COGERSA

Política de Seguridad de la Información de

COGERSA, S.A.U.

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Índice

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde su aprobación por parte del Comité de Seguridad de la Información hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Compañía para la Gestión de los Residuos Sólidos de Asturias, en adelante COGERSA, S.A.U., es la sociedad instrumental, integrada por el Gobierno del Principado y los 78 ayuntamientos de la comunidad. COGERSA, S.A.U. basa su estrategia en la gestión eficiente de los residuos, en mantener y adaptar las infraestructuras de tratamiento centralizado para ofrecer soluciones adecuadas a las necesidades presentes y futuras, así como en fomentar la corresponsabilidad de toda la sociedad en torno a los residuos a través de acciones de sensibilización y educación ambiental dirigidas a toda la sociedad asturiana; todo ello con el objetivo último de contribuir a avanzar en Asturias hacia la economía circular.

COGERSA, S.A.U. protegerá su ecosistema tecnológico tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los ecosistemas tecnológicos deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapta a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que las áreas deben aplicar las medidas mínimas de seguridad de la información exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes áreas deben cerciorarse de que la seguridad de la información en entornos digitales es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los proyectos tecnológicos, los requisitos de seguridad de la información, la normativa y las necesidades de financiación deben identificarse e incluirse en el plan de contratación.

3. MISIÓN DEL COGERSA, S.A.U.

COGERSA, S.A.U., tiene publicados sus intereses, funciones y competencias en el siguiente enlace: https://cogersa.es/que_es_cogersa/.

4. ALCANCE

Esta Política se aplicará a todo el sistema de información de COGERSA, S.A.U., al personal interno y externo que acceden o prestan servicio al mismo.

El alcance de esta política es:

El sistema de información que da soporte a los servicios informáticos internos de TI de COGERSA, S.A.U., de acuerdo con la declaración de aplicabilidad vigente.

5. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del COGERSA, S.A.U. en el alcance de esta Política, y, en particular, la prestación de sus servicios afectado por el alcance, se recoge en el ANEXO I - MARCO NORMATIVO y deberá mantenerse actualizado, siendo responsabilidad del Comité de Seguridad de la Información de COGERSA, S.A.U.

En dicho anexo se incluirán los siguientes apartados:

1. Legislación estatal y/o autonómica en materia de seguridad de la información y disposiciones que la desarrollan.
2. Instrucciones técnicas de seguridad de la información de obligado cumplimiento, dictadas al amparo de lo previsto en el Esquema Nacional de Seguridad.
3. Otras guías o recomendaciones distintas a las anteriores, que puedan ser de aplicación en la seguridad de la información de COGERSA, S.A.U.

6. CUMPLIMIENTO DE ARTÍCULOS

COGERSA, S.A.U., para lograr el cumplimiento de los artículos que recogen los principios básicos y de los requisitos mínimos, del Real Decreto por el que se regula el Esquema Nacional de Seguridad ha implementado diversas medidas de seguridad de la información proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad de la información como un proceso integral y seguridad de la información por defecto

La seguridad de la información 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 a COGERSA, S.A.U., estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará 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 de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad de la información.

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

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
d) Se aplicarán guías de configuración de seguridad de la información para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad de la información

La vigilancia continua por parte de COGERSA, S.A.U. permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

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

Las medidas de seguridad de la información se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad de la información, si fuese 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 monitorización permanentes permitirán adecuar el estado de seguridad de la información 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 de la información implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de la información de las tecnologías de la información.

Gestión de personal y profesionalidad

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

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

La seguridad de la información de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su 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.

Gestión de la seguridad de la información basada en los riesgos y análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad de la información y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad de la información, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II del ENS, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir

los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad de la información, prevención, detección, reacción y recuperación

COGERSA, S.A.U., dispone de procedimientos de gestión de incidentes de seguridad de la información de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad de la información correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad de la información del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo 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 de la información.

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

De igual modo, el sistema mantendrá disponibles los servicios 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 ante otros sistemas de información interconectados

COGERSA, S.A.U. ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad de la información, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

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

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su 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 de la información-

COGERSA, S.A.U. ha organizado su seguridad de la información comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad de la información con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN" del presente documento.

Autorización y control de los accesos

COGERSA, S.A.U. 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

COGERSA, S.A.U. 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 de la información, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad de la información y contratación de servicios de seguridad de la información

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

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

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

COGERSA, S.A.U. prestará especial atención a la información almacenada o en tránsito 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 lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y 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 ello sea exigible.

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

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

Registros de actividad y detección de código dañino

COGERSA, S.A.U. con el propósito de satisfacer el objeto del Real Decreto por el cual se regula el Esquema Nacional de Seguridad con plenas garantías 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 resulten de aplicación, 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.

Al objeto de preservar la seguridad de la información 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, COGERSA, S.A.U. 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 forma 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 dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo 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

COGERSA, S.A.U. 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

COGERSA, S.A.U. tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos que sean de aplicación.

Mejora continua del proceso de seguridad de la información

COGERSA, S.A.U. actualizará y mejorará de forma continua el proceso de seguridad de la información integral implantado, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información, adaptada a las necesidades y particularidad de COGERSA, S.A.U., se han definido los siguientes roles:

7.1 Roles o perfiles de seguridad de la información

- **Responsables de Información y Responsable de Servicios:** sus funciones y responsabilidades serán asumidas por el Comité de Seguridad de la Información de COGERSA, S.A.U..
- **Responsable de Seguridad de la información:** Jefe del Área de Digitalización y Sistemas de COGERSA, S.A.U..
- **Responsable del Sistema:** será uno de los operarios del Área de Digitalización y Sistemas de Informática.

7.2 Comité de Seguridad de la información

COGERSA, S.A.U. dispone de un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

- **Presidente:** Gerente de COGERSA S.A.U.
- **Secretario:** Jefe de Área Digitalización y Sistemas (Responsable de Seguridad de la información)
- **Vocales:**
  - Operario de Sistemas (responsable del Sistema)
  - Jefa de Área de Personas
  - Jefa de Área de Contratación
  - Técnico del Área de Tratamiento
  - Responsable de Puntos Limpios y Transferencia
  - Responsable de Calidad
- **Otros miembros convocados para consultas concretas:**

- Asesores/grupos de trabajo externos, especialistas en la materia, que podrán participar como asesores, con voz, pero sin voto.
- El delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de Seguridad de la Información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del delegado de Protección de Datos.

El Comité de Seguridad de la Información celebrará sus sesiones ordinarias en las dependencias de COGERSA con una periodicidad anual, pudiendo convocar reuniones extraordinarias cuando se requiera.

7.3 Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad de la información ENS:

Funciones del Responsable de Información y Servicios (Comité de Seguridad de la información):

- Establecer y aprobar los requisitos de seguridad de la información aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del ENS previa propuesta al Responsable de Seguridad de la información ENS, y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad de la información:

El Responsable de Seguridad de la información desempeñará las siguientes funciones:

- Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad; identificar medidas de seguridad de la información; determinar configuraciones necesarias; elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad de la información y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.

- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad de la Información los cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad de la información.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad de la información se integren adecuadamente dentro del marco general de seguridad de la información.
- Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad de la información y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad de la información del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de la información.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad de la información 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 de la información no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad de la información proporcionado por las herramientas de gestión de eventos de seguridad de la información y mecanismos de auditoría técnica.

7.4 Funciones del Comité de Seguridad de la Información

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

- Recoger las responsabilidades y funciones de los Responsables de Información y Responsables de Servicios.
- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad de la información y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos 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 ecosistemas tecnológicos.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad de la información y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
    - Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Gerencia.
    - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la organización en materia de seguridad de la Información.

El Comité se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad de la información.

7.5 Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política aprobada por los miembros del Comité de Seguridad de la Información y resuelta por Gerencia.

Los miembros del Comité, así como los roles de seguridad de la información serán revisados cada cuatro años o con ocasión de vacante.

8. DATOS DE CARÁCTER PERSONAL

COGERSA, S.A.U. solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De conformidad con la vigente normativa de protección de datos, entre otra, el 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), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y los criterios interpretativos de las autoridades de control, COGERSA, S.A.U. implementa las medidas de cumplimiento normativo, entre otras, el análisis de base de licitud de los tratamiento incluidas en el registro de actividades del tratamiento, el análisis de riesgos, la evaluación de impacto cuando existe un riesgo alto para los derechos y libertades de las personas afectadas por el tratamiento o el nombramiento de un Delegado de Protección de Datos.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de los objetivos marcados en esta Política de Seguridad de la información se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad de la información asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información, proponiendo la aprobación, en caso de que sea necesario, de mejoras de la misma al mismo órgano que la aprobó inicialmente.

10. TERCERAS PARTES

Cuando COGERSA, S.A.U. preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. COGERSA, S.A.U., definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad de la información, así como el resto de las actuaciones que COGERSA, S.A.U. lleve a cabo en materia de Seguridad de la información en relación con otros organismos.

Cuando COGERSA, S.A.U. utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la información y de la Normativa de Seguridad de la Información que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad de la información, al menos al mismo nivel que el establecido en esta Política de Seguridad de la información.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad de la información y del Real Decreto por el que se regula el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad de la información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un análisis del Responsable de Seguridad de la Información ENS que precise los riesgos en que se incurre y la forma de tratarlos.

11. Responsabilidades y funciones

Responsable	Funciones
Comité de Seguridad de la Información	Aprueba y da seguimiento a la Política de Seguridad de la Información
Responsable de	Define, desarrolla y supervisa las medidas recogidas en la Política.

Seguridad de la Información	
Responsable del Sistema	Apoya y despliega las medidas.

12. Control de cambios

Identificación	Fecha	Control de cambios
PD_ENS_01_Política_Seguridad_de_la_Información_v00	09/04/2026	Versión inicial del documento