Política de Seguridad de la Información

0. Aprobación y entrada en vigor

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

1. Introducción

SIPTIZE 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 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 de forma rápida y eficiente frente 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 y en la solicitud de ofertas.
Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

1.1 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.

1.2 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.

1.3 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).

1.4 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.

2. Alcance

Esta política se aplica a todos los sistemas TIC de y a todos los miembros de la organización, sin excepciones.

3. Misión

SIPTIZE es una empresa especializada en la provisión de Servicios Gestionados para el despliegue de soluciones de voz para empresas y operadores de comunicaciones. Además de ser Operador de telecomunicaciones.
Los servicios prestados consiguen obtener una mejora en el rendimiento de la infraestructura, mejorar la productividad del personal técnico y reducir significativamente el coste de las inversiones. Es decir, se busca maximizar el tiempo útil y la seguridad de los sistemas de información, sin tener que realizar inversiones en equipamiento, software o formación de recursos humanos.

4. Marco normativo

Siptize se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- RD-Ley 13/2012 de 30 de marzo, ley de cookies.
- 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.
- Ley 9/2014 de 9 de mayo, General de Telecomunicaciones.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS).

5. Organización de la seguridad

5.1 Comité: funciones y responsabilidades

El Comité de Gestión de la Seguridad de la Información estará formado por los responsables de servicios e información, responsable de seguridad y responsable del sistema, además de otros responsables o usuarios que se considere en cada caso.

5.2 Roles: funciones y responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en la matriz de roles y responsabilidades de SIPTIZE.

a) Responsable de la Información

El Responsable de la Información (information owner) de SIPTIZE es la dirección de la organización. Este cargo tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
El ENS asigna al “Responsable de la Información” la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de

determinar los niveles de seguridad de la información (aunque en este caso, esta responsabilidad recaerá sobre el Responsable de la Información de los organismos públicos a los que se les presta el servicio).

b) Responsable del Servicio

Por igual, el Responsable del Servicio de SIPTIZE es la propia dirección de la organización. El ENS asigna al “Responsable del Servicio” la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

c) Responsable de la Seguridad

El Responsable de Seguridad ha sido designado directamente por la Dirección para gestionar y mantener el SGSI.
Entre sus responsabilidades se encuentra la de mantener el proceso de mejora continua del sistema, trabajando junto con los responsables de los procesos y de los servicios.
Asimismo, es responsable de verificar el cumplimiento del Manual de Gestión, detectar las desviaciones que se produzcan en el Sistema, recomendar y canalizar mejoras y comprobar y evaluar la puesta en marcha y eficacia de las mismas. Con respecto a las actividades de gestión, planificará las auditorías internas y llevará la gestión de los incidentes relativos a los servicios que gestiona.
Dispondrá principalmente de las siguientes responsabilidades:

- Mantener y supervisar la gestión de la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

d) Responsable del Sistema

El Responsable del Sistema ha sido designado directamente por la Dirección para gestionar y mantener el ENS.
Cabe destacar, que el Responsable del Sistema se encargará entre sus funciones de:

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

El Responsable del Sistema podrá acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión será acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

5.3 Procedimientos de designación

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

5.4 Política de seguridad de la información

Será misión del Comité de Gestión de la Seguridad de la Información 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 mismo comité y difundida para que la conozcan todas las partes afectadas.

6. Gestión de riesgos

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 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 Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

7. Gestión documental

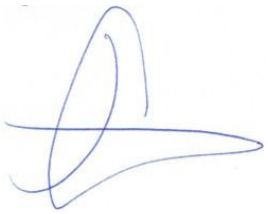
Esta Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, buenas prácticas, etc.).
Las directrices para la estructuración de la documentación del sistema de seguridad de la información, su gestión y acceso se encuentran documentadas siguiendo lo exigido por la ficha de proceso “FP-01 Gestión de la información documentada”.

8. Concienciación, formación y obligaciones del personal

Todos los miembros de SIPTIZE tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Gestión de la Seguridad de la Información disponer de los medios necesarios para que la información llegue a los afectados.
Todos los miembros de SIPTIZE asistirán a sesiones de concienciación de manera periódica en materia de seguridad de la información. Se establecerá un programa de concienciación

continua para atender a todos los miembros de SIPTIZE, 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.

El gerente de SIPTIZE



En Elche a 29 de junio de 2021