SYSRED-CONSULTORÍA Y DESARROLLOS S.L.

Seguridad de la Información

PLS-GLB-001

Política General de Seguridad de la Información

CONTROL DE EDICIÓN

FECHA	VERSIÓN	CREACIÓN	APROBACIÓN	CAMBIOS
20/04/2020	01	CSI	Gerencia	Versión inicial
04/11/2020	02	CSI	Gerencia	Cambios en roles
18/12/2023	03	CSI	Gerencia	Adaptación nuevo RD y nuevos requisitos mínimos de seguridad
Las aprobaciones de los documentos figuran en sus actas correspondientes, e incluyen su revisión.				

CLASIFICACIÓN

PÚBLICO

LISTA DE DISTRIBUCIÓN

PERSONA	CARGO
Difusión pública	----------

El presente documento está dirigido EXCLUSIVAMENTE a las personas nombradas en la lista de distribución, quienes podrán, en base a su criterio, divulgarlo a quienes consideren oportuno. Se recomienda encarecidamente una divulgación controlada en la que todos los cesionarios del documento conozcan inequívocamente su CLASIFICACIÓN y se comprometan a mantener la consecuente confidencialidad en todo su ciclo de uso y, en su caso, archivo y/o destrucción.

ÍNDICE

Contenido y objetivos del presente documento.
Este documento contiene la Política General de Seguridad de la Información (PGSI en adelante) de SYSRED-CONSULTORÍA Y DESARROLLOS S.L. ("la Organización" o "la Empresa", en adelante).

El objetivo fundamental de esta Política se centra en definir las estructuras organizativas, roles, responsabilidades, criterios e iniciativas de esta Organización respecto a la Seguridad de la Información que almacena y gestiona, así como el cumplimiento de los diferentes marcos normativos que la regulan.

1. Datos de SYSRED-CONSULTORÍA Y DESARROLLOS S.L.

Razón social	SYSRED-CONSULTORÍA Y DESARROLLOS S.L.
NIF	B54124441
Domicilio	Calle Gabriel Miró, 3
Población	Castalla
Código Postal	03420
Provincia	Alicante
País	España
Sector de actividad	Desarrollo y mantenimiento de aplicaciones informáticas

2. Justificación de una Política General de Seguridad de la Información.

Los marcos normativos vigentes en materia de Seguridad de la Información requieren la disponibilidad de una Política de Seguridad corporativa que, aprobada por el denominado "Órgano Superior Competente", representado en el caso de SYSRED-CONSULTORÍA Y DESARROLLOS S.L. por su Gerencia, y adecuadamente difundida entre el personal y todas las entidades afectadas, implemente los requerimientos de dichos Marcos con el fin de preservar los derechos y libertades de los interlocutores sociales con quienes interactúa la Organización, englobados todos ellos en adelante bajo la denominación genérica "interlocutores", "interlocutores sociales", "terceros" o "partes interesadas".

La diversidad de marcos normativos, sus diferentes ámbitos objetivos y subjetivos, así como la evolución permanente de los mismos, aconsejan desarrollar una PGSI unificada y permitir con ello eliminar redundancias en actividades, documentos y controles, optimizando con ello las actuaciones corporativas y el nivel de cumplimiento normativo.

3. Ámbito objetivo de la PGSI.

La PGSI abarca todos los medios, automatizados o no, que la Organización utiliza para el desarrollo de sus competencias y actividades, así como todos los medios por los cuales interopera con otras Entidades, públicas y/o privadas. Las actividades incluyen:

(1). Las relaciones de carácter jurídico-económico-administrativo entre los interlocutores sociales y la Organización.

(2). La realización de las funciones de negocio / servicio por parte de la Organización, tanto los desarrollados por medios electrónicos como los manuales.

(3). El tratamiento de la información gestionada por la Organización en el ejercicio de sus competencias, especialmente aquélla relacionada con datos personales.

(4). Las relaciones de la Organización con las Administraciones Públicas.

4. Ámbito subjetivo de la PGSI.

La PGSI será aplicada por todos los servicios, departamentos, secciones, áreas, unidades administrativas de la Organización y, en general, por todas las entidades internas y externas de cualquier tipo vinculadas a esta Entidad mediante cualquier modelo de relación. Con el fin de unificar la terminología las estructuras organizativas internas serán denominadas “departamentos” en adelante.

La PGSI afecta a todo el personal de la Organización, sea cual sea su relación laboral con la misma. Asimismo, la PGSI afecta a todo el personal que presta servicios a la Organización a través de empresas externas y que, en razón de esta relación, acceda, almacene y/o trate información cuya competencia y/o responsabilidad recaiga sobre la Organización.

La PGSI será aplicada en las relaciones de la Organización con los interlocutores sociales, Empresas y Entidades públicas y/o privadas con las que interactúe, por lo que las personas que intervengan en estas relaciones están incluidas en los sujetos a quienes resulta de aplicación esta política.

5. Misión y servicios prestados.

SYSRED-CONSULTORÍA Y DESARROLLOS S.L. ha definido como misión la oferta de productos y servicios líderes en su sector, cumpliendo los marcos normativos que les afectan, aportando a sus interlocutores de negocio valor añadido, colaboración, honestidad, implicación y compromiso, todo ello en base a equipos de trabajo formados, motivados y compartiendo la misión corporativa.

La aplicación SYSPOL, destinada a la gestión de la Policía Local, materializa la misión corporativa, aplicando los fundamentos de ésta en todas las fases de su ciclo de vida, haciendo especial énfasis en la seguridad de sus datos y operaciones.

6. Marcos normativos referenciales de la PGSI.

Los marcos normativos referenciales se encuentran en el Registro Corporativo de Marcos Normativos:

SYSRED-RGS-GLB-610-Normativa aplicable

Conteniendo los marcos normativos aplicables en SYSRED-CONSULTORÍA Y DESARROLLOS S.L.

7. Órgano Superior Competente.

A los efectos de las actuaciones previstas en el SGSI y encomendadas al denominado "Órgano Superior Competente", este Órgano, en SYSRED-CONSULTORÍA Y DESARROLLOS S.L., será la Gerencia y, en su caso, en quien se establezca la oportuna delegación.

8. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD

SYSRED, para alcanzar el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad en SYSRED, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se debe prestar la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que la ignorancia, la falta de organización y coordinación o instrucciones inadecuadas constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para el correcto ejercicio, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance los objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo las desarrollan las personas autorizadas, desde

emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultades.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas para que se persigue. El uso ordinario del sistema debe ser sencillo y seguro, de manera que una utilización insegura requiera un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, para eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Vigilancia continua, re-evaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte de SYSRED permitirá la detección de actividades o comportamientos anómalos y la respuesta oportuna.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se re-evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuera necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y la monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de manera continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Gestión de personal y profesionalidad

Todo el mundo, propio o ajeno relacionado con los sistemas de información de SYSRED, dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y el alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De la misma manera, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo del puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases del ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Incidentes de seguridad, prevención, detección, reacción y recuperación

SYSRED dispone de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de las vías de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, con el fin de minimizar las vulnerabilidades y conseguir que las amenazas sobre éste no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

Del mismo modo, el sistema mantendrá los servicios disponibles durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención frente a otros sistemas de información interconectados

SYSRED ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de manera que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada ante los incidentes que no se han podido evitar, reduciendo la probabilidad de que el sistema sea comprometido en conjunto y minimizar su impacto final.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema de SYSRED se conecta a redes públicas, tal y como se definen en la legislación vigente en materia de telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará el punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la instrucción técnica de seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

SYSRED ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "MODELO DE GOBERNANZA" del presente documento.

Autorización y control de los accesos

SYSRED ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

SYSRED ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad, SYSRED, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tráfico y continuidad de la actividad

SYSRED prestará especial atención a la información almacenada o en tráfico a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para conseguir una adecuada protección.

Deben aplicarse procedimientos que garanticen la recuperación y la conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este Real Decreto, cuando sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a que se refiere este Real Decreto, deberá estar protegida con el mismo grado de seguridad que la misma. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que sean aplicables.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código nocivo

SYSRED, con el propósito de satisfacer el objeto de este Real Decreto, con garantías plenas del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que sean aplicables, registrará las actividades de los usuarios, reteniendo

la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Con el fin de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, SYSRED podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de manera que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código nocivo así como otros daños en las redes y sistemas de información mencionadas.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de manera única, de manera que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

SYSRED, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

SYSRED tendrá en cuenta la aplicación de los perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

9. Organización de la Seguridad.

9.1. Definición de roles.

Tal como indican las normas de referencia, la seguridad deberá comprometer a todos los miembros de la Organización. La Política de Seguridad debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la Organización.

Adicionalmente, otros marcos normativos requieren asimismo la creación de roles específicos, tales como el rol Delegado de Protección de Datos en el RGPD-LOPDGDD.

Se establecen por tanto los siguientes roles en la Organización relacionados con la Seguridad de la Información:

9.2. Responsable de Desarrollo de SW (RDSW).

Competencias y responsabilidades con el ciclo de vida del desarrollo de SW y su cumplimiento de los requisitos de seguridad, tanto de los clientes como de los internos.

Entre sus competencias en materia de seguridad:

1. Es responsable de definir e implementar las metodologías apropiadas para un desarrollo sistemático y controlado de las aplicaciones corporativas.
2. Es responsable de controlar el ciclo de vida integral del desarrollo de las aplicaciones, desde la ingeniería de requerimientos hasta la liberación del producto, manteniendo la consistencia en todas las etapas del ciclo de vida.
3. Es responsable de implementar las medidas de seguridad en las aplicaciones que permitan el cumplimiento de las mismas respecto a los marcos referenciales requeridos, muy especialmente las relacionadas con el precepto "Privacidad por diseño y por defecto" del RGPD, así como las medidas del ENS relacionadas con el desarrollo de software.
4. Es responsable del mantenimiento y evolución de las aplicaciones corporativas, manteniendo en todo momento el cumplimiento normativo requerido y el alineamiento de las aplicaciones con los objetivos corporativos.
5. En directa relación con el Responsable del Sistema, debe participar activamente en la respuesta a los incidentes imputables a las aplicaciones corporativas.
6. Es responsable de la integración de las aplicaciones corporativas con otros componentes propios y externos, aplicando en todos los casos las medidas de seguridad apropiadas a dichas integraciones, muy especialmente cuando éstas incluyan tratamientos de datos personales o de datos corporativos sensibles.

9.3. Responsable de Seguridad de la Información. (RSEG o CISO).

El rol de Responsable de Seguridad debe asumir las siguientes funciones:

- Tareas y controles asignados al rol Responsable de Seguridad en ENS. Coordinará y controlará las medidas definidas en las políticas, normas, procedimiento e instrucciones sobre Seguridad y, en general, se encargará del cumplimiento de las medidas de seguridad que detalla el ENS.
- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Mantendrá la Seguridad de la Información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en esta Política de Seguridad de la Organización.

- Promoverá la formación y concienciación en materia de Seguridad de la Información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema.
- Realizará el Análisis y Gestión de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme a lo requerido en las Normas, al Anexo II del ENS (cuando aplique) y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a Seguridad de la Información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
- Actuará en plena coordinación con el Delegado de Protección de Datos (RGPD).

9.4. Responsable de Sistema (RSIS o CIO).

Las funciones del Responsable del Sistema (o Responsables de Sistemas si así se establece) son:

- Desarrollar, operar y mantener los Sistemas de Información durante todo su ciclo de vida, así como de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir el sistema de gestión de los Sistemas 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.
- El 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 los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad de los Sistemas de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema para que sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

9.5. Administrador de la Seguridad del Sistema (ASS).

Al rol Administrador de la Seguridad del Sistema le corresponden las siguientes funciones:

- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los Sistemas de Información.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los Sistemas de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente de los Sistemas de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

En caso de ocurrencia de incidentes de Seguridad de la Información:

- Llevar a cabo el registro, seguimiento y gestión de los incidentes de seguridad en los sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar los incidentes para evitar la propagación a elementos ajenos a la situación de riesgo.
- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves.
- Asegurar la integridad de los elementos críticos del sistema si se ha visto afectada la disponibilidad de los mismos.
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar incidentes. Determinar el modo, los medios, los motivos y el origen del incidente, su causa raíz, sus mecanismos de solución y documentar "lecciones aprendidas".

9.6. Equipo de Respuesta a Incidentes (IRT).

- Detección, recepción y actuación ante las incidencias relacionadas con la seguridad de la información. Procedimientos de escalada.
- Desarrollo de un entorno de "lecciones aprendidas" para evitar que se repita un incidente.
- Métricas e indicadores de incidencias, informando al Comité de Seguridad.
- Dirigido por RSEG / CISO.

9.7. Delegado de Protección de Datos (DPD).

El rol de Delegado de Protección de Datos (DPD) es requerido por el RGPD en base a su Art. 37:

> *Artículo 37 Designación del delegado de protección de datos*
> *1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*
>
> *a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.*
> *b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.*
> c) *Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 RGPD y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD.*

Adicionalmente, la LOPDGDD, en su *Artículo 76. Sanciones y medidas correctivas* incluye como punto a considerar en un posible procedimiento sancionador:

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

En base a estas consideraciones, SYSRED-CONSULTORÍA Y DESARROLLOS S.L. asume la necesidad de disponer del rol Delegado de Protección de Datos.

Por tanto, se identificará y nombrará un Delegado de Protección de Datos corporativo, si bien este rol podrá ser asignado a personal interno o a un servicio externo.

La titularidad concreta del DPD corporativo se determinará mediante designación del Órgano Superior Competente, tras informe del Comité de Seguridad de la Información.

Las funciones del DPD están definidas en el RGPD.

9.8. Comité de Seguridad de la Información.

9.8.1. Composición.

Se crea el Comité de Seguridad de la Información, que estará compuesto por los siguientes miembros:

Posición	Asignación
Presidente	Gerencia
Secretario	Responsable de Seguridad (RSEG)
Vocal 1	Responsable de Sistema (RSIS)

El Comité de Seguridad de la Información podrá convocar a responsables departamentales y/u otras personas cuya intervención sea requerida para el desarrollo de las actuaciones del Comité. Es obligatoria la asistencia de las personas convocadas, la aportación de toda la información que les sea solicitada y el cumplimiento de las instrucciones recibidas del Comité de Seguridad de la Información.

Corresponde al Secretario/a del Comité de Seguridad de la Información:

- Convocar 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.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Todos los miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

9.8.2. Funciones del Comité de Seguridad de la Información.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Atender los requerimientos, objetivos y necesidades de información del Órgano Superior Competente y de los diferentes departamentos.
- Informar regularmente del estado de la Seguridad de la Información al Órgano Superior Competente.
- 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 la 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 Dirección.
- 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.
- Asegurar que la Seguridad de la Información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación, incluyendo el principio de “Privacidad por diseño y por defecto” requerido por el RGPD. 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.
- Recabar regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

- Obtener asesoramiento sobre los temas que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
  - Grupos de trabajo especializados internos, externos o mixtos.
  - Asesoría interna y/o externa.
  - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.
- Aprobar el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente, para su presentación al Órgano Superior Competente y su correspondiente aprobación formal.
- Asumir los roles de Responsable de Servicio y Responsable de Información especificados en el ENS.

9.9. Jerarquía en el proceso de decisiones y mecanismos de coordinación.

Los diferentes roles de Seguridad de la Información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple:

9.9.1. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información da instrucciones al Responsable de Seguridad de la Información, quien se encarga de cumplimentarlas, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en esta PGSI.

9.9.2. Responsable de Seguridad de la Información.

El Responsable de la Seguridad de la Información:

1. Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
2. Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
3. Rinde cuentas al Comité de Seguridad de la Información, como secretario:
   - Resumen consolidado de actuaciones en materia de seguridad.
   - Resumen consolidado de incidentes relativos a la Seguridad de la Información.
   - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
4. Rinde cuentas al Órgano Superior Competente, según lo acordado en el Comité de Seguridad de la Información.
   - Resumen consolidado de actuaciones en materia de seguridad.
   - Resumen consolidado de incidentes relativos a la Seguridad de la Información.

- Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

9.9.3. Responsable de sistema.

El Responsable del Sistema:

1. Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
2. Informa al Responsable de Servicio de las incidencias funcionales relativas al servicio que le compete.
3. Da cuenta al Responsable de la Seguridad:
   - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
   - Resumen consolidado de los incidentes de seguridad.
   - Medidas de la eficacia de las medidas de protección que se deben implantar.

9.10. Procedimientos de designación de personas.

El Órgano Superior Competente nombrará formalmente, mediante las resoluciones pertinentes:

- Comité de Seguridad de la Información.
- Delegado de Protección de Datos.
- Responsable/s de la Seguridad.
- Responsable/s de los Sistemas de Información.
- Administrador/es de Seguridad del Sistema, a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

9.11. Segregación de funciones.

El ENS recoge el principio de “seguridad como función diferenciada”. Este principio exige:

- Responsable de Seguridad debe ser independiente del Responsable del Sistema.
- Responsable de Servicio o de Información debe ser independiente de Responsable del Sistema.
- Las personas asignadas a funciones de desarrollo deberán ser independientes de las personas asignadas a los pases a producción.
- Las personas asignadas a la operación de sistemas deberán ser independientes de las personas asignadas al mantenimiento de sistemas.
- Delegado de Protección de Datos debe ser independiente de toda influencia que pudiera condicionar sus actuaciones, en base a lo requerido en el RGPD.

La asignación de roles y responsabilidades tendrá en cuenta la preceptiva segregación de funciones, de forma que las actuaciones de las personas titulares de los mismos no comprometan

la seguridad de Informaciones y Servicios en cualquiera de sus dimensiones (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).

En casos excepcionales, sobre todo cuando no están disponibles los recursos necesarios, pueden exceptuarse estas reglas de segregación de funciones, estableciendo las medidas compensatorias apropiadas para la resolución de los conflictos de intereses que puedan surgir.

En este sentido, el Responsable de Sistema asumirá el rol de Responsable de Desarrollo de SYSRED-CONSULTORÍA Y DESARROLLOS S.L.

9.12. Suplencias y delegaciones.

Los roles requeridos por los marcos normativos referenciales de esta PGSI deben estar permanentemente operativos. La Organización establecerá un procedimiento formal de suplencias y/o delegaciones de forma que la ausencia de una persona, por cualquier motivo, no cause la carencia de las funciones y/o competencias que desarrolla.

10. Datos de carácter personal.

10.1. Tratamiento.

Para la prestación de los servicios corporativos deben ser recabados, tratados y almacenados datos de carácter personal. Es compromiso de SYSRED-CONSULTORÍA Y DESARROLLOS S.L. respetar y proteger los derechos recogidos en la Constitución Española respecto a la intimidad, privacidad, imagen y honor de las personas, por lo que el cumplimiento de los marcos normativos que los regulan y, por ende, la implementación de las medidas de seguridad y control requeridas constituye un objetivo prioritario de esta Organización.

El cumplimiento de RGPD, LOPDGDD y sus marcos normativos que los desarrollan será una iniciativa prioritaria. Se adoptarán las medidas necesarias para que esta Organización cumpla en sus fechas de entrada en vigor todos los preceptos de los nuevos marcos, siendo uno de los puntos más importantes el nombramiento de la figura DPO/DPD (Data Protection Officer/Delegado de Protección de Datos).

Asimismo, deberán realizarse los ciclos de formación y concienciación específicos para que el personal conozca las medidas que deben aplicar en sus puestos de trabajo y los medios disponibles para la resolución de dudas, problemas e incidentes relacionados.

Será prioritario implementar las medidas organizativas y técnicas apropiadas para proteger los derechos y libertades de las personas físicas afectadas por los tratamientos de datos personales realizados por la Organización.

10.2. Videovigilancia.

La Organización observará en todo momento la normativa vigente en materia de videovigilancia de los espacios públicos y privados, respetando los derechos de las personas captadas y cancelando las imágenes en los plazos establecidos por dicho ordenamiento.

11. Terceras partes.

Cuando se presten servicios o se gestione información de otras Organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Las entidades terceras deberán seleccionarse atendiendo a los principios de idoneidad y cumplimiento de los marcos normativos exigibles, además del resto de criterios aplicables en su contratación.

Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

En caso de que 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 departamentales afectados antes de seguir adelante con la contratación.

En caso de que los tratamientos desarrollados por terceras partes involucren datos de carácter personal, se realizarán todas las actuaciones requeridas por el RGPD y LOPDGDD. En este último caso, se evaluará la idoneidad de los proveedores, tal como requiere el RGPD, y se firmarán los correspondientes contratos de “encargado de tratamiento” o “corresponsabilidad” con todo proveedor que desarrolle sus tareas tratando datos personales o “compromisos de confidencialidad y seguridad de la información” cuando los tratamientos de datos personales sean incidentales.

12. Revisión y aprobación de la Política de Seguridad

La Política General de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el Órgano Superior Competente.

Cualquier cambio sobre la Política de Seguridad de la Información deberá ser difundido a todas las partes afectadas y, en su caso, objeto de reciclaje en la formación para el personal afectado.

13. Documentación complementaria.

La Política de Seguridad de la Información se completará con documentos más detallados, que ayudan a materializar sus preceptos. Para ello se utilizarán:

13.1. Normas de Seguridad.

Las normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

13.2. Procedimientos de Seguridad.

Los procedimientos de seguridad detallan tareas concretas, indicando su operativa claramente.

13.3. Instrucciones de Seguridad.

Las instrucciones de seguridad desarrollan la operativa descrita en los procedimientos, explicando a nivel técnico su implementación.

14. APROBACIÓN Y ENTRADA EN VIGOR.

Esta Política General de Seguridad de la Información es efectiva desde la fecha de su aprobación y será válida hasta que sea reemplazada por una nueva Política o sea derogada por resolución del Órgano Superior Competente de SYSRED-CONSULTORÍA Y DESARROLLOS S.L.

Este texto anula cualquier Política de Seguridad de la Información vigente hasta la fecha de aprobación de la presente.

Texto aprobado en Castalla, el día 18 de diciembre de 2023.

LAHOSA LAGUNA RICARDO ALFREDO - 21442187T

Firmado digitalmente por LAHOSA LAGUNA RICARDO ALFREDO - 21442187T
Fecha: 2023.12.18 15:19:12 +01'00'

Firmado: **Ricardo Lahosa Laguna**
Gerente de SYSRED-CONSULTORÍA Y DESARROLLOS S.L.