POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

POL-01

Contenido

INTRODUCCIÓN

Excem Grupo 1971, S.A. (en adelante "Excem Technologies") depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio. 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 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 con el 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.

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).

ALCANCE

Esta política se aplica a todos los sistemas TIC de Excem Technologies, así como a todos los miembros de la organización, sin excepciones.

MISIÓN

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, Excem Technologies, está altamente comprometido con mantener la Promoción de proyectos de investigación, desarrollo tecnológico e innovación, en un entorno de calidad, donde el desarrollo de buenas prácticas en Seguridad de la Información es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada. En consecuencia, a lo anterior, Excem Technologies, define los siguientes principios

de aplicación a tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información (SGSI):

La Dirección de Excem Technologies, entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de los servicios de la organización, y, por tanto, soporta los siguientes objetivos y principios:

I. Implementar el valor de la Seguridad de la Información en el conjunto de la Organización.
II. Contribuir, todas y cada una de las personas de Excem Technologies, a la protección de la Seguridad de la Información.
III. Preservar la confidencialidad, integridad, disponibilidad y resiliencia de la información, con el objetivo de garantizar que se cumplan los requisitos legales, normativos, y de nuestros clientes, relativos a la seguridad de la información; y de forma específica en lo que respecta a datos de carácter personal:
    a. Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado (Licitud, lealtad y transparencia).
    b. Serán, recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (Limitación de la finalidad)
    c. Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (Minimización de datos).
    d. Los datos deberán ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (Exactitud).
    e. Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (Limitación del plazo de conservación)
    f. Tratados de manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (Integridad y confidencialidad).
IV. Proteger los activos de la información de Excem Technologies de amenazas, ya sean internas o externas, deliberadas o accidentales, con el objetivo de garantizar la

continuidad del servicio ofrecido a nuestros clientes y la seguridad de la información.

V. Establecer un plan de seguridad de la información que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por Excem Technologies.

VI. Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.

VII. Asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información como medio para garantizar el cumplimiento de esta política.

VIII. Extender nuestro compromiso con la seguridad de la información a nuestro personal trabajador y proveedores.

IX. Mejorar continuamente la seguridad mediante el establecimiento y seguimiento periódico de objetivos de seguridad de la información.

Esta Política será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

De igual forma, para gestionar los riesgos que afronta Excem Technologies se establece un procedimiento de evaluación de riesgos formalmente definido. Por su parte, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección de Excem Technologies.

PRINCIPIOS BÁSICOS

- La seguridad como un proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.

REQUISITOS MÍNIMOS

La organización se compromete con esta política de seguridad a cumplir y velar por el cumplimiento de los siguientes puntos tal y como lo marca el RD 311/2022:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

MARCO NORMATIVO

La gerencia de Excem Technologies se asegura de que la documentación de origen externo necesaria para el funcionamiento de la empresa es conocida por los empleados de la empresa que lo necesitan y es mantenida actualizada y disponible en todo momento.

Para ello se utilizan los medios definidos en este documento y los procedimientos que lo desarrollan.

Documentos de referencia

- Esquema Nacional de Seguridad
- Guía CCN-STIC-801
- Normativa aplicable a Excem Technologies

ORGANIZACIÓN DE LA SEGURIDAD

Comités, funciones y responsabilidades

Se ha establecido un comité de seguridad formado por:

- Dirección
- Responsable de seguridad
- Responsable de los sistemas
- Responsable de protección de datos
- Responsable de la información
- Responsable del servicio

Este comité de seguridad tiene las siguientes funciones y responsabilidades:

- Atender las inquietudes de la dirección y de sistemas.
- Obtener una fotografía del estado de la seguridad de la información.
- Promover la mejora continua del SGSI.
- Elaborar la estrategia de evolución
- Revisar la Política, Normativa y procedimientos al menos anualmente
- Aprobar los requisitos de formación
- Priorizar actuaciones
- Promover la realización de auditorías del SGSI y técnicas.
- Comprobar que la Seguridad de la Información está presente en todos los proyectos

ROLES: FUNCIONES Y RESPONSABILIDADES

Dirección ejecutiva

Participa en la elaboración de objetivos y mediciones. Aprueba las políticas. Aprueba las revisiones por dirección del SGSI. Valida las conclusiones de las auditorías de sistemas.

La dirección ejecutiva establece el organigrama de la organización que contiene más funciones y roles de los que se especifican aquí. En esta política detallamos los responsables relacionados con la seguridad de la información.

Responsable de seguridad

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.

- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a la norma ENS, en colaboración con el responsable de Sistemas.
- Realizar con la colaboración del responsable del Sistema, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Coordinar el proceso de Gestión de la Seguridad, en colaboración con el responsable de Sistemas.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

Responsable del sistema

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el responsable de Seguridad.
- Realizar con la colaboración del responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
- La aplicación de los procedimientos operativos de seguridad.

- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los respectivos responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Responsable de protección de datos

- Informar y asesorar al responsable de la información y a sus empleados de las obligaciones que les incumben en relación con el RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

Responsable del servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad del servicio, de acuerdo con el responsable de Seguridad y el Responsable del Sistema.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

Responsable de la información

- Velar por el buen uso de la información y, por tanto, de su protección.

- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.

Usuarios y empleados

- Cumplir la política de seguridad de la información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de la empresa, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de las políticas, normas, procedimientos y medidas de seguridad aplicables

PROCEDIMIENTOS DE DESIGNACIÓN

La dirección de Excem Technologies se encarga de realizar unos nombramientos para designar roles y responsabilidades en seguridad de la información, así como se encarga de establecer los comités necesarios para velar por el cumplimiento de esta política. Estos nombramientos y estructuras internas permanecerán en documentos internos.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad 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 Comité de Seguridad y difundida para que la conozcan todas las partes afectadas

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 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.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD E LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afrontará aspectos específicos en la operativa de los usuarios de la organización. 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.

La política de seguridad estará disponible en https://excemtech.com/politica-de-seguridad-de-la-informacion/

OBLIGACIONES DEL PERSONAL

Todos los miembros de Excem Technologies 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 disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Excem Technologies 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 la organización, en particular a los de nueva incorporación.

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

TERCERAS PARTES

Cuando Excem Technologies 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 Excem Technologies 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.

APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 20 de noviembre del 2023 por Miguel Benito Martín, responsable de Seguridad de Excem Technologies.

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

Ante cualquier discrepancia con la anterior política o una solicitud de mejora se podrá realizar a través del buzón de correo habilitado para expresamente para ello.

Por otro lado, ante la situación de conflicto entre roles será gerencia la encargada de realizar la resolución de conflictos entre los causantes.