SAMPOL

Versión 1.0

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO SAMPOL

Aprobada por Carmen Sampol Massanet el
1 de febrero de 2024.

01. APROBACIÓN Y ENTRADA EN VIGOR

Texto **aprobado el día 1 de febrero de 2024 por Carmen Sampol Massanet, CEO de SAMPOL.**

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

Este texto no anula ninguno anterior, ya que este se trata del primer documento de Política.

02. REVISIÓN

La política será revisada de forma anual por el Comité de Seguridad TIC, a no ser que sucedan cambios suficientes para poder cambiarla.

03. INTRODUCCIÓN

SAMPOL depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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, confidencialidad, trazabilidad o autenticidad 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 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 pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

Prevención

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

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Detección

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

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

Los departamentos deben:

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

Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

04. ALCANCE

Esta política se aplica a todos los sistemas TIC de SAMPOL, y a todos los miembros de la organización que trabajan en él, sin excepciones.

05. MISIÓN U OBJETIVOS DEL ORGANISMO

La misión de SAMPOL es clara: ser capaces de dar respuesta a las necesidades energéticas y tecnológicas de sus clientes, creando y diseñando soluciones ad hoc a través de sus unidades de negocio, para que la energía y la tecnología ofrezcan una vida mejor y un consumo energético más eficiente.

Su visión es ser líderes en la generación y distribución de energía y en las instalaciones e infraestructuras de telecomunicaciones; contribuyendo activamente al bienestar social, al desarrollo sostenible y a la generación de valor para sus grupos de interés.

06. MARCO NORMATIVO

En SAMPOL se dispone de un departamento y un equipo dedicado a la revisión periódica de la legislación cambia, tanto por si se modifica como si entran en vigor nuevas leyes que puedan ser de aplicación. Para más información contactar con **Yolanda Rodríguez García.**

Dentro del marco normativo que aplica a SAMPOL, podemos encontrar en materia de seguridad los siguientes:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016.

07. ORGANIZACIÓN DE SEGURIDAD

Comités: Funciones y responsabilidades

El **Comité de Seguridad TIC** estará formado por **Carmen Sampol Massanet,** CEO de la empresa.

El Comité de Seguridad TIC será el responsable de la aprobación de las normas y procedimientos sobre el uso de las TIC y la definición de los requisitos de formación del personal TIC.

El **Secretario del Comité de Seguridad TIC** será **Juan del Junco** y tendrá como funciones la redacción del documento de Política de Seguridad, velar por el cumplimiento de la normativa, estar al tanto de los cambios de la tecnología y realizar el análisis de riesgos.

El Secretario del Comité de Seguridad TIC reportará al Comité de Seguridad cualquier cambio o modificación que se realice.

Roles: Funciones y responsabilidades

De forma detallada, este punto está desarrollado en el documento DOC.ENS.01_Roles y Responsabilidades. Se incluyen los siguientes cargos:

- Responsable de la Información: **Rafael Aldana.**
- Responsable del Servicio: **Juan del Junco.**
- Responsable del Tratamiento (Protección de Datos): **SAMPOL.**
- Responsable de Seguridad: **Pedro Llorente Flores.**
- Delegado de Protección de Datos: Y**olanda Rodríguez García.**
- Responsable del Sistema: **Yolanda Rodríguez García.**
- Administrador de la Seguridad del Sistema: **Jose Manuel Valle Gómez.**

Procedimientos de designación

El Responsable de Seguridad de la Información será nombrado a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Comité de Seguridad TIC designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

Política de seguridad de la información

Será misión del Comité de Seguridad TIC 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 el Responsable de la Seguridad de la Información y difundida para que la conozcan todas las partes afectadas.

08. DATOS DE CARÁCTER PERSONAL

SAMPOL trata datos de carácter personal. El Documento de Seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de SAMPOL se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

09. CONCIENCIACIÓN Y FORMACIÓN

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de SAMPOL y a todas las actividades, de acuerdo con el principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

10. POSTURA PARA LA GESTIÓN DE RIESGOS

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los 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. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones de SAMPOL.

La normativa de seguridad estará disponible en la carpeta Ciberseguridad dentro de Recursos Públicos de Egnyte.

12. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de SAMPOL atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de SAMPOL, 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.

13. TERCERAS PARTES

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

Cuando SAMPOL utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

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

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

SAMPOL

Camí del Reis, 308. 1ª Planta. Edificio Mapfre
07011 Palma de Mallorca. Islas Baleares
+34 971 76 44 76
www.sampol.com