La vigencia de este proceso se tiene que confrontar con la fecha que consta en Qualitas CLOUD

El original en vigor está disponible en Qualitas CLOUD

Descripción

POLÍTICA de Seguridad de la Información del ENS RD311/2022 de EMALSA

Aprobado

08/01/2025

Cambios Versión

Redefinición Comité de Seguridad de la Información.

Objeto

La Política que inspira los sistemas de Gestión de Seguridad de la información y específicamente del Esquema Nacional de Seguridad (ENS), según el RD 311/2022 de **EMALSA**, responde a la inquietud de mejora e innovación en el desarrollo y gestión con alto nivel de prestaciones acorde a los requisitos reglamentarios y legales, así como los específicos de sus clientes. La orientación y el valor para los clientes y la sociedad debe asegurar la información soportada en las Tecnologías de la Información, y garantizar una eficaz gestión de los servicios.

EMALSA integra las politias del SGSI de SAUR y establece:

- Dadas las amenazas ambientales actuales, es necesario avanzar hacia modelos de desarrollo más resilientes. EMASLSA, dentro del Grupo SAUR se compromete a aportar su experiencia y valores para proporcionar un mejor acceso a agua de calidad.
- El suministro de agua para Consumo Humano es un servicio de alta críticidad (NIS 2); esta capacidad es necesaria para mantener la confianza de los ciudadanos en las instituciones y en los servicios públicos.
- El Sistema de Información (IS) está en el corazón de nuestras actividades. Proporciona un soporte esencial a nuestros procesos de negocio. La evolución actual de las restricciones ambientales, los requisitos normativos, las expectativas sociales y la organización del trabajo aumentan la necesidad de protección, resiliencia y calidad de la información: **debemos defender el agua en la era cibernética.**
- Estos cambios requieren mitigar diferentes tipos de riesgos: riesgos financieros, riesgos operativos y en nuestro SGSI especialmente los riesgos cibernéticos. Es por eso que cada usuario de los Sistemas de Información de EMALSA debe contribuir a su protección.
- Este documento establece principios de alto nivel y pautas en cuanto a la implementación de ciberseguridad dentro de EMALSA. Es aplicable a todos los participantes de la cadena de valor del agua: clientes, empleados, contratistas, socios.

Datos de entrada

EMALSA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada, o los servicios prestados.
Se adoptan los principios básicos del Esquema Nacional de Seguridad nivel ALTO, que tienen por objeto asegurar que una organización podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

1. Seguridad integral.
2. Gestión de riesgos.
3. Prevención, reacción y recuperación.
4. Líneas de defensa.
5. Reevaluación periódica.
6. Función diferenciada.

OBJETIVOS:

Para poder cumplir con estos compromisos, la empresa establece anualmente (aprovechando la revisión y análisis del Sistema de Gestión por la Dirección, así como el análisis de Riesgos/Oportunidades con las partes interesadas y los procesos), una serie de objetivos y metas de Seguridad de la Información (SGSI), relacionados de forma directa con nuestro compromiso de seguridad de la información, que pueden tener carácter cualitativo o cuantitativo, pero en cualquier caso, deben ser verificables en cuanto a cumplimiento y efectividad.

La Subdirección de Transformación Tecnológica, evalúa el avance en la consecución de estos objetivos cuando efectúa la revisión periódica del Sistema Integrado de Gestión.

Dentro de las Políticas de Seguridad de la Información, **EMALSA** está preparado para prevenir, detectar, reaccionar y recuperarse de incidentes.

MARCO REGULATORIO:

El SGSI de **EMALSA** y de forma específica para el ENS, contempla el marco regulatorio que afecta a las actividades desarrolladas por la actividad, y de forma específica, integra los criterios de:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- 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.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Leyes de Propiedad Industrial, que protegen marcas y nombres comerciales, patentes y modelos de utilidad.
- Real Decreto Legislativo 1/1996, de 12 de abril, que regula los derechos relativos a las creaciones de software.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, (NIS 2)
- Así como las Guías CCN-STIC (Serie 800).

Proceso

PRINCIPIOS DE ESTA POLÍTICA:

La política de seguridad de la información integra un conjunto de directrices que rigen la forma en que **EMALSA** gestiona y protege la información que trata y los servicios que presta, estando preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

PREVENCIÓN

EMALSA evita que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se cuenta con la Subdirección de Transformación Tecnológica. que entres sus funciones tiene como herramientas y objetivos:

- Proteger la información y los sistemas de la organización de las amenazas y vulnerabilidades de seguridad.
- Detectar y responder a los incidentes de seguridad de manera oportuna y eficaz, previo análisis de las causas.

- Mejorar continuamente la seguridad de la organización.

Así como un conjunto de controles adicionales identificados a través de la evaluación de amenazas y riesgos en revisión continua. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **EMALSA**:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa 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.

DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios monitorizan las operaciones de manera continua para detectar anomalías en los niveles de prestación de los mismos y actuar en consecuencia según lo establecido.

Están establecidos mecanismos de detección, análisis y reporte, que llegan a los responsables de los sistemas regularmente y se actúa cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

RESPUESTA

Se dispone de mecanismos para responder eficazmente a los incidentes de seguridad.

El punto de contacto para las comunicaciones con respecto a incidentes es dmacho@emalsa.es. El protocolo para el intercambio de información relacionada con el incidente, se establece por medio del proceso de gestión de NO CONFORMIDADES e INCIDENTES del SGSI. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CCCN-CERT), según el Proceso de comunicaciones.

RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, **EMALSA** dispone de planes de continuidad de los sistemas TIC, como parte de su plan general de continuidad de negocio y actividades de recuperación; según el Plan de CONTINUIDAD del negocio.

Así mismo se establecen un conjunto de políticas:

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que esté coordinada e integrada con el resto de iniciativas estratégicas para conformar un todo coherente y eficaz; integrado con las normas ISO y el Esquema Nacional de Seguridad.
- Responsabilidad diferenciada: Los sistemas de información diferencian el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- Seguridad integral: La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
- Gestión de Riesgos: El análisis y gestión de riesgos es parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación es proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información es atendida, revisada y auditada por personal cualificado, instruido y dedicado, liderado por la Subdirección de Transformación Tecnológica de EMALSA.
- Seguridad por defecto: Los sistemas se diseñan y configuran de forma que garanticen un grado suficiente de seguridad por defecto, incluyendo los servicios en la nube.

- La estructura de la documentación del SGI se gestiona y mantienen en vigor por la dirección en Qualitas CLOUD, a la cual tienen acceso todos los miembros del área de Transformación Tecnológica.

Políticas específicas y responsabilidades.

Estas políticas se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información acorde al ENS y el RD 311/2022 que regula el ENS, que inspiran las actuaciones de **EMALSA**.

1.- Protección de datos de carácter personal: **EMALSA** adopta las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal, cumpliendo el RGPD.

2.- Gestión de activos de información: Los activos de información de **EMALSA** están inventariados y categorizados y están asociados a un responsable.

3.- Seguridad ligada a las personas: se tienen implantados los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

4.- Seguridad física: Los activos de información están emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas están suficientemente protegidos frente a amenazas físicas o ambientales.

5.- Seguridad en la gestión de comunicaciones y operaciones: se tienen establecidos los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmite a través de redes de comunicaciones está adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garantizan su seguridad.

6.- Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, queda registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a las actividades de **EMALSA**.

7.- Adquisición y mantenimiento de los sistemas de información: se contemplan los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

8.- Gestión de los incidentes de seguridad: se dispone de los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

9.- Gestión de la continuidad: se dispone de los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

10.- Cumplimiento: se adoptan las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

Asegurando el cumplimiento de los requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

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

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

ORGANIZACIÓN DE LA SEGURIDAD:

EMALSA establece un conjunto de roles y funciones para la gestión de la seguridad de la información, que está establecido en su Manual de Funciones y Organigrama, compuesto por:

- **El Comité de Dirección y de Seguridad de la Información que ejerce las funciones de**:

a) Aprobar las propuestas de modificación y actualización permanente que se hagan sobre los procesos de seguridad de la información.

b) Cooperar en la definición de procesos, IT y normativa de seguridad para su aprobación por parte de la Subdirección de Transformación Tecnológica.

c) Velar e impulsar el cumplimiento de los PSI y su desarrollo normativo.

d) Promover la mejora continua en la gestión de la seguridad de la información.

e) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

El CDSI se reunirá con carácter ordinario al menos semestralmente y con carácter extraordinario cuando lo decida la Subdirección de Transformación Tecnológica de EMALSA.

El CDSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Los principales roles y funciones de seguridad se establecen en:

- **Responsable de seguridad:** Subdirección de Transformación Tecnológica.
- **Responsable de los sistemas**: Responsable del área de Sistemas.
- **Responsable de los servicios:** Técnico del área de Desarrollo.
- **Responsable de la información:** Responsable del área de Soporte.

El Comité de seguridad de la información cuenta con el apoyo del DPD y del equipo de responsables técnicos de las diversas áreas.

la Subdirección de Transformación Tecnológica de **EMALSA** designa estas responsabilidades, en el Manual de Funciones y Organigrama, y los 4 roles principales aceptan en acta dicho nombramiento y sus responsabilidades.

ESTRUCTURA DOCUMENTACIÓN SEGURIDAD:

El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollara? en niveles, según el ámbito de aplicación y el nivel de detalle técnico. Dichos niveles de desarrollo son los siguientes:

- Políticas de seguridad de la información, constituido por el presente documento y el manual de gestión de la Seguridad de la Información y el Proceso de Gestión de Seguridad de la Información.
- Procesos operativos, e instrucciones técnicas, que describen explícitamente el objeto, el proceso de las actividades para la seguridad de la información y los activos; las herramientas de gestión del SGSI en el que se soportan, indicadores y sistemas de control.
- Así como políticas y normativa de obligado cumplimiento, asociado a los diversos ámbitos de la actividad, incluido el tratamiento asociado a tipologías de incidente.

DATOS DE CARÁCTER PERSONAL:

EMALSA, trata los datos de carácter personal. Y establece en los documentos de información a empleados y subcontratas, los cuales firma, el tratamiento a la información a la que tendrán acceso autorizado y recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de **EMALSA**, se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

GESTIÓN DE LOS RIESGOS:

EMALSA, dispone de un proceso con los criterios de categorización de riesgos, su correspondiente plan de tratamiento de riesgos y la matriz de riesgos del SGSI; que Integrar los resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos para la Revisión por la Dirección; Formular el Plan de Tratamiento de los riesgos del SGSI; La aprobación y aceptación del plan de tratamiento de riesgos residuales del SGSI y la aceptación por parte de los dueños de los riesgos; e Implementación del Plan de Tratamiento de los Riesgos.

OBLIGACIONES DEL PERSONAL:

Dentro de las políticas de seguridad de la información, y los procesos, **EMALSA** establece para todos los miembros de la organización la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de

Seguridad, siendo responsabilidad del Comité de Seguridad, disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **EMALSA** atenderán las sesiones y medidas de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros y en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas reciben 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. Así mismo se les forma e informa para la notificación y gestión de incidentes, así como el mínimo privilegio en los accesos. Así mismo se les informa el conjunto de normativa y criterios de confidencialidad y uso adecuado de los activos a los que tienen acceso.

TERCERAS PARTES:

Cuando **EMALSA** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecen canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecen procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **EMALSA** utilice servicios de terceros o 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. 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. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

MEJORA CONTINUA:

Uno de los principios fundamentales de **EMALSA** es mejorar continuamente la eficacia del sistema integrado de gestión según las normas: ISO 27001 y ENS, la toma de medidas para la mejora continua de las medidas de seguridad, facilitando la participación en las decisiones que les afecta, así como el derecho a ser consultados, la mejora continua de las medidas para garantizar la seguridad de la información en base al SGSI y el ENS.

Para ello se considera entro otros:

- Analizar y maximizar la satisfacción de los clientes y usuarios con nuestras soluciones y servicios.
- Nuestra continua orientación hacia la excelencia está fundamentada en una temprana identificación y erradicación de las fuentes de los errores. La prevención y anticipación es prioritaria frente a la corrección.
- Lograr la motivación de nuestros recursos humanos, su capacitación, cualificación y experiencia, a través de las actividades apropiadas de selección, formación y adiestramiento.
- Establecer y mantener los cauces de comunicación e información permanente con nuestros clientes, empleados, proveedores y sociedad en general.

Salida de datos

Subdirección de Transformación Tecnológica.
Daniel Macho González