POLÍTICA DE SEGURIDAD ENS

REGISTRO DE EDICIONES

Edición	Fecha	Descripción del cambio
1.0	31/01/24	Redacción inicial

Contenido

1 MISIÓN Y ALCANCE

La misión de Safe Troop es empoderar a las fuerzas del orden público con las herramientas y tecnologías más avanzadas, permitiéndoles anticipar, prevenir y resolver delitos de manera más efectiva y eficiente.

Nos dedicamos a proporcionar soluciones innovadoras que transformen la forma en que se abordan los problemas de seguridad pública, brindando a las fuerzas del orden las capacidades que necesitan para proteger a nuestras comunidades.

La Visión de Safetroop es construir un mundo más seguro utilizando la tecnología como nuestra principal herramienta.

Nuestra visión es un mundo donde las fuerzas del orden público tengan acceso a las soluciones tecnológicas más avanzadas, permitiéndoles combatir el crimen de manera más efectiva y eficiente, y creando un entorno más seguro para todos.

Para lograr nuestra misión y visión, nos enfocamos en:

Desarrollar soluciones tecnológicas innovadoras que respondan a las necesidades específicas de las fuerzas del orden público.

Colaborar estrechamente con las fuerzas del orden público para comprender sus desafíos y desarrollar soluciones que satisfagan sus necesidades.

Ofrecer un servicio al cliente excepcional y brindar soporte continuo a las fuerzas del orden público.

En Safe Troop, creemos que la tecnología puede ser una herramienta poderosa para combatir el crimen y construir un mundo más seguro.

Las actividades de SAFETROOP se relacionan con organismos de la Administración Pública, por lo que se ha optado por la implantación de las medidas establecidas en el Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad). En concreto, el ENS se aplica a:

“Los sistemas de información que dan soporte a las actividades de:

- Aplicación SaaS para la movilización y comunicación de eventos a efectivos policiales y cuerpos de seguridad en general

de acuerdo al documento de determinación de la categoría vigente”.

2 MARCO NORMATIVO

2.1 Identificación

La sistemática utilizada por SAFETROOP para la identificación, análisis y cumplimiento de la legislación y normativa vigentes se recoge en el procedimiento general de Identificación de requisitos legales, que se mantiene debidamente actualizado.

2.2 Datos de carácter personal

En el ámbito de los datos de carácter personal, SAFETROOP ha realizado la adecuación a la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales". Dentro de esta adecuación se han desarrollado las nuevas cláusulas del deber de información, nuevos contratos de ETD, RAT, análisis de riesgos, análisis de necesidad de EIPD, etc.

La información documentada relativa al RGPD se integra dentro la documentación del Sistema de Gestión de la Calidad, Medioambiente y Seguridad

2.3 Esquema Nacional de Seguridad

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3 PRINCIPIOS Y DIRECTRICES

Los principios que deben contemplarse a la hora de garantizar la seguridad de la información son los marcados en el artículo 5 del RD 311/2022, por el que se regula el Esquema Nacional de Seguridad, de manera que las amenazas existentes no se materialicen o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

3.1 Prevención

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

Para garantizar el cumplimiento de la política, los departamentos (o servicios externos contratados) 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.

3.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS.

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

3.3 Respuesta

Se deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.

3.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, se deben desarrollar planes de continuidad de los sistemas TIC y actividades de recuperación.

3.5 Otros principios generales

- El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.
- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de la Organización deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.
- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018 de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales.

4 ORGANIZACIÓN DE LA SEGURIDAD

4.1 Roles y responsabilidades

La estructura organizativa, roles y responsabilidades del SAFETROOP están definidos en los documentos Manual de Seguridad y Procedimiento de Gestión de personal y correspondientes Fichas de puesto de trabajo.

En el marco del ENS, la gestión de la seguridad de la información implica la existencia de una estructura organizativa que defina unas responsabilidades diferenciadas en relación a los requisitos de información, requisitos del servicio y requisitos de seguridad (art. 11).

Se definen los siguientes roles relativos al ENS de acuerdo con lo desarrollado en el documento Roles de la BD de gestión del sistema SGSI:

a) Responsable de la Información
b) Responsable del Servicio
c) Responsable del Sistema de Gestión de la Seguridad de la información
d) Responsable de Seguridad
e) POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado
f) Responsable de Seguridad protección datos personales
g) Responsable de TI

La relación de personas que desempeñan estas funciones viene recogida en el registro Asignación de Roles en la BD de gestión.

La coordinación se lleva a cabo en el seno del Comité de Dirección. Podrá delegar en el Comité de Seguridad.

Tanto los nombramientos como la posible resolución de conflictos correrán a cargo de la Dirección de la organización.

5 FORMACIÓN Y CONCIENCIACIÓN

Las acciones específicas de concienciación y formación relativas al ENS se gestionan por el Departamento de RRHH.

La sistemática seguida por SAFETROOP para la detección de necesidades de formación y concienciación y para darles curso se describe en el procedimiento P Procedimiento de Gestión de personal.

6 GESTIÓN DE RIESGOS

Una correcta identificación y gestión de los riesgos a los que se encuentran sometidos los activos de información, que sustentan los servicios de cara al ciudadano de SAFETROOP, es primordial para la correcta toma de decisiones de la Dirección de SAFETROOP. Esto ha motivado a basar la Metodología de Análisis y Gestión de Riesgos del ENS en MAGERIT versión 3.

Para la implementación de la metodología de Análisis y Gestión de Riesgos se ha utilizado el modelo de Magerit sobre la BD relacional Airtable como se establece en el procedimiento interno P.11 Identificación de riesgos para la seguridad de la info.

7 DESARROLLO DE LA POLÍTICA

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de Seguridad de la Información.
- Segundo nivel: Normativas y Procedimientos de Seguridad.
- Tercer nivel: Procedimientos Técnicos de Seguridad.
- Cuarto nivel: Informes, registros y evidencias electrónicas.

7.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Organización, recogido en el presente documento y aprobado mediante Decreto de la Organización.

7.2 Segundo Nivel: Normativas y Procedimientos de Seguridad

De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente, desarrollados por SAFETROOP en el marco del ENS para cumplir con los requisitos mínimos de seguridad que marca su artículo 11.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión de la Dirección.

7.3 Tercer Nivel: Procedimientos Técnicos de Seguridad

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

7.4 Cuarto Nivel: Informes, registros y evidencias electrónicas

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

7.5 Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500, 600 y 800.

8 DOCUMENTACIÓN

La información documentada asociada al ENS se organiza, codifica y aprueba y se recogen en el procedimiento general de información documentada y registro en la BD del SGSI.

Toda la información documentada relativa al ENS se aloja en los servidores de Google Cloud.

Respecto a la calificación de la información, se documenta en la tabla de la BD de gestión del sistema.

9 PROCESO DE APROBACIÓN Y REVISIÓN

Esta Política de Seguridad de la Información ENS será aprobada por la Dirección y revisada de forma periódica o cuando circunstancias técnicas u organizativas lo requieran para evitar que quede obsoleta.

Comité de seguridad de Safetroop Technologies, SL