PSI-*01* | Política de Seguridad de la Información

DOCUMENTO PÚBLICO

INDICE DEL DOCUMENTO

1 ENTRADA EN VIGOR

Esta **Política de Seguridad de la Información** entrará en vigor al día siguiente de su aprobación por la Gerencia de la SOGEPIMA, S.A. Con fecha del 2 de noviembre de 2023.

2 INTRODUCCIÓN

SOGEPIMA, con su Gerencia a la cabeza, reconoce expresamente la importancia de la información y de los sistemas de información, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta poder llegar a poner en peligro la continuidad de la entidad, o al menos suponer daños muy importantes si se produjera una pérdida irreversible de determinados datos, incluida la privacidad de las personas. Además, por estar así establecido en la legislación española en lo que atañe a los datos de carácter personal y en defensa de los intereses de la empresa, empleados, clientes y otros posibles afectados.

Consciente de todo ello, SOGEPIMA implementa un modelo de gestión de seguridad de la información como herramienta para estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, para garantizar la calidad y seguridad de la información (confidencialidad, integridad, disponibilidad y usos previstos), así como el cumplimiento legislativo vigente. Supervisando la actividad diaria y reaccionando con prontitud ante estos incidentes comentados.

Esta política será revisada con regularidad como parte del proceso de revisión por la Gerencia, o cuando se identifiquen cambios significativos en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

Esta política de seguridad debe de estar disponible como información documentada, comunicada a y conocida por todo el personal de la empresa y partes interesadas, según sea apropiado.

Para la implantación del modelo de gestión de seguridad de la información se ha decidido tomar como referencia el estándar de gestión las normas ISO/IEC 27000 creadas para facilitar dicha implantación, aplicable a cualquier tipo de organización y que contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el comentado modelo de gestión y también teniendo en cuenta las normas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante ENS).

Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos reflejados en el artículo 5 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica:

- 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.
- Seguridad por defecto.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

La utilización de este modelo nos puede permitir, la certificación de nuestro sistema de gestión de seguridad de la información implantado. Según lo reflejado en ENS I Categoría del Sistemas, el sistema se ha categorizado con nivel MEDIO, esto implica directamente que haya que certificar el sistema ante una empresa certificadora acreditada por el ENS.

3 PRINCIPIOS Y DIRECTRICES

Los principios y directrices que se contemplan desde SOGEPIMA a la hora de garantizar la seguridad de la información son la prevención, la detección, la respuesta y la recuperación, de manera que las amenazas existentes no se materialicen, o en caso de materializarse no afecten gravemente a la información que maneja, o los servicios que se prestan.

3.1 PREVENCIÓN

SOGEPIMA con todos sus departamentos y áreas funcionales evita, o al menos en la medida de lo posible evita, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos tienen implementado las medidas mínimas de seguridad determinadas por este documento, 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 esta política, SOGEPIMA

- Autoriza los sistemas TI antes de entrar en operación.
- Evalúa y monitoriza regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.2 DETECCION

Dado que los servicios y los sistemas se pueden degradar rápidamente debido a incidentes, se monitoriza la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a las o los responsables regularmente y en el momento en que se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.3 RESPUESTA

SOGEPIMA debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar el punto de contacto para las comunicaciones con respecto a incidentes detectados en los departamentos o en otros organismos relacionados con SOGEPIMA.

3.3.1 RECUPERACION

Para garantizar la disponibilidad de los servicios críticos, SOGEPIMA debe desarrollar planes de continuidad de los sistemas TI como parte de su **plan general de continuidad de negocio y actividades de recuperación**.

4 MISION

SOGEPIMA, es una empresa pública municipal que, gestiona, explota y comercializa el patrimonio inmobiliario propiedad del Ayuntamiento de Alcobendas, así como cualquier otro en el que el Ayuntamiento tenga intereses públicos y cuyos principales objetivos son:

- Gestión, explotación y comercialización de inmuebles en el término municipal de Alcobendas que pertenezcan al Ayuntamiento, incluida la gestión de Viviendas Públicas Municipales en arrendamiento.
- Gestión de Derechos de Superficie, Concesiones Administrativas, Arrendamientos o cesiones de espacios y otros contratos.
- Comercialización, arrendamiento y gestión de edificios de oficinas, locales comerciales, trasteros y naves de propiedad municipal
- Gestión de plazas de aparcamiento mediante abonos mensuales.

Nuestra finalidad es obtener el máximo rendimiento económico del patrimonio municipal con el menor coste y la máxima satisfacción del usuario final; así como satisfacer las necesidades del

usuario final de las instalaciones gestionadas por SOGEPIMA, mediante atención personalizada y una relación óptima calidad/ precio.

5 ALCANCE

Esta política se aplica a todos los sistemas TI de SOGEPIMA, a toda la información y a todos sus miembros, sin excepciones.

6 MARCO NORMATIVO

El marco legal del sector de la organización es la Ley Arrendamientos Urbanos, CTE, Plan Estatal de Vivienda, Reglamentos a nivel municipal (como el Regulador del Registro Abierto Permanente de Solicitudes de Vivienda).

Esta política se sitúa dentro del marco jurídico definido por las leyes y Reales Decretos siguientes:

- Ley 34/2002, de servicios de la sociedad de la información y de comercio electrónico
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 1/07/2007 Reglamento de desarrollo de la Ley Orgánica y sus leyes posteriores Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias:
    - Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
    - Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- 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
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Real Decreto 951/2015, de 23 de octubre, de modificación del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica
- RGPD 27/04/2016 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

- Real Decreto Ley 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información.
- Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid.
- Real Decreto-Ley 2/2020, de 21 de enero de 2020, por el que se aprueban medidas urgentes en materia de retribuciones en el ámbito del Sector Público.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Real Decreto (RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS)
- https://www.ccn-cert.cni.es/. Medidas de seguridad establecidas en el ENS.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

7 ORGANIZACIÓN DE LA SEGURIDAD

7.1 ROLES: FUNCIONES Y RESPONSABILIDADES

En la tabla se usan las siguientes abreviaturas:

Gerencia – Persona con la máxima responsabilidad en la organización
CSI – Comité de Seguridad de la Información
RINFO – Responsable de la Información
RSERV – Responsable del Servicio
RSEG-CISO – Responsable de la Seguridad
RSIS – Responsable del Sistema
ASS-CISM – Administrador de la Seguridad del Sistema

Tarea	**Responsable**
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba: Gerencia
Normativa de seguridad	elabora: RSEG aprueba: Gerencia
Procedimientos operativos de seguridad	elabora: RSEG S aprueba: CSI aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI + Gerencia
Planes de concienciación y formación	elabora: RSEG aprueba: CSI + Gerencia
Planes de continuidad	elabora: RSIS valida: RSEG coordina: CSI aprueba: Gerencia ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

Respuesta a incidentes de seguridad de la información:

- ASS: Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- ASS: Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- ASS: Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).

- ASS: Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de estos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- ASS: Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- ASS: Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.
- RSEG: Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.
- RSIS: Planificar la implantación de las salvaguardas en el sistema.
- Comité de Seguridad de la Información: Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.
- RSIS: Ejecutar el plan de seguridad aprobado.

7.1.1 Comité de Seguridad de la Información

El Comité de Seguridad de la Información coordina la seguridad de la información a nivel de organización. La seguridad de la información necesita estar coordinada:

- Es conveniente coordinarla para racionalizar el gasto.
- Es necesario coordinarla para evitar disfunciones que permitan fallas de seguridad al ofrecer el Sistema puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques

El Comité de Seguridad de la Información estará formado por:

- Gerente de SOGEPIMA
- RINFO – Responsable de la Información
- RSERV – Responsable del Servicio
- RSEG – Responsable de la Seguridad
- RSIS – Responsable del Sistema
- ASS – Administrador de la Seguridad del Sistema

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

- Atender las inquietudes de la Gerencia y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Gerencia.
- 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 Gerencia.
- 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 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 y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Divulgación de la normativa y política de seguridad de la Empresa.
- Desarrollo del procedimiento de designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento de:
- Tareas de adecuación
- Análisis de Riesgos.
- Auditoría bienal.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TI en su ámbito de responsabilidad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Promover la formación y concienciación del Servicio de Informática dentro de su ámbito de responsabilidad.
- Coordinar con los distintos responsables que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del sistema.

7.1.2 Responsable de los servicios de información

Tendrá el rol de responsable de los servicios SOGEPIMA. Teniendo por funciones las siguientes:

- Tiene la potestad de establecer los requisitos de una información en materia de seguridad
- Establecimiento y aprobación de los requisitos de los servicios e información TI en materia de seguridad.
- Aceptación del riesgo residual
- Determinación de los niveles de seguridad requeridos en cada dimensión
- Trabajo en colaboración con el Comité de Seguridad de la Información

7.1.3 Responsable del servicio

Tendrá el rol de responsable de los servicios e información de SOGEPIMA. Teniendo por funciones las siguientes:

- Tiene la potestad de establecer los requisitos de una información en materia de seguridad
- Establecimiento y aprobación de los requisitos de los servicios ad.
- Aceptación del riesgo residual
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Trabajo en colaboración con el Comité de Seguridad de la Información

7.1.4 Responsable de la seguridad de la información

Tendrá el rol de responsable de la seguridad de la información de SOGEPIMA. Teniendo por funciones las siguientes:

- Determinación de la categoría del sistema
- Declaración de aplicabilidad
- Medidas de seguridad adicionales
- Elaborar Configuración de seguridad
- Documentación de seguridad del sistema
- Elaboración Normativa de seguridad

- Aprobar los Procedimientos operativos de seguridad
- Reportar el Estado de la seguridad del sistema
- Elaborar Planes de mejora de la seguridad
- Elaborar Planes de concienciación y formación
- Elaborar Planes de continuidad
- Aprobar Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios

7.1.5 Responsable del sistema

Tendrá el rol de responsable del sistema de SOGEPIMA. Trasladando la gestión diaria del sistema a la empresa encargada del mantenimiento. Teniendo por funciones las siguientes:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y nuevas personas usuarias en el sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del sistema y cerciorarse de que estas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
- Determinar la categoría del sistema realizando la evaluación de riesgos, evaluando las amenazas y los riesgos a los que puede estar expuesto y determinar las medidas de seguridad que deben aplicarse para eliminación, mitigación y/o asumir estos riesgos.
- Elaborar y aprobar la documentación de seguridad del sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicación a la persona responsable de seguridad o a quien está determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, la persona 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 las personas responsables de la información afectada, el servicio afectado y la persona responsable de seguridad, antes de ser ejecutada.
- Elaboración Planes de mejora de la seguridad y Planes de Continuidad
- Suspensión Temporal del Servicio
- Elaborar el Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios
- Planificar la implantación de las salvaguardas en el sistema.
- Ejecutar el plan de seguridad aprobado
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

7.1.6 Responsable de la Seguridad del Sistema

Tendrá el rol de responsable del sistema de SOGEPIMA. Trasladando la gestión diaria de la Seguridad del Sistema a la empresa encargada del mantenimiento. Teniendo por funciones las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Ejecutar el plan de seguridad aprobado

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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 Responsables de la Seguridad y del Sistema 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.
- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de estos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.

7.1.7 Delegado de Protección de datos (DPD)

Las funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión en, entre otras, las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Diseño e implantación de políticas de protección de datos
- Auditoría de protección de datos
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de datos

7.2 PROCEDIMIENTO DE DESIGNACION

El Comité de Seguridad de la Información y los demás responsables serán nombrado por Gerencia. Estos nombramientos serán revisables por la Gerencia, siempre que lo considere oportuno o por que el puesto quede vacante.

7.3 POLITICA DE SEGURIDAD DE LA INFORMACION

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 esta. La Política será aprobada por LA GERENCIA y difundida para que la conozcan todas las partes afectadas.

8 DATOS DE CARÁCTER PERSONAL

- SOGEPIMA realiza tratamientos en los que hace uso de datos de carácter personal. Cumpliendo o 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Todos los sistemas de información de SOGEPIMA se ajustan a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal. Las medidas de seguridad implantadas garantizan los derechos y libertades de los interesados.

9 GESTIÓN DE RIESGOS

A todos los sistemas sujetos a esta Política se 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 cada 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.

10 DESARROLLO DE LA NORMATIVA DE SEGURIDAD

Toda la normativa de seguridad se estructura en los siguientes niveles jerárquicos documentales:

Nivel 1: Política de Seguridad de la Información

Nivel 2: Procedimientos de Seguridad de la Información

Nivel 3: Instrucciones Técnicas, Normas y Guías de Seguridad de la Información,

Toda la normativa de seguridad estará a disposición de cualquier persona de la empresa que necesite conocerla, en particular para quienes utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en el servidor de documentación de la empresa en la carpeta SGSI con la ruta: \\servidorh\SGSI

10.1 Primer nivel: Política de Seguridad de la Información

Constituye el primer nivel la Política de Seguridad de la Información, recogida en el presente documento, PS 01, realizado por el Responsable de seguridad, revisado por el Comité de Seguridad de la Información y aprobado por la Gerencia.

PS 01 Política de Seguridad de la Información

10.2 Segundo nivel: Normas y Procedimientos de Seguridad de la información

El segundo nivel desarrolla la Política de Seguridad de la Información mediante normas y procedimientos de seguridad, NOR – XX y PRS – XX, que desarrollan un tema o aspecto determinado de la seguridad de la información.

Los Procedimientos de Seguridad serán realizados por el Responsable del Departamento implicado, revisados por el Responsable del Sistema y aprobados por el Comité de Seguridad de la Información.

10.3 Tercer nivel: Instrucciones Técnicas y guías de Seguridad de la información

El tercer nivel está constituido por instrucciones técnicas de seguridad (ITS) de carácter técnico o procedimental que se deben realizar en tareas o actividades relacionadas con la seguridad de la información y la protección de la información y de los servicios, y que podrán ser elaboradas por cualquier técnico o empleado, revisadas por el Responsable de Seguridad y el Responsable del Departamento correspondiente y aprobadas por el Responsable del Sistema.

Dependiendo del aspecto tratado, se aplicarán a un ámbito específico o a un sistema determinado.

11 OBLIGACIONES DEL PERSONAL

Todas las personas que forman parte de SOGEPIMA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a las personas o servicios afectados.

Todos los miembros de SOGEPIMA atenderán a una sesión de concienciación en materia de seguridad TI, al menos una vez al año. Se establecerá un **programa de acciones de concienciación** continua para atender a la totalidad del personal y en particular a las nuevas incorporaciones.

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

12 TERCERAS PARTES

Cuando SOGEPIMA preste servicios a otros organismos / empresas o maneje información de otros organismos / empresas, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comité de Seguridad Información / Responsables de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SOGEPIMA utilice servicios de terceros o ceda información a terceros, se les exigirá el cumplimento 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se define en los párrafos anteriores, se requerirá un informe del Comité de Seguridad de la información 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.

13 ACUERDOS DE CONFIDENCIALIDAD

Todos los empleados de SOGEPIMA y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la empresa, los cuales reflejan los compromisos de protección y buen uso de la información, de acuerdo con los criterios establecidos por ella.

En el caso de contratistas y personas o entidades externas, los respectivos contratos deben incluir una cláusula de confidencialidad que regule el acceso a la información y/o a los recursos de SOGEPIMA.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Anexo 1. PROHIBICIONES

Se prohíben expresamente las siguientes actividades:

Compartir o facilitar el identificador de usuario y la contraseña para acceder a los sistemas de información a otra persona física, incluido el personal de SOGEPIMA. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona física que utilice de forma no autorizada el identificador del usuario.

- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad.
- El uso del sistema informático de SOGEPIMA para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad de SOGEPIMA y los cometidos del puesto de trabajo del usuario.
- El acceso a debates en tiempo real (Chat / IRC, Redes Sociales, Redes P2P, Descargas Directas) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido; a excepción de cuando sea necesario para desempeñar las funciones de su puesto de trabajo.
- El acceso a páginas web, grupos de noticias (Newsgroups) y otras utilidades como FTP, telnet, etc. se limita a aquellos sitios que contengan información relacionada con la actividad de SOGEPIMA o con los cometidos del puesto de trabajo del usuario.
- El uso de dispositivos portables (tipo pendrive) de información para transportar o almacenar información.
- SOGEPIMA se reserva el derecho de comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa con el fin de prevenir un uso fraudulento, ilegal, abusivo o no autorizado de Internet. Dicha comprobación incluye la revisión de registros que muestran los ficheros cargados, los que se han accedido, las páginas web visitadas y los usuarios que han ejecutado tales acciones, así como el momento en el que se han producido. Todos los empleados quedan avisados que pueden ser monitorizado su trabajo.
- Cualquier persona que acceda a Internet a través de la red de SOGEPIMA acepta esta comprobación, así como las normas aquí establecidas, asumiendo la imposición de acciones disciplinarias por incumplimiento de las citadas normas.
- Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Se prohíbe la descarga a través de Internet de software de origen desconocido o de propiedad del usuario en los sistemas de SOGEPIMA, salvo que exista una autorización previa.

50693372S JULIA PEREZ (R: A79402038)

Firmado digitalmente por 50693372S JULIA PEREZ (R: A79402038)
Fecha: 2024.01.17 11:29:03 +01'00'