INDICE

Introducción

La información es en un activo principal para nuestra organización y por tanto tratamos la seguridad de la información como un elemento crítico y fundamental. Este reto se multiplica en exigencia e importancia si lo aplicamos a un entorno tan específico y crítico como el nuestro, donde el tratamiento y la gestión segura de la información se imponen como una necesidad para competir y mejorar en el futuro.

Asimismo, la legislación actual es clara en lo referente a la seguridad de la información, disponiendo de un marco legal muy concreto que requiere de un cumplimiento exigente por parte de todos, pero que ayuda a adoptar las medidas de seguridad apropiadas en los sistemas de la información.

El Objeto de este documento es establecer los principios y reglas básicas en las que se sostiene la Seguridad de la información de Exides S.L. Este conjunto de principios fundamentales ha sido formulado basándose en necesidades válidas de negocio, reconocimiento del valor añadido de los sistemas a proteger y una compresión de los riesgos asociados a estos sistemas. 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 destreza 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 (ENS) y la norma ISO27001 que Exides S.L toman como referencia, 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.

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 y la norma ISO27001, 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. La monitorización es especialmente relevante cuando se establecen líneas de defensa. 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.

Documentos de referencia

- ISO/IEC 27001.
- Esquema Nacional de Seguridad

Alcance

Esta política aplica a todo el Sistema de Gestión Integrado de Exides S.L, a todos los empleados y usuarios, incluso a terceras partes que traten información por encargo nuestro.

Afectará a los sistemas de información de la organización tanto a equipos personales o servidores, redes, aplicaciones, sistemas operativos, procesos de la empresa que pertenecen y/o son administrados por Exides S.L. Esta política cubre los aspectos más directamente relacionados con la responsabilidad y buen uso del personal de estos sistemas.

Roles: Funciones y Responsabilidades

Dirección:

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.

Dirección se encargará de realizar de responsable de la información y determinará los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS, los requisitos de clientes y los de la ISO27001, y otras normas que nos sean de aplicación como la normativa de Protección de Datos de Carácter Personal. la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.

Sera el responsable del servicio y determinará los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS, los requisitos de clientes y los de la ISO27001, y otras normas que nos sean de aplicación. La aprobación de los niveles de seguridad de los servicios constituye una actividad indelegable

Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control

Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios. Se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Por último, será el responsable de Protección de Datos :

- informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la normativa de Protección de Datos
- Supervisar el cumplimiento de lo dispuesto en la normativa de Protección de datos 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 la normativa
- Cooperar con la autoridad de control (Agencia Española de Protección de Datos);
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.
- El delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

La faceta de supervisión del DPD exige que sea una entidad diferente de la supervisada, de forma que si las funciones de tratamiento recaen en el responsable del Sistema, este no puede asumir las funciones de DPD

Responsable de la seguridad:

Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Es una persona física, jerárquicamente independiente del responsable del Sistema. El perfil deberá ser el de un profesional cualificado y con unos niveles idóneos de gestión y madurez en los servicios prestados interna o externamente.

Las 2 funciones esenciales serán:

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

Adicionalmente se encargará de:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de la Seguridad.

Las medidas de control establecidas en el cuerpo y anexos del ENS, en la ISO27001, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la Seguridad. Las medidas de seguridad referenciadas anteriormente podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos y los requisitos mínimos previstos en el ENS. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración en caso de prestación de servicios a la Administración Pública y de acuerdo con los pliegos de licitación que apliquen.

Los informes de autoevaluación y/o los informes de auditoría serán analizados por el responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas y a la dirección ejecutiva para que conozca las implicaciones esenciales.

Responsable del sistema:

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de la Seguridad.

Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.

Los informes de autoevaluación y/o los informes de auditoría serán analizados por el responsable de la Seguridad competente, que elevará las conclusiones al responsable del Sistema para que adopte las medidas correctoras adecuadas.

En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

Responsable del tratamiento

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. A todos los efectos en relación con los tratamientos de EXIDES S.L

Encargado del tratamiento

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del Tratamiento.

Técnicos:

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que trabajan con Sistemas de Información. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad serán sujetos a acciones disciplinarias según se contempla en este documento.

Procedimientos de designación

Los roles definidos en esta política serán designados por la dirección ejecutiva y constarán en acta de reunión formalmente aprobada y comunicada a las partes por las vías de comunicación de la entidad (correo electrónico, reunión, o aplicaciones de mensajería oficiales). El nombramiento se revisará cada 2 años o cuando el puesto quede vacante. La dirección decidirá asignar más de un rol a una misma persona cuando así se estime adecuado y cumpliendo los requisitos del ENS, para lo cual se tendrá en consideración El Departamento responsable de un servicio público que se preste electrónicamente de acuerdo a la Ley11/2007 designará al Responsable del Sistema en cada caso. precisando sus funciones y responsabilidades dentro del marco establecido por esta Política

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del responsable de seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la dirección ejecutiva y difundida para que la conozcan todas las partes afectadas.

Distribución de la Política

La distribución de la política de seguridad se distribuirá de las siguientes formas en función del grupo de interés al que se dirija:

- Personal y directivos de la organización: la distribución de la política de seguridad se realizará mediante correo electrónico o herramientas mensajería oficiales de la organización.
- Clientes, partners, proveedores y restantes grupos de interés: la política de seguridad se le incluirá como un apartado de nuestra página web donde podrá consultarse actualizada en todo momento.

Resumen de la Política de Seguridad de la información.

Exides S.L, está altamente comprometida 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, EXIDES S.L, define los siguientes principios de aplicación a tener en cuenta en el marco del Sistema de Gestión de Seguridad de la Información

La Dirección de Exides S.L 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:

- Implementar el valor de la Seguridad de la Información en el conjunto de la Organización.
- Contribuir, todas y cada una de las personas de Exides S.L, a la protección de la Seguridad de la Información.
- 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:
  - Los datos serán tratados de manera lícita, leal y transparente en relación con el interesado (Licitud, lealtad y transparencia).
  - Serán, recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (Limitación de la finalidad).
  - Los datos serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (Minimización de datos).
  - 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).
  - 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).
  - 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).

- Proteger los activos de la información de EXIDES S,L 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.
- 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 EXIDES S.L
- Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.
- 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.
- Extender nuestro compromiso con la seguridad de la información a nuestro personal trabajador y proveedores.
- 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 esta. 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 Exides S.L. 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 Exides S.L.

Violaciones y Sanciones

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a Exides S.L., será sancionada de acuerdo con los mecanismos habilitados en el convenio de Empresa y en la normativa legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de Exides S.L y que no estén previstas en esta política, deberán ser revisadas por el responsable de Seguridad de la Información para dictar una resolución sujetándose al criterio de la empresa y la legislación prevista.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad de la Información son atribución de la Dirección de Exides S.l y de los órganos de gobierno según la legislación aplicable.

Existe un protocolo de gestión de incidencias puesto a disposición de los trabajadores a través del cual cualquier miembro de la empresa puede comunicar una posible incidencia o incumplimiento al responsable de seguridad.

Aprobación y entrada el vigor

Esta Política de Seguridad de la información es efectiva desde la fecha de aprobación y hasta que fuere reemplazada por una nueva.

Aprobado por Francisco Manuel Valles Caña a fecha de 24/02/2023

Historial de modificaciones

Fecha	Versión	Modificado por	Descripción de la modificación
01/11/2011	1	Javier Legitec	Creación inicial
24/02/2023	2	Ana Buendía	Modificación nueva certificación ISO 27001