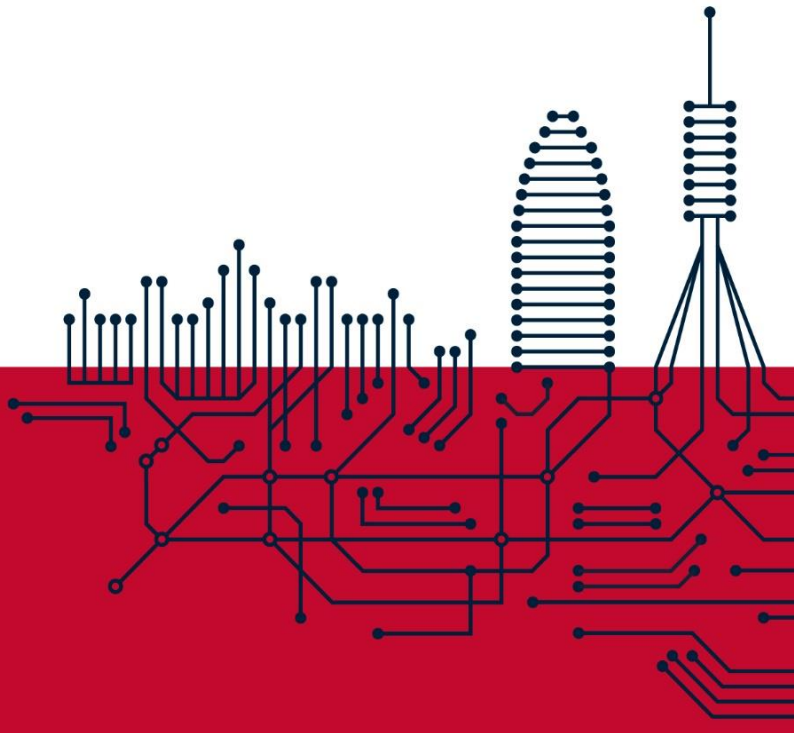
Smarting
ENGINEERING

Política de Seguridad de la Información



SGSI.PR.01.es

Versión	1.0
Fecha	12/02/2024

> Go beyond

CONTENIDO

1. OBJETIVOS Y MISIÓN DE SMARTING

Smarting, como empresa especializada en el desarrollo de soluciones digitales de ticketing para el transporte público, reconoce la importancia crítica de la seguridad de la información en el éxito continuo de sus operaciones y la satisfacción de sus partes interesadas. Esta política establece el marco para gestionar la seguridad de la información en la organización de acuerdo con los principios y requisitos de la norma ISO 27001 y del ENS (Esquema Nacional de Seguridad).

Objetivos de Seguridad de la Información

La política de seguridad de la información de Smarting tiene como objetivos fundamentales:

- Garantizar la confidencialidad, integridad y disponibilidad de la información crítica de la empresa y de sus clientes, así como asegurar la trazabilidad y autenticidad.
- Cumplir con las leyes, regulaciones y requisitos contractuales aplicables a la seguridad de la información en el ámbito del transporte público
- Fomentar una cultura de conciencia y responsabilidad en la gestión de la seguridad de la información entre los empleados.
- Establecer y mantener un sistema de gestión de la seguridad de la información que promueva la mejora continua y la adaptabilidad a los cambios tecnológicos y empresariales.

Compromiso con la Seguridad de la Información

La alta dirección de Smarting, representada por el CEO y el CTO, se compromete a:

- Proporcionar recursos adecuados para implementar y mantener un sistema de gestión de la seguridad de la información efectivo.
- Establecer roles y responsabilidades claros para la gestión de la seguridad de la información en todos los niveles de la organización.
- Fomentar la participación de los empleados en la protección de la información y proporcionar la formación necesaria para mejorar las competencias en seguridad de la información.
- Evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información y realizar ajustes según sea necesario.

2. MARCO LEGAL Y REGULATORIO

Smarting llevará a cabo sus actividades de acuerdo con el marco legal y regulatorio vigente. Se compromete a cumplir con todas las leyes y regulaciones pertinentes relacionadas con la seguridad de la información, incluyendo, pero no limitándose a las indicadas en el documento **SGSI.RG.01.es**, en la hoja Marco Legal.

Smarting integra el ENS y la ISO 27001 en la política de seguridad de la organización para brindar una estructura más completa y robusta para abordar los aspectos específicos de la seguridad de la información, tanto a nivel nacional como internacional. Además, la adopción de estos estándares mejora la credibilidad de la empresa, demostrando su compromiso con las mejores prácticas de seguridad.

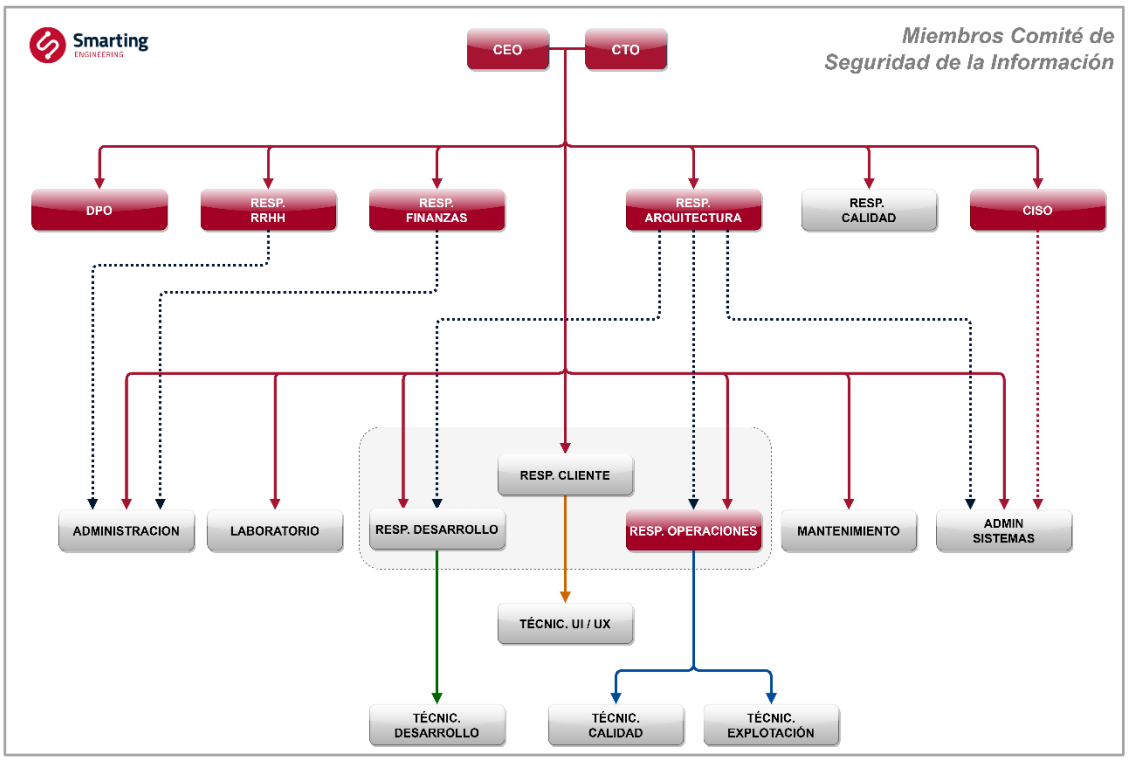
3. MARCO ORGANIZATIVO DE LA SEGURIDAD

La presente política de seguridad ha establecido de acuerdo con los principios básicos señalados en el capítulo II del Real Decreto 311/2022 y se ha desarrollado aplicando los siguientes requisitos mínimos:

Smarting ha identificado y definido los roles y funciones de seguridad necesarios para garantizar la protección de la información. Cada rol tiene responsabilidades claramente definidas (**SGSI.RG.04.es - Personas**).

Smarting ha nombrado un Comité de Seguridad (**SGSI.DC.00.es – Acta designación Comité**) que supervisará el seguimiento y cumplimiento del SGSI. El Comité de Seguridad está formado por cargos corporativos y de responsabilidad dentro de la organización La relación de los miembros constituyentes del Comité de Seguridad queda definido en el registro creado al efecto (**SGSI.RG.04.es - Personas**). Dicho comité de Seguridad TIC tendrá las siguientes funciones y responsabilidades:

- Coordinar todas las actividades relacionadas con la seguridad de las TIC.
- Es responsable de la redacción de la Política de Seguridad.
- Es responsable de la creación y aprobación de las normas que enmarcan el uso de los servicios TIC.
- Aprobará los procedimientos de actuación en lo relativo al uso de los servicios TIC.
- Aprobará los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.

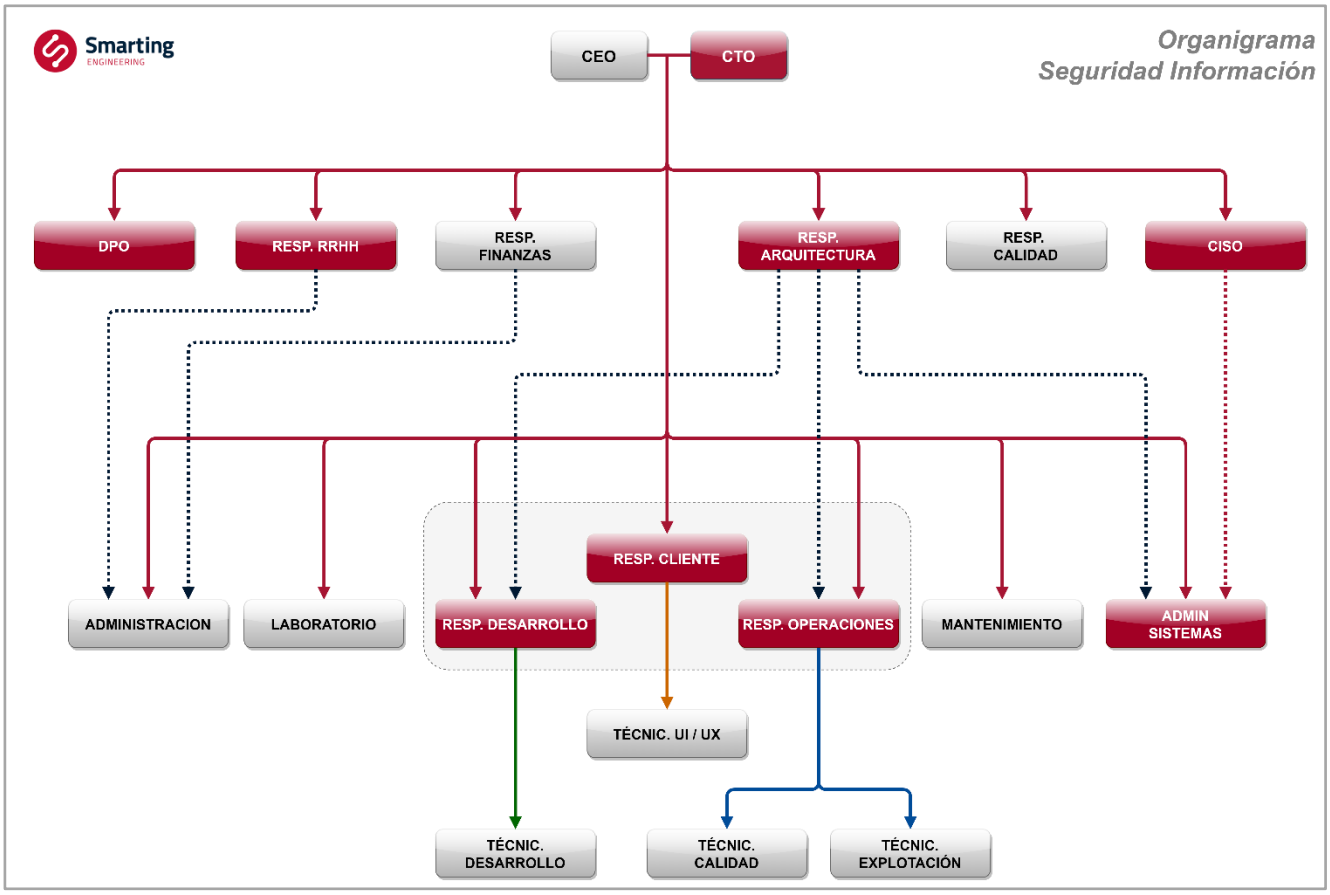


Asimismo, se han definido las funciones y responsabilidades del responsable de Seguridad, del responsable de la Información y del responsable de los Servicios, así como la relación de éstos con el Comité de Seguridad (SGSI.RG.04.es - Personas).

Con el fin de describir el proceso y jerarquía para resolver conflictos de autoridad que pueda ocurrir durante la gestión del ENS entre los perfiles críticos con responsabilidades en materia de seguridad, en Smarting **se ha definido las funciones para la resolución de conflictos ante responsables** y que aplica a todos los perfiles específicos de gestión del ENS (SGSI.RG.04.es - Personas).

El responsable de Seguridad de la Información (CISO), el responsable del Servicio (RE) y el responsable de Protección de Datos (DPO) serán nombrados por la Dirección a propuesta del Comité de Seguridad. Dichos nombramientos se revisarán cada 2 años o cuando el puesto quede vacante. El responsable de la Información (CIO) recae en Smarting en la figura del responsable Tecnológico (CTO)

En el siguiente organigrama se marcan los puestos con funciones o responsabilidades relacionadas con la seguridad de la información. La escalación en ausencia de alguno de estos responsables se realizará según las líneas jerárquicas marcadas en este diagrama.



4. ANÁLISIS Y GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política han sido evaluados mediante 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

5. CATEGORIZACIÓN DE LOS SISTEMAS

Smarting ha definido los criterios para determinar el nivel de seguridad requerido en cada sistema de información. Para ello se analizan los elementos esenciales, información y servicios, pivotando alrededor de ellos los criterios que el responsable de cada tipo de información y cada servicio podrá utilizar, considerando que la facultad de determinar la categoría del sistema corresponde al responsable de este.

El Esquema Nacional de Seguridad establece en su Anexo II medidas de seguridad condicionadas a la valoración del nivel de seguridad en cada dimensión y a la categoría de seguridad (artículo 40) del sistema de información respectivo. A su vez, la categoría de seguridad del sistema se calcula en función del nivel de seguridad más alto de las dimensiones valoradas.

La categorización de los sistemas de información en Básica, Media o Alta según los criterios del Esquema Nacional de Seguridad (ENS) implica evaluar varios factores que afectan la seguridad de la información. A continuación, se describe el proceso general para determinar la categorización de los sistemas de información de **Smarting**.

- **Identificación de los Sistemas de Información:**
  - Enumerar y clasificar todos los sistemas de información que maneja la organización.
- **Evaluación del Valor de la Información:**
  - Analizar la importancia y el valor de la información manejada por cada sistema.
  - Considerar la confidencialidad, integridad y disponibilidad de los datos.
  - Se consideran **datos personales sensibles**:
    - Datos relativos a la salud.
    - Datos genéticos y biométricos.
    - Datos relativos a la sexualidad u orientación sexual.
    - Datos personales que revelen el origen racial o étnico, las opiniones políticas y las convicciones religiosas o filosóficas.
    - Datos sobre la afiliación sindical.
  - Se clasifica la información por **su nivel de confidencialidad: SGSI.PR.06.es – 4.1.1. Niveles de clasificación**
  - Se clasifica la información por su **impacto: SGSI.PR.06.es – 4.1.2. Clasificación de la información**
- **Identificación de Activos Críticos:**
  - Identificar los activos críticos para el funcionamiento y la continuidad del negocio.
  - Determinar cómo la pérdida o compromiso de estos activos afectaría a la organización.
- **Análisis de Riesgos:**
  - Realizar una evaluación de riesgos para cada sistema.
  - Identificar amenazas, vulnerabilidades y posibles impactos en la seguridad de la información.
- **Cumplimiento Normativo:**
  - Evaluar el cumplimiento de los sistemas con los requisitos legales y normativos, incluyendo aquellos establecidos en el ENS.
- **Nivel de Exposición:**
  - Determinar el nivel de exposición a riesgos de seguridad para cada sistema.
  - Evaluar la probabilidad y gravedad de posibles incidentes de seguridad.
- **Dependencia de Otros Sistemas:**
  - Considerar la interconexión y dependencia entre diferentes sistemas de información.
  - Evaluar cómo la afectación de un sistema podría tener repercusiones en otros.
- **Requisitos de Confidencialidad, Integridad y Disponibilidad:**
  - Evaluar los requisitos específicos de confidencialidad, integridad y disponibilidad para cada sistema.
  - Comparar estos requisitos con los niveles establecidos en el ENS.

- **Evaluación de Capacidad de Recuperación:**
    - Evaluar la capacidad de recuperación de cada sistema ante posibles incidentes de seguridad.
    - Considerar la existencia de planes de continuidad del negocio y medidas de recuperación.
- **Definición de Categoría**:
    - Clasificar cada sistema en una de las categorías establecidas por el ENS **(Básica, Media, Alta)** según los resultados de la evaluación.
    - Cuando un cliente determine una categorización para los sistemas de información que Smarting le ofrece, **prevalecerá la categoría establecida por el Cliente**.
- **Documentación y Revisión Continua:**
    - Documentar la categorización de cada sistema de información.
    - Revisar periódicamente la categorización para asegurarse de que siga siendo adecuada y ajustarla según sea necesario.

6. GESTIÓN DEL PERSONAL Y PROFESIONALIDAD

Todos los miembros de Smarting 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 aplicar las medidas necesarias para que la información llegue a los afectados.

Todos los empleados recibirán una sesión de concienciación en materia de seguridad al menos una vez al año. Asimismo, se establecerá un programa de concienciación continua para sensibilizar a todos los miembros de Smarting, en particular a los de nueva incorporación, el cual se encuentra alineado con otros estándares implementados.

El personal que esté dedicado a las tareas de seguridad está cualificado de manera apropiada, dada la sensibilidad y complejidad de algunas de esas tareas. Esto es aplicable a todas las fases del ciclo de vida del proceso de seguridad (instalación, mantenimiento, gestión de incidencias y desmantelamiento). Para ello el personal recibe la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios sujetos al ENS.

Lógicamente, los mismos requisitos requeridos internamente deben exigirse a cualquier proveedor que preste servicios relacionados con seguridad. Para ello desde Smarting se ha impulsado un procedimiento para la evaluación de los proveedores de forma que se asegure el nivel de seguridad similar al requerido por la entidad.

7. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

El primer paso para asegurar que la información y los sistemas están protegidos es limitar el acceso a los mismos. Por ello, se ha definido quienes, y en qué medida tendrán acceso a los recursos, de manera que cada uno tenga el acceso necesario para realizar sus tareas, pero no a equipos o datos que no deben estar a su alcance.

Asimismo, los sistemas de información de Smarting cuentan con mecanismos de autorización para permitir el acceso y denegarlo y revocarlo cuando sea necesario.

8. PROTECCIÓN DE LAS INSTALACIONES

Las instalaciones se encuentran protegidas contra daños que puedan afectar a los sistemas que albergan y contra accesos de personas no autorizadas. El acceso a nuestras instalaciones está securizado y se encuentra regulado en el procedimiento habilitado a tal efecto (SGSI.PR.03.es - Procedimientos).

9. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD.

Smarting establece los requisitos del negocio y de seguridad de la información para sus sistemas de información, ya sean nuevos o bien existentes y que se amplíen o mejoren.

Así, toda nueva adquisición de producto y servicios de seguridad que pueda afectar al SGSI deberá evaluarse previamente, desde el punto de vista funcional y de requisitos de seguridad necesarios. Tras la validación, se procederá con la prueba formal del producto indicando si cumple con los requisitos.

Todo servicio contratado deberá ser evaluado antes de su puesta en producción con el fin de asegurar que cumpla con los requisitos mínimos de seguridad definidos en la presente Política de Seguridad de la Información y la Normativa de Seguridad vigente.

10. MÍNIMO PRIVILEGIO

El Sistema de Seguridad de la Información implementado en **Smarting** sigue el Principio del Mínimo Privilegio según el cual se otorga a los usuarios del sistema los niveles (o permisos) de acceso mínimos necesarios para desempeñar sus funciones, con el objetivo de restringir el acceso a la información y recursos únicamente a lo que es estrictamente necesario para cumplir con una tarea específica.

Este principio de mínimo privilegio garantiza que cada parte (ya sea un proceso, un usuario o un programa) solo pueda acceder a lo que es esencial para su propósito legítimo, no otorgando privilegios innecesarios. No obstante, este principio no se limita solo al acceso de los usuarios humanos también se aplica a aplicaciones, sistemas o dispositivos conectados que requieren privilegios para realizar tareas necesarias.

Al limitar los privilegios se reduce la exposición a ciberataques y se evita la "acumulación de privilegios".

11. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Para garantizar la integridad de los sistemas de información siempre, cualquier cambio físico y lógico, se realiza solo tras su aprobación formal y mediante un procedimiento formal.

Para ello, se actualizan los sistemas de manera controlada y según el estado de seguridad requerido en cada momento. Los cambios en las especificaciones de los fabricantes, la aparición de nuevas vulnerabilidades, la emisión de actualizaciones y parches que afecten a los sistemas son analizados para tomar las medidas necesarias para que no se degraden los sistemas ni su nivel de seguridad, gestionando asimismo los riesgos que introducen los cambios que se realizarán.

12. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Una parte significativa del ciclo de vida de la información corresponde a su almacenamiento y a su transporte. La información debe estar protegida en todo momento. Para ello se han desarrollado procedimientos adecuados, que cubren tanto a la información en soporte electrónico como en papel, así como política para el manejo y el tratamiento de la información.

13. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS.

La prevención ante otros sistemas de información interconectados es un aspecto crucial para **Smarting**. Para ello se han establecido medidas para garantizar la seguridad cuando los sistemas de información se conectan entre sí, teniendo en cuenta, aspectos tales como la protección del perímetro, el control de accesos o el debido registro de actividad con el que poder detectar posibles anomalías o comportamientos inusuales en la interconexión.

Cualquier conexión hacía o desde servicios interconectados serán realizados siguiendo las directrices definidas en las guías CCN-STIC publicadas al efecto.

14. REGISTRO DE LA ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO.

La empresa realiza la supervisión de sus sistemas de información y procesamiento registrándolas como incidencias de seguridad, revisando el registro de operación y fallos de sus sistemas para identificar el problema. Así, las actividades de supervisión del uso de los sistemas de **Smarting** respetan los requisitos legales de privacidad y se utilizan para verificar la efectividad de los controles de seguridad implantados y el cumplimiento de la política de control de accesos.

Asimismo, los equipos corporativos, mediante el uso de antivirus de última generación (EDR) con gestión centralidad, cuentan con herramientas para la protección, detección, recuperación y eliminación de código malicioso.

15. INCIDENTES DE SEGURIDAD

Desde la dirección de **Smarting** se ha establecido un procedimiento de notificación formal por el cual todo el personal debe notificar incidencias relacionadas con la seguridad mediante el canal establecido (security@smarting.es) de forma inmediata y sin demoras. Ello permite garantizar una respuesta rápida y efectiva ante incidencias y debilidades en la seguridad.

16. CONTINUIDAD DE LA ACTIVIDAD

La empresa ha establecido un procedimiento para actuar contra interrupciones en la actividad empresarial y proteger los procesos críticos de los efectos de fallos importantes en los sistemas de información y asegurar su restablecimiento inmediato. Para ello, se ha implementado un plan de continuidad de negocio (**SGSI.RG.03.es | Valoración BIA**) para reducir el impacto sobre la infraestructura de **Smarting**, y consecuentemente sobre la empresa, y la recuperación de activos de información (ya sea por accidentes, fallo en equipamiento, actos deliberados, etc.) de forma tal que los procesos del departamento alcancen un nivel aceptable de continuidad mediante medidas de recuperación correctivas y preventivas.

17. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

La Dirección, por su parte, valora especialmente y establece como criterio principal para la estimación de sus riesgos, la valoración de la confidencialidad, integridad y disponibilidad de la información crítica de la empresa y de sus clientes, así como asegurar la trazabilidad y autenticidad de estos.

Así, se compromete a desarrollar, implantar, mantener y mejorar continuamente la presente **Política de Seguridad** y su **Sistema de Gestión** con el objetivo de la mejora continua en la forma en que prestan sus servicios y en que tratan la información.

18. DATOS DE CARÁCTER PERSONAL

Smarting trata datos de carácter personal. En este sentido, y en cumplimiento con la legislación vigente en materia de protección de datos, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **Smarting** ha aplicado medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

19. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD

La documentación de seguridad del sistema seguirá las directrices establecidas por **Smarting**. Se implementarán medidas para estructurar, gestionar y controlar el acceso a la documentación de seguridad, garantizando su integridad y confidencialidad. El acceso estará restringido a personal autorizado y se llevará a cabo de acuerdo con las políticas de acceso definidas.

Se ha creado un canal específico **ENS-ISO27001** en Microsoft Teams, dentro del equipo general de normas ISO creado para la gestión de Normas. Se asignarán los permisos necesarios a las personas que pueden tener acceso a esta documentación: Miembros del Comité de Seguridad de la Información, Representantes del Cliente y Consultores y Auditores de Seguridad de la Información.

La documentación se repartirá en carpetas distinguiendo entre ISO y ENS. La estructura de carpetas interna seguirá, cuando se considere oportuno para facilitar su clasificación, los apartados de las respectivas normas/reglamentaciones.

La documentación generada para el Sistema de Gestión de Seguridad de la Información de **Smarting** seguirá la estructura de identificación definida en **SGSI.RG.01.es - Sistema**. En dicho documento se lleva también el registro de documentación y el control de versiones.

20. DOCUMENTACIÓN Y COMUNICACIÓN

Esta Política de seguridad de la Información estará disponible como información documentada y se comunicará dentro de la organización. Además, se compartirá con las partes interesadas relevantes, como autoridades, operadores y usuarios de transporte público, según sea apropiado.

21. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada anualmente o antes si hay cambios significativos en el entorno operativo o tecnológico de **Smarting**. La alta dirección se compromete a mantener esta política alineada con los objetivos de la empresa y los requisitos de seguridad de la información aplicables.

22. FIRMA DE LA DIRECCIÓN

Mediante la aprobación de esta política, la Dirección de Smarting manifiesta su determinación y compromiso en alcanzar un nivel de seguridad adecuado a las necesidades del negocio que garantice la protección de los activos de forma homogénea.

Nota: Los documentos mencionados en la presente política son de actualización periódica y se encuentran disponibles para su consulta por las partes interesadas. Pueden solicitarse a security@smarting.es