SGSI-000 Anexo 1
POLÍTICA DE SEGURIDAD

Histórico de revisiones

Revisión	Fecha	Descripción	Aprobación
1	14/11/2024	Redacción inicial	Acta Comité de Gestión
2	27/05/2025	Incorporación requisitos NIS2 + ampliación alcance ENS	Acta Comité de Gestión
3	15/06/2025	Integración ISO 27001 + cambio de nomenclatura del documento + referencia **GRUPO EMPARK**	Acta Comité de Gestión
4	19/03/2026	Actualización según la Guía CCN-STIC-805 – Política de Seguridad de la Información (junio 2025)	Acta Comité de Gestión

Control de cambios

Revisión	Descripción del cambio
1	Redacción inicial
2	Incorporación requisitos NIS2 + ampliación alcance ENS
3	Integración ISO 27001 + cambio de nomenclatura del documento + referencia **GRUPO EMPARK**
4	Actualización según la Guía CCN-STIC-805 – Política de Seguridad de la Información (junio 2025)

Tabla de contenido

1 APROBACIÓN Y ENTRADA EN VIGOR

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

2 INTRODUCCIÓN

GRUPO GRUPO EMPARK 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 de **GRUPO EMPARK** 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 las condiciones de contratación para para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

Los departamentos de **GRUPO EMPARK** deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3 MISIÓN

GRUPO EMPARK es una empresa líder en la gestión de la movilidad urbana en la Península Ibérica, con más de 50 años de experiencia en el sector. Operando bajo la marca comercial Telpark, Empark ofrece soluciones integrales y especializadas para la gestión de aparcamientos, estacionamiento regulado en vía pública y carga eléctrica en España y Portugal.

La misión de **GRUPO EMPARK** es facilitar la movilidad urbana de bienes y personas de manera más rápida, fácil y sostenible. La empresa se destaca por su compromiso con la innovación tecnológica, la sostenibilidad y la inclusión de prácticas ambientales, sociales y de gobernanza (ESG) en su industria.

GRUPO EMPARK colabora estrechamente con administraciones públicas y empresas de gestión urbana para mejorar la vida y la movilidad en las ciudades, utilizando tecnologías de vanguardia y plataformas digitales para garantizar transparencia y accesibilidad a la información.

4 ALCANCE

4.1.1 Alcance ISO 27001

El alcance del Sistema de Gestión de Seguridad de la Información de **GRUPO EMPARK** es**,** de acuerdo con la norma UNE-ISO/IEC 27001:2023, es el sistema de información que da soporte a:

- Gestión de movilidad urbana; el diseño, la aplicación móvil, la explotación, la gestión y el control de estacionamiento regulado en la vía pública y de superficie.
- Servicio de carga eléctrica

Que se prestan desde las siguientes ubicaciones:

- Av. del General Perón, 36, 1ª planta - 28020 Madrid

4.1.2 Alcance ENS

El alcance del Sistema de Gestión de Seguridad de la Información de acuerdo con la norma RD311/2022 de **categoría ALTA** sobre los sistemas de información que dan soporte a:

- Gestión de movilidad urbana; el diseño, la aplicación móvil, la explotación, la gestión y el control de estacionamiento regulado en la vía pública y de superficie.
- Servicio de carga eléctrica

Que se prestan desde las siguientes ubicaciones:

- Av. del General Perón, 36, 1ª planta - 28020 Madrid

5 MARCO NORMATIVO

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos.

Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad.
- UNE-ISO/IEC 27001:2023, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- 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 (RGPD).
- CORRIGENDUM 8088/18, de 19 de abril, sobre corrección de errores en diferentes traducciones del RGPD.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- 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.
- 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.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- REGLAMENTO (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019 (ENCS 2019).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2).

6 PRINCIPIOS BÁISCOS

Los principios básicos son las directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

6.1 Alcance estratégico

La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.

6.2 Seguridad como proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar 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 TIC.

6.3 Gestión de la seguridad basada en los riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá 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. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

6.4 Prevención, detección, respuesta y conservación

6.4.1 Prevención

GRUPO EMPARK debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos. Estos controles, van a 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.

6.4.2 Detección

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

6.4.3 Respuesta

GRUPO EMPARK:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.4.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, las distintas áreas deben desarrollar, cuando sea necesario, planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del servicio de actividades de recuperación.

6.4.5 Conservación

La información gestionada debe mantenerse accesible y utilizable durante el tiempo que sea necesario para cumplir con las obligaciones legales, administrativas o contractuales. Este principio garantiza que la información no se pierda ni se degrade, y que pueda ser recuperada en condiciones adecuadas de calidad, integridad y autenticidad.

Se debe asegurar la continuidad operativa y la trazabilidad de las actuaciones de la organización, permitiendo responder ante auditorías, reclamaciones o revisiones.

6.5 Existencia de líneas de defensa

El sistema de información dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

6.6 Vigilancia continua y reevaluación periódica

GRUPO EMPARK llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permite a **GRUPO EMPARK** medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. **GRUPO EMPARK** reevaluará y actualizará periódicamente las medidas de seguridad, 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.

6.7 Seguridad por defecto y desde el diseño

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

6.8 Diferenciación de responsabilidades

GRUPO EMPARK tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

7 REQUISITOS MÍNIMOS

Esta política de seguridad de la Información complementa las políticas de seguridad de **GRUPO EMPARK** en materia de protección de datos de carácter personal.

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 8 ORGANIZACIÓN DE LA SEGURIDAD de esta Política.**
- Análisis y gestión de los riesgos, de acuerdo a lo previsto en el procedimiento **IU-SGSI-008 PLANIFICACIÓN.**
- Gestión de personal, de acuerdo a lo previsto en el procedimiento **IU-SGSI-015 GESTIÓN DE PERSONAL.**
- Profesionalidad, de acuerdo a lo previsto en el procedimiento **IU-SGSI-015 GESTIÓN DE PERSONAL.**
- Autorización y control de los accesos, de acuerdo a lo previsto en el procedimiento **IU-SGSI-009 CONTROL DE ACCESO.**
- Protección de las instalaciones, de acuerdo a lo previsto en el procedimiento **IU-SGSI-014PROTECCIÓN DE INSTALACIONES.**
- Adquisición de productos de seguridad y contratación de servicios de seguridad, de acuerdo a lo previsto en el procedimiento **IU-SGSI-008 PLANIFICACIÓN.**
- Mínimo privilegio, de acuerdo a lo previsto en el procedimiento **IU-SGSI-009 CONTROL DE ACCESO.**

- Integridad y actualización del sistema, de acuerdo a lo previsto en el procedimiento **IU-SGSI-010 EXPLOTACIÓN.**
- Protección de la información almacenada y en tránsito, de acuerdo a lo previsto en el procedimiento **IU-SGSI-020 PROTECCIÓN DE INFORMACIÓN.**
- Prevención ante otros sistemas de información interconectados, de acuerdo a lo previsto en el procedimiento **IU-SGSI-017 PROTECCIÓN DE COMUNICACIONES.**
- Registro de actividad y detección de código dañino, de acuerdo a lo previsto en el procedimiento **IU-SGSI-010 EXPLOTACIÓN.**
- Incidentes de seguridad, de acuerdo a lo previsto en el procedimiento **IU-SGSI-010 EXPLOTACIÓN.**
- Continuidad de la actividad, de acuerdo a lo previsto en el procedimiento **IU-SGSI-012 CONTINUIDAD DEL SERVICIO.**
- Mejora continua del proceso de seguridad, de acuerdo a lo previsto en el procedimiento **IU-SGSI-005 GESTIÓN DEL SISTEMA.**

8 ORGANIZACIÓN DE LA SEGURIDAD

La implantación de la Política de Seguridad en **GRUPO EMPARK** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol especifico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

- El Comité de Seguridad de la Información
- Responsables del Servicio (RSER)
- Responsables de la Información (RINFO)
- Responsable de Seguridad de la Información (RSEG o CISO)
- Responsable de Sistemas (RSIS)
- Delegado de Protección de Datos (DPD)
- Dirección

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

8.1 Comité de Seguridad de la Información

El Comité de Seguridad de la Información coordina la seguridad de la información en **GRUPO EMPARK**. Dicho Comité está compuesto por el Responsable del Servicio, el responsable de la Información, el Responsable de Seguridad de la Información y el Responsable del Sistema, y actuando el Responsable de Seguridad como Secretario.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;

- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.

- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.

- Supervisión y seguimiento de aspectos tales como:

    - Principales incidencias en la Seguridad de la Información;
    - Elaboración y actualización de planes de continuidad
    - Cumplimiento y difusión de las Políticas de Seguridad

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

8.2 Dirección

La Dirección de la empresa:

- Proporciona los recursos necesarios para el sistema de **GRUPO EMPARK**.
- Lidera el sistema.
- Se compromete a responder por las obligaciones inherentes a la seguridad de la información y proteger sus activos de información implementando las medidas de seguridad más apropiadas para conseguirlo de una manera efectiva con los recursos disponibles.

8.3 Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.
- Determina los niveles de seguridad de la información, efectuando las valoraciones del impacto que tendría un incidente que afectase a la seguridad de la información, así como posteriores modificaciones que fuesen necesarias.

8.4 Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio, efectuando las valoraciones del impacto que tendría un incidente que afectase este, así como posteriores modificaciones que fuesen necesarias.

8.5 Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos estratégicos de la organización.

El Responsable de Seguridad será el Punto de Contacto (PoC) en materia de seguridad de la información y tendrá las siguientes funciones:

- La determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio.

- Formalizar y aprobar la Declaración de Aplicabilidad, que incluirá las medidas seleccionadas del Anexo II del ENS, incluyendo las medidas compensatorias o complementarias de vigilancia.

- Analizar los informes de Auditoria que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.

- Aprobar explícitamente los cambios que impliquen un riesgo alto, con carácter previo a su implantación.

- Actuará como Punto o Persona de Contacto (POC), canalizando las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio con los destinatarios de los servicios.

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de **GRUPO EMPARK**.

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:

    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de **GRUPO EMPARK** y normativa de desarrollo.

- Supervisar (como responsable último) los incidentes de seguridad informática producidas en **GRUPO EMPARK.**

- Difundir en **GRUPO EMPARK** las normas y procedimientos contenidos en la Política de Seguridad de la Información de **GRUPO EMPARK** y normativa de desarrollo, así como las funciones y obligaciones de todo **GRUPO EMPARK** en materia de seguridad de la información.

- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.

- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de **GRUPO EMPARK.**

8.6 Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad de **GRUPO EMPARK**, de acuerdo a los objetivos estratégicos de **GRUPO EMPARK**.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- 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.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de **GRUPO EMPARK**, conforme a la estrategia de seguridad definida.
- Adoptar las medidas correctoras adecuadas derivadas de los informes de Auditoría. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

- Garantizar la actualización del inventario de activos de Sistemas de Información de GRUPO EMPARK.
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en GRUPO EMPARK.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

8.7 Delegado de Protección de datos

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

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas 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 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, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

8.7.1 Propietario de Activos

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la normativa aplicable en materia de Protección de Datos y aplicar, en su caso, los procedimientos correspondientes.
- Asegurarse de que el software que se utiliza tiene licencia.
- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Asegurarse de que el activo cuenta con el mantenimiento adecuado

- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- Asegurarse de que los soportes y equipos que contengan información sean desechados según lo establecido.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
- Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- Informar al responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.
- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

8.7.2 Propietario del Riesgo

El propietario del riesgo, asociado a uno o varios activos de información, tendrá las siguientes responsabilidades:

- Participar en el desarrollo del análisis y evaluación de riesgos realizada al menos con carácter anual
- Verificar la conformidad con los niveles de riesgo aceptable y colaborar en la aprobación de los mismos (que le afecten), así como la gestión de los riesgos asociado a los activos de información y los riesgos de los que es responsable.
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del riesgo deberá informar a su vez al responsable de Seguridad para tratar la incidencia.
- Informar al responsable de Seguridad cuando ocurran cambios del personal, la organización, o del resto de los activos de información, que pueda implicar una revisión o actualización del análisis de riesgos, o de los permisos de acceso asignados

8.8 Procedimiento de designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio:** Carlos Carballo Cuevas
- **Responsable de la Información:** Jordi Curià Piñol
- **Responsable de Seguridad:** Óscar Valderrama Romero
- **Responsable del Sistema:** Leandro F. de Castro
- **Delegado de protección de datos:** Pedro Manuel Fernández Atencia
- **Dirección:** Socios- Administradores

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene

que subordinar su actividad a ningún otro elemento de nuestra empresa.

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

8.9 Resolución de conflictos

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 General.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

9 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

10 DATOS DE CARÁCTER PERSONAL

GRUPO EMPARK trata datos de carácter personal.

Todos los sistemas de información de **GRUPO EMPARK** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado **5 MARCO NORMATIVO**, de la presente Política de Seguridad de la Información.

11 GESTIÓN DE RIESGOS

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

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

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento **IU-SGSI-010 EXPLOTACIÓN.**

12 OBJETIVOS DE SEGURIDAD

La Dirección de **GRUPO EMPARK** establece objetivos y metas enfocados hacia la evaluación del desempeño en materia de seguridad de la información, así como a la mejora continua en sus actividades, reguladas en el Sistema de Gestión de Seguridad de la Información que desarrolla esta política.

13 MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD D ELA INFORMACIÓN

GRUPO EMPARK garantiza un análisis continuo de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

La Dirección de **GRUPO EMPARK** se compromete al cumplimiento de mejora continua del Sistema de Gestión de Seguridad de la Información que desarrolla esta política.

14 ESTRUCTURA DE LA DOCUMENTACIÓN

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del SGI de **GRUPO EMPARK**, se definen en el procedimiento "**IU-SGSI-005 GESTIÓN DEL SISTEMA".**

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por la Dirección a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información aprobada por la Dirección. En ella se establecerán unas normas de uso aceptable de los sistemas de información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Ha de ser aprobada por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

15 CALIFICACIÓN DE LA INFORMACIÓN

Para calificar la información de **GRUPO EMPARK** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **IU-SGSI-020 PROTECCIÓN DE INFORMACIÓN.**

16 OBLIGACIONES DEL PEROSNAL

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

Los miembros de **GRUPO EMPARK** recibirán formación 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 **GRUPO EMPARK**, 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.

17 Terceras partes, prestadores de servicios y proveedores de soluciones

Cuando Grupo EMPARK preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

Cuando Grupo EMPARK 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, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

Dichas terceras partes quedarán sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que Grupo EMPARK pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

18 Gestión de incidentes de seguridad

Grupo EMPARK dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios. Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados

19 INCUMPLIMIENTO

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

19/03/2026

Firmado por la Dirección General