1. Aprobación y entrada en vigor

Texto aprobado el día 01 Abril de 2024 por el Comité de Seguridad de GRUPO DEPOROCIO.

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

2. Introducción

GRUPO DEPOROCIO 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 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.

Desde la Dirección de GRUPO DEPOROCIO, siguiendo con nuestro planteamiento de mejora continua, enfocamos nuestras líneas estratégicas de Seguridad de la Información en la triada CIA

(confidencialidad, integridad y disponibilidad). Nos comprometemos a evidenciar el desarrollo e implementación de un sistema de gestión de la seguridad en la información y ofrecer una mejora continua en nuestra actividad, para ello establecemos los siguientes principios:

- Llevar a cabo una formación y concienciación constante en el personal de la empresa en temas de Seguridad de la Información
- Cumplir con los requisitos de las normas ISO de Seguridad de la Información, de los requisitos establecidos con nuestros clientes relativos a seguridad de la información y de la reglamentación legislativa aplicable a nuestra actividad.
- Revisar periódicamente todos los datos obtenidos, el análisis de riesgos de seguridad de la información, para analizar y obtener conclusiones sobre nuestro funcionamiento y con ellos establecernos objetivos y metas de progreso.
- Cumplir y mejorar continuamente la eficacia del sistema de gestión de seguridad de la información.
- Promover la mentalización sobre esta política a todos los empleados para hacer frente común en nuestros objetivos.

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. 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

Dados 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 mecanismo de detección, análisis Gestión del Conocimiento y reporte que llegue 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 los mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de negocio y actividades de recuperación.

3. Alcance

Procesos de negocio y sistemas de información que dan soporte a los procesos de Desarrollo, Implantación, Mantenimiento, Soporte y Alojamiento de Aplicaciones Web y la innovación en Aplicaciones Web y Móviles, de acuerdo a la declaración de aplicabilidad en vigor

4. Misión

Nuestra MISIÓN es mejorar las organizaciones aplicando la innovación tecnológica y el conocimiento libre.

Nuestra VISIÓN es ser una empresa internacional, de referencia en el campo de la innovación tecnológica y en el desarrollo de soluciones de gestión de contenido empresarial.

5. Marco Normativo

Según la legislación vigente, las leyes aplicables a GRUPO DEPOROCIO en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Este real decreto es el que establece el marco normativo del ENS, y define sus principios básicos, requisitos mínimos y procedimientos de aplicación.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Establece las normas relativas a la protección de datos personales y garantiza los derechos digitales.
- Norma Básica de Protección de Infraestructuras Críticas: Esta norma tiene como objetivo establecer las medidas y requisitos necesarios para garantizar la protección de las infraestructuras críticas.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Establece las normas relativas a la protección de datos personales y garantiza los derechos digitales.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Real Decreto 611/2023, de 11 de julio, por el que se aprueba el Reglamento del Registro de la Propiedad Intelectual.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Reglamento eIDAS
- El RGPD entró en vigor el 25 de mayo de 2018 y sustituye a la Directiva 95/46/CE, que era la normativa anterior sobre protección de datos en la UE.
- 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: Establece las medidas de seguridad que deben aplicarse a la información manejada por los sistemas y servicios electrónicos utilizados por las entidades del sector público.
- Norma Básica de Protección de Infraestructuras Críticas: Esta norma tiene como objetivo establecer las medidas y requisitos necesarios para garantizar la protección de las infraestructuras críticas.
- Real Decreto 4/2010, de 8 de enero, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público: Contiene disposiciones relativas a la seguridad de la información en contratos del sector público.

Norma UNE-ISO/IEC 27001 sobre Sistemas de Gestión de Seguridad de la Información: Aunque no es específica del ámbito del ENS, es una norma internacional reconocida que establece los requisitos para establecer,

GRUPO DEPOROCIO cumple con la legislación citada y con todos sus requisitos y dispone de asesoría legal.

6. Organización de la seguridad

6.1. Comités: Funciones y responsabilidades

El Comité de Seguridad de la Información coordina la seguridad de la información en GRUPO

DEPOROCIO.. El Comité de Seguridad de la Información estará presidido la Dirección de GRUPO

DEPOROCIO. y Formado:

- Responsable de la Información: Dirección de GRUPO DEPOROCIO.
- Responsable de los Servicios: Dirección de GRUPO DEPOROCIO.
- Responsable de Seguridad: Dirección de GRUPO DEPOROCIO.
- Responsable del Sistema: Responsable del Departamento de informática

El Comité de Seguridad tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Comité de Seguridad de la Información de GRUPO DEPOROCIO
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de GRUPO DEPOROCIO 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 el Comité de Seguridad de la Información de GRUPO DEPOROCIO
- 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 GRUPO DEPOROCIO 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 GRUPO DEPOROCIO 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 TIC 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 TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Responsable de Seguridad tendrá como funciones:

- Convocar, según las indicaciones de la presidencia, las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Llevar a cabo la ejecución directa o delegada de las decisiones del Comité.

6.2. Roles: Funciones de los miembros del comité

Las funciones de los miembros del Comité de Seguridad de la Información serán las siguientes:

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

Responsable de los Servicios

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los correspondientes a interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

Responsable de Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información.

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.
- 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.

6.3. Procedimiento de designación

Los responsables serán nombrados por el Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando un puesto quede vacante.

6.4. Revisión de la 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 el Comité de Seguridad de la Información de GRUPO DEPOROCIO. y difundida para que la conozcan todas las partes afectadas.

7. Datos de caracter personal

GRUPO DEPOROCIO trata datos de carácter personal. En el registro de actividades del tratamiento describe los tratamientos de datos personales que llevan a cabo en el mismo para dar cumplimiento al artículo 30 del RGPD. Además, cada uno de esos tratamientos incluye un análisis de riesgos para detectar esos posibles riesgos y mitigarlos o eliminarlos inherentes al tratamiento de datos personales.

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.

9. Desarrollo de la política de seguridad de la información

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de GRUPO DEPOROCIO

Es objetivo de esta Institución es asegurar que:

- La información y los servicios estén protegidos contra pérdidas de disponibilidad, confidencialidad e integridad.
- La información esté protegida contra accesos no autorizados.
- Se cumplan los requisitos legales aplicables.
- Se cumplan los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.

- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establezcan procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información será el encargado de mantener esta Política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio será el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- GRUPO DEPOROCIO. implemente, mantenga y realice un seguimiento del cumplimiento de las normativas que aplican a este SGSI.

10. Obligaciones del personal

Todos los miembros de GRUPO DEPOROCIO.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 de los medios necesarios para que la información llegue a los afectados.

Todos los miembros de GRUPO DEPOROCIO atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de Gestión del Conocimiento y concienciación continua para atender a todos los miembros de GRUPO DEPOROCIO, 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.

11. Terceras Partes

Cuando GRUPO DEPOROCIO 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 GRUPO DEPOROCIO utilice los servicios de tercero o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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 esté 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.

12. Principios básicos

La presente política de seguridad establece los principios básicos especificados en el Real Decreto, y se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

La empresa establece una estructura organizativa que define claramente las responsabilidades en materia de seguridad de la información. Se asegura la implantación de políticas, procedimientos y controles alineados con los objetivos estratégicos. La Dirección supervisa y aprueba las actuaciones que garantizan la protección integral de la información.

b) Análisis y gestión de los riesgos.

Se realiza de forma periódica la identificación, valoración y tratamiento de los riesgos que puedan afectar a la confidencialidad, integridad y disponibilidad de la información. Los resultados del análisis sirven como base para establecer medidas preventivas y correctivas adecuadas. Este proceso se revisa y actualiza ante cualquier cambio relevante en la organización o su entorno tecnológico.

c) Gestión de personal.

Todo el personal recibe formación y sensibilización en materia de seguridad de la información antes y durante su relación laboral. Se establecen compromisos de confidencialidad y se asignan accesos en función de las funciones y responsabilidades. El cumplimiento de las normas de seguridad se supervisa de forma continua.

d) Profesionalidad.

La empresa garantiza que las funciones relacionadas con la seguridad sean desempeñadas por personal competente y cualificado. Se fomenta la actualización continua de conocimientos técnicos y normativos. Esta profesionalidad refuerza la confianza de los clientes y la eficacia de los controles implantados.

e) Autorización y control de los accesos.

El acceso a los sistemas y a la información se otorga únicamente a usuarios autorizados y de acuerdo con el principio de necesidad. Se aplican mecanismos de autenticación y control para prevenir accesos indebidos o usos no autorizados. Los privilegios se revisan periódicamente para asegurar su adecuación.

f) Protección de las instalaciones.

Las oficinas y equipos se encuentran protegidos mediante medidas físicas y ambientales que evitan accesos, daños o interferencias no autorizadas. Se controla el acceso de visitantes y proveedores, garantizando la seguridad de la información tanto en soporte físico como digital. Las instalaciones se supervisan para mantener su integridad.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

Los productos y servicios que afectan a la seguridad se seleccionan conforme a criterios de calidad, cumplimiento normativo y fiabilidad técnica. Los contratos incluyen cláusulas específicas de confidencialidad y protección de datos. Antes de su implantación, se verifica la compatibilidad con las políticas internas de seguridad.

h) Mínimo privilegio.

Cada usuario, proceso o sistema dispone únicamente de los permisos necesarios para el desempeño de sus funciones. Este principio reduce el riesgo de accesos indebidos y de manipulación de la información. Los privilegios se revisan periódicamente y se revocan cuando dejan de ser necesarios.

i) Integridad y actualización del sistema.

Se establecen procedimientos para garantizar la integridad de los sistemas y la correcta aplicación de actualizaciones y parches de seguridad. Los cambios se gestionan de forma controlada y documentada. Esto asegura la estabilidad operativa y la protección frente a vulnerabilidades conocidas.

j) Protección de la información almacenada y en tránsito.

La información se protege mediante el uso de mecanismos de cifrado, copias de seguridad y controles de acceso. Se garantiza su confidencialidad tanto en los sistemas internos como durante su transmisión. Se revisan periódicamente las medidas técnicas para asegurar su eficacia.

k) Prevención ante otros sistemas de información interconectados.

Se evalúan los riesgos derivados de las conexiones con sistemas externos, clientes o proveedores. Se establecen medidas de seguridad que limiten la exposición ante vulnerabilidades de terceros. Todo intercambio de información se realiza bajo protocolos seguros y controlados.

l) Registro de la actividad y detección de código dañino.

Se mantienen registros de las actividades relevantes de los sistemas con el fin de detectar comportamientos anómalos o incidentes. Los sistemas se protegen mediante herramientas de detección y eliminación de malware. La revisión periódica de los registros permite anticipar posibles amenazas.

m) Incidentes de seguridad.

Se dispone de un procedimiento formal para la detección, notificación y gestión de incidentes de seguridad. Se registran todas las incidencias, evaluando su impacto y aplicando medidas correctivas y preventivas. La experiencia obtenida se aprovecha para mejorar continuamente los controles existentes.

n) Continuidad de la actividad.

La organización cuenta con medidas que garantizan la continuidad operativa en caso de incidentes o desastres que afecten a los sistemas de información. Se mantienen copias de seguridad, procedimientos de recuperación y planes de contingencia. La eficacia de estos mecanismos se prueba y revisa regularmente.

ñ) Mejora continua del proceso de seguridad.

El sistema de gestión de la seguridad se revisa de forma periódica para identificar oportunidades de mejora. Se analizan los resultados de auditorías, incidentes y revisiones de la dirección. Este enfoque permite adaptar la política de seguridad a los nuevos riesgos y necesidades de la organización.

13. Estructuración, gestión y acceso a la documentación de seguridad.

La organización establecerá un marco homogéneo para la estructuración, identificación y mantenimiento de la documentación de seguridad del sistema de información, garantizando su coherencia, trazabilidad y actualización permanente.

Toda la documentación de seguridad (políticas, normas, procedimientos, guías, registros y evidencias) se organizará conforme a una estructura común definida por el Responsable de Seguridad, diferenciando claramente entre documentos estratégicos, normativos, operativos y registros.

La documentación será gestionada mediante mecanismos que aseguren el control de versiones, la integridad, la disponibilidad y la conservación histórica, de forma que pueda conocerse en todo momento su vigencia y estado.

El acceso a dicha documentación se realizará bajo el principio de necesidad de conocer, aplicando controles de acceso acordes al nivel de sensibilidad de cada documento. Solo el personal autorizado podrá consultar, modificar o aprobar la documentación, quedando registradas las acciones relevantes.

Asimismo, se garantizará que la documentación de seguridad esté disponible para los roles que la necesiten para el desempeño de sus funciones, y para los procesos de auditoría, supervisión y mejora continua del sistema, de acuerdo con lo establecido en el Esquema Nacional de Seguridad y en la normativa aplicable.

José María Aguilar