POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

APROBACIÓN Y ENTRADA EN VIGOR

El presente texto ha sido aprobado a fecha de firma por la Dirección de GEDSA y GESTORA ANDALUZA.
Esta Política de Seguridad de la Información es efectiva desde la fecha de su aprobación y hasta que la misma sea reemplazada por la aprobación de una nueva Política.

INTRODUCCIÓN

GEDSA y GESTORA ANDALUZA para alcanzar sus objetivos en el normal desarrollo de sus actividades, depende, en su gran mayoría, de los sistemas TIC (Tecnologías de información y Comunicaciones). Estos sistemas deben ser administrados con la debida diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar tanto a la disponibilidad, integridad o confidencialidad, así como autenticidad y trazabilidad de la información tratada o los servicios prestados.

El único fin de la seguridad de la información, y por tanto de la presente política, es garantizar la calidad de la información y la prestación continuada de los servicios, actuando de forma preventiva, supervisando las actividades diarias que se desarrollan en la organización y reaccionando con celeridad frente a los incidentes que puedan ocurrir.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial suficiente para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y de valor de la información y de los servicios. Es necesario que para defenderse o prevenir estas amenazas, se implemente una estrategia que se adapte a cualquier cambio, en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto significa que todos los departamentos deben de aplicar al menos las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) y a nivel de buenas prácticas las establecidas en la Norma ISO/IEC 27001, 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 de la organización deben asegurarse de que la seguridad TIC es una parte integral de cada una de las etapas del ciclo de vida del sistema. Asimismo, los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de los posibles incidentes en sus sistemas de información.

PREVENCIÓN, DETECCIÓN, REACCIÓN Y RECUPERACIÓN

GEDSA y GESTORA ANDALUZA pone a disposición los recursos para evitar que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos y áreas deben implementar, al menos, las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), a nivel de buenas prácticas las establecidas en la Norma ISO/IEC 27001 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 se 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.

Dado que, debido a incidentes, los servicios pueden verse rápidamente degradados, éstos deben de monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia; se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Para garantizar la disponibilidad de los servicios, 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.

ALCANCE

La presente política se aplica a todos los sistemas TIC de GEDSA y GESTORA ANDALUZA y a todas las personas de la organización, que dan soporte en la prestación de los servicios comprendidos dentro del documento de *Alcance del SGSI*.

VISIÓN Y MISIÓN

GEDSA y GESTORA ANDALUZA como empresas pertenecientes a un mismo grupo accionarial y que operan el mismo sector pretenden integrarse bajo una única razón social a corto / medio plazo y potenciar los servicios vinculados a nuevas soluciones tecnológicas (tales como consultoría e implantación de software ECM o BMP) frente a los tradicionales servicios de custodia y digitalización de documentos, así como extender su área de influencia convirtiéndose en una compañía de corte más tecnológico puntera en el ámbito nacional a nivel de facturación y número de clientes.

GEDSA y GESTORA ANDALUZA prestan sus servicios a instituciones públicas y clientes privados cuya intención es minimizar el impacto de la gestión documental sobre sus costes y/o optimizar el desempeño optimizando los procesos y flujos documentales.

GEDSA y GESTORA ANDALUZA están integradas por un equipo técnico multidisciplinar conformado por Ingenieros en Informática, Licenciados y Diplomados en Documentación, Técnicos en Documentación Sanitaria y expertos en Logística, capaces de comprender, interpretar y traducir a requerimientos técnicos las necesidades y expectativas de nuestros clientes.

GEDSA y GESTORA ANDALUZA tienen como misión es optimizar la gestión documental de sus clientes (públicos y privados) diseñando e implementando servicios y soluciones adecuadas a sus necesidades y expectativas.

MARCO NORMATIVO

Esta Política se desarrollará conforme al marco normativo y legal aplicable en materia de seguridad, según lo identificado en nuestro *registro de requisitos legales y otros requisitos*.

Normativa interna

La presente política se desarrolla mediante un conjunto de documentos que forman la normativa interna del sistema integrado de gestión listada en nuestro registro de *control de la documentación y de los registros.*

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.

ORGANIZACIÓN DE LA SEGURIDAD

Comité

Con el fin de facilitar la implantación y gestión del proceso de seguridad en GEDSA y GESTORA ANDALUZA, mediante la aprobación de la presente política, se aprueba también la formación de un Comité de Seguridad de la Información orientado a la gestión de la seguridad en la organización.

Este comité tiene la función de coordinar todas las funciones de seguridad de GEDSA y GESTORA ANDALUZA, vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial. Asimismo, este comité se encarga de velar por el alineamiento de las actividades de seguridad y los objetivos de la organización.

Roles y Responsabilidades

En el marco de cumplimiento del ENS y la ISO27001, y a fin de conformar la estructura de responsables en materia de seguridad, se han determinado los siguientes roles principales:

- Responsable de Organización, Calidad e Innovación, en representación de la alta dirección de la organización (máximo responsable de la seguridad de la información) y encargado de planificar, establecer y mantener las Políticas de Seguridad de la Información, estándares, directivas y procedimientos de la Organización, con el soporte y asesoramiento del CISO y del DPD.
- CISO (*Chief Information Security Officer*): responsable de marcar las pautas a seguir en esta materia, a la par que apoyar al Responsable de Organización en la coordinación de la gestión de las acciones a

realizar en materia de seguridad de la información y, concretamente, en el cumplimiento del Esquema Nacional de Seguridad y la ISO 27001.

- DPD (*Delegado de Protección de Datos*): revisión, supervisión y asesoramiento en el cumplimiento de la normativa aplicable en materia de protección de datos y privacidad, su documentación y justificación.
- Responsables de Servicio, representado por los responsables de cada de los departamentos de Digitalización y Operaciones.
- Responsable de IT, responsable de la infraestructura de sistemas y comunicaciones.
- Responsable de Operaciones, encargado de la seguridad física de las instalaciones, delegando lo que corresponda a sus homólogos en cada sede.
- La atención, revisión y auditoría de la seguridad de los sistemas será realizada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

Asimismo, GEDSA y GESTORA ANDALUZA dispone de mecanismos de coordinación y resolución de conflictos recayendo en la Dirección la responsabilidad de su gestión y toma de decisiones.

Procedimientos de designación

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección General de GEDSA y GESTORA ANDALUZA según la relación jerárquica de los perfiles afectados.

GESTIÓN DE RIESGOS

El procedimiento de Auditorías Internas asegura el alineamiento de las Tecnologías de la Información con las Políticas, Procedimientos y Legislación Aplicable.

Todos los sistemas sujetos a la presente 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 exista un cambio significativo en los sistemas de información
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, los responsables de la Información y Servicios establecerán 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.

OBLIGACIONES DEL PERSONAL

Todas las personas de la entidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, así como desempeñar sus competencias con profesionalidad y ética.

Es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados. Se establecerá un plan de formación y concienciación continua, en materia de seguridad de la información para atender a todas las personas de GEDSA y GESTORA ANDALUZA según su grado de responsabilidad.

TERCERAS PARTES

En el momento en el que GEDSA y GESTORA ANDALUZA preste servicios o maneje información de terceros, se les hará participes de esta Política de Seguridad de la Información en la medida que se requiera, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad Corporativos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la entidad utilice servicios de terceros o ceda información a terceros, transmitirá también los requisitos de esta Política de Seguridad.

La organización únicamente cederá información a terceros que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos establecidos en su Política de Seguridad de la Información.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Asimismo, 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.

Se adoptarán las medidas oportunas en caso de incumplimiento de estos requerimientos, por parte de un tercero.

Aprobado en Picassent (Valencia)

35981382K FRANCISCO JAVIER ARMENTER (R: A97185854)

Firmado digitalmente por 35981382K FRANCISCO JAVIER ARMENTER (R: A97185854)
Fecha: 2022.11.14 09:25:51 +01'00'

Fdo.: D. Francisco Javier Armenter Vidal