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 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 permanente 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

7.3.- Profesionalidad, concienciación y formación

La seguridad de los sistemas de información es gestionada por personal de Planifica Madrid cualificado y personal externo especializado, que recibe y actualiza la formación necesaria para garantizar la seguridad de la información.

Tanto la PSI como la normativa de seguridad y los procedimientos e instrucciones al respecto que pudieran darse, deberán se adecuadamente comunicados y puestos en conocimiento de las personas y empresas que presten sus servicios en Planifica Madrid.

Se realizarán periódicamente actividades de concienciación y formación, y se entregará copia de la normativa correspondiente a los usuarios.

7.4.- 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 uso indebido de dichos activos.
En la actual PSI se establecen las directrices para gestionar y soportar la seguridad del personal, los activos y la información bajo la responsabilidad de Planifica Madrid.

Para su desarrollo se ha definido la normativa de seguridad de la información, en documento anexo, que contiene:

- Cómo hacer uso correcto de equipos, servicios e instalaciones y lo que se considera uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias.
- Procedimientos y guías técnicas que contemplan cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Todo el personal de Planifica Madrid deberá conocer y cumplir esta PSI y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer de los medios y recursos necesarios para formar e informar a los usuarios.

Las personas con responsabilidad en la operación o administración de sistemas TIC recibirán formación específica para el manejo seguro de los mismos.

Todo el personal de Planifica Madrid atenderá a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Asimismo, se establecerá un programa de concienciación continua para todos los usuarios de Planifica Madrid, en particular a los de nueva incorporación.

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**.**

7.5.- Gestión de activos de información

Los activos de información de cada Área o departamento se encuentran inventariados y categorizados y están asociados a un responsable.

7.6.- Gestión de los Recursos Humanos

Se establecerán medidas de seguridad ligadas al personal propio en las etapas correspondientes: antes, durante y después del cese de empleo o cambio de puesto de trabajo. Estas medidas también se extrapolarán a los contratistas que participen en los servicios prestados por Planifica Madrid, así como a personal externo que realice tareas dentro de la empresa.

RRHH incluirá instrucciones de seguridad de la información en las descripciones de los trabajos del personal de la empresa, informará a todo el personal que contrate de sus obligaciones con respecto al cumplimiento de la PSI y gestionará los compromisos de confidencialidad con el personal.
Asimismo

Los objetivos de esta política son, entre otros:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la incorporación del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Velar por que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la PSI de la organización en el curso de sus tareas normales.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

7.7.- Gestión de terceros

Se establecerán medidas de seguridad destinadas a mitigar el riesgo que suponen los accesos por parte de terceros a información, sistemas o instalaciones propiedad de Planifica o bajo su responsabilidad.
En este sentido, cuando Planifica Madrid maneje información de otras entidades se les hará partícipes de esta PSI. Planifica Madrid definirá y aprobará los canales para la coordinación del suministro de información y de los procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando Planifica Madrid utilice servicios de terceros o ceda información a terceros, también se les hará partícipes de esta PSI y de la Normativa de Seguridad existente que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.
Se establecerán procedimientos específicos de comunicación de las debilidades de seguridad existentes, y de incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia, así como de resolución de incidencias.

7.8.- Autorización y control de accesos a los sistemas de información

El acceso controlado a los sistemas de información debe estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información debidamente autorizados y exclusivamente para las funciones permitidas.
Se limitará por tanto 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 Planifica Madrid.

7.9.- Adquisición, desarrollo y mantenimiento de sistemas de información

Se contemplarán los aspectos de seguridad de la información en todas sus fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
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.
Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos de TIC.

7.10.- Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento de los objetivos de la seguridad de la información, así como asegurar la integridad y rendimiento de los dispositivos digitales puestos a disposición del personal de Planifica, 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.

7.11.- Gestión de incidentes de seguridad

Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
Esta política cubrirá los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas, tan pronto como se detecten los incidentes para activar la alarma.

7.12- Protección física de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones asociada están situadas en áreas protegidas debidamente dotadas de medidas de seguridad físicas y ambientales y con controles de acceso adecuados. Asimismo, se contempla la protección en su posible traslado y permanencia fuera de las áreas protegidas por mantenimiento u otros motivos.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de
Planifica Madrid: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El responsable de la Seguridad junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de las diferentes Áreas definirán los niveles de acceso físico del personal de Planifica Madrid a las Áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de Planifica Madrid cuando lo consideren apropiado.

7.13.- Integridad y actualización del sistema

Planifica Madrid se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por el Área de Sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en
relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

7.14.- Prevención de sistemas de información interconectados

Planifica Madrid, establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

7.15.- Protección de la información almacenada y en tránsito

Planifica Madrid establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

7.16.- Continuidad de la actividad

Planifica Madrid, con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo

7.17.- Mejora continua del proceso de seguridad

Planifica Madrid establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en el Esquema Nacional de Seguridad.

En Madrid a fecha de la firma

Firmado digitalmente por: CORBALAN RUIZ PEDRO
Fecha: 2025.03.06 13:45

Pedro Corbalán Ruiz
CONSEJERO DELEGADO

PLANIFICA MADRID

PLANIFICA MADRID, Proyectos y Obras, M.P., S.A.