POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 2 de diciembre de 2.019 por la Comisión de Seguridad de la Información.

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

Este texto deriva de la anterior, que fue aprobado el día 12 de Noviembre de 2.017 por la Alta Dirección.

2. INTRODUCCIÓN

Socassat Instalaciones y Servicios S.L.. 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 con rapidez 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 y la norma ISO 27001 de Sistemas de Seguridad de la Información, 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 de la información 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. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. 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, y todos los requisitos necesarios para dar cumplimiento a la norma ISO 27001. 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.

2.2. 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.

2.3. 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 que se especifican en el Plan de Continuidad de Negocio.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización se dotará de un plan general de continuidad de negocio, valorando los posibles escenarios de desastre y estrategias de recuperación, y estableciendo planes de emergencia que se revisan periódicamente.

3. ALCANCE

Esta política se aplica a todos los sistemas de información de Socassat Instalaciones y Servicios S.L. tanto en su vertiente tecnológica como de organización, y a todos los miembros de la organización, sin excepciones.

4. MISIÓN Y OBJETIVOS MARCO

Se han establecido los siguientes objetivos marco:

- Establecer un compromiso de mejora continua del SGSI.
- Asegurar el cumplimiento de los requisitos legales, regulaciones, licencias, contratos y los acuerdos pactados con los clientes.
- Mejorar continuamente el funcionamiento operativo interno tanto desde el estudio de nuestro contexto como los requisitos de nuestras partes interesadas y los resultados de nuestro sistema de gestión, como proactivamente a través de evaluar riesgos y oportunidades que nos impulsen acciones de mejora.
- Someter nuestros activos de información a análisis de riesgos continuamente.
- Garantizar que la información tratada sólo será utilizada para los propósitos originales y bajo la supervisión de la empresa, asignando un propietario para cada sistema de información.
- Concienciando y formando al personal sobre la importancia de la seguridad de la información.

5. MARCO NORMATIVO

- 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 y por el que se deroga la directiva 95/46/CE (Reglamento general de protección de datos).
- Guía CCN-STIC 809 Declaración y Certificación de Conformidad con el ENS.
- Guía CCN-STIC 815 Indicadores y métricas en el ENS.
- Guía CCN-STIC 824 Informe del Estado de Seguridad.
- Guía CCN-STIC 844 Manual de Usuario de INES.
- Y además, voluntariamente se supeditan los sistemas a la ISO 27001.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información estará formado por el responsable de seguridad, la responsable de calidad y medioambiente y el gerente.

- Dirección, que integra las siguientes funciones:
  - Responsable en materia de protección de datos.
  - Responsable de información.
  - Responsable del servicio.
- Jefe de Informática y seguridad, reportando a dirección, asume la función de:
  - Responsable y administrador de seguridad.
- Jefes de área, reportando a dirección, que asume la función de:
  - Responsable del sistema.

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección y de los diferentes departamentos.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos para la Administración Pública desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas de información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Constituirse como Comité de Crisis, con el fin de coordinar la aplicación del Plan de Continuidad, cuando sea necesario.
- Realizar una revisión del estado de seguridad de la empresa y de los posibles incidentes, a partir del informe anual de Revisión por Dirección, remitido por el responsable de Seguridad.
- Aprobar el resultado del análisis de riesgos, y establecer el riesgo residual aceptable, así como los planes de tratamiento de los riesgos importantes o intolerables.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Dirección:

- La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.
- Los miembros de la Dirección deben dar buen ejemplo en el cumplimiento de las normas de seguridad establecidas.
- Aprobar la normativa de seguridad.
- Aprobar los procedimientos operativos de seguridad.
- Aprobar los planes de continuidad.

El Responsable de Seguridad es designado por Dirección, y sus funciones y responsabilidades son:

- Mantener la seguridad de la información manejada y el 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 Información.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Realizar las funciones de Secretario del Comité de Seguridad de la Información.
- Determinación de la categoría del sistema.
- Realizar los análisis de riesgos y proponer los planes de tratamiento.
- Realizar la declaración de aplicabilidad.
- Considerar medidas de seguridad adicionales.
- Elaborar y mantener la documentación de seguridad del sistema.
- Elaborar la normativa de seguridad.
- Proponer los procedimientos operativos de seguridad.
- Reportar el estado de seguridad del sistema.
- Elaborar los planes de mejora de la seguridad.
- Elaborar los planes de concienciación y formación.
- Proponer los planes de continuidad.
- Aprobar el ciclo de vida de los desarrollos de software: especificación, arquitectura, desarrollo, operación y cambios.

Jefes de área. Sus funciones y responsabilidades son:

- Operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Colaborar en la definición de 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 puede 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 debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutadas.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por Dirección a propuesta del Comité de Seguridad de la Información.

Dirección designará a los Responsables de Sistema y a los Administradores de Seguridad, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

Estos nombramientos se revisarán cada año o cuando alguno de los puestos quede vacante.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de 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 la Dirección de la empresa y difundida para que la conozcan todas las partes afectadas, y puesta a disposición a través de la web de la empresa.

7. DATOS DE CARÁCTER PERSONAL

Socassat Instalaciones y Servicios S.L.. trata datos de carácter personal. El documento de seguridad adaptado al Reglamento General de Protección de Datos, al que tendrán acceso sólo las personas autorizadas, recoge los procesos afectados y los responsables correspondientes. Todos los sistemas de información de Socassat Instalaciones y Servicios S.L. se ajustarán a los requisitos de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal tratados.

8. 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 Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de 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.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad en diferentes materias que se están elaborando durante este año 2019 y 2020.

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.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de Socassat Instalaciones y Servicios, S.L. 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 de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Socassat Instalaciones y Sercicios, S.L. atenderán a una sesión de concienciación 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 Socassat Instalaciones y Sercicios, S.L., en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas de la información 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.

11. TERCERAS PARTES

Cuando Socassat Instalaciones y Sercicios S.L. 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 y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Socassat Instalaciones y Servicios S.L. 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.

Santa Cruz de Tenerife, 2 de diciembre 2019

La Dirección