CLECE Y FILIALES

SEGURIDAD DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD

Aprobado: Director General

Fecha: mayo 2026

CONTROL DE MODIFICACIONES

Revisión	Motivo
01 Noviembre 2022	Versión Inicial
02 Marzo 2025	Cambio de formato. Reorganización de capítulos. Adaptación a política del grupo.
02 Mayo 2026	Adaptación a directrices guía CCN-STIC 805 en los siguientes capítulos: marco legal y regulatorio (cap5) gestión documental (cap9) gestión de riesgos (cap11). Gestión del personal (cap13) gestión de incidentes (cap23), seguridad en la cadena de suministro (cap27), Seguimiento y revisión (cap30)

ÍNDICE

1 INTRODUCCIÓN

La Política de Seguridad establece las directrices y principios establecidos por Clece S.A. y filiales (en adelante, Clece) para garantizar la protección de la información, así como el cumplimiento de los objetivos de seguridad definidos, asegurando así la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los sistemas de información y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

La dirección de Clece, consciente de la importancia de la seguridad de la información en el ámbito laboral, asume y dispone los siguientes compromisos con respecto al Esquema Nacional de Seguridad (en adelante, ENS):

- Asegurar que los requisitos de seguridad se integran en los procesos de la organización.
- Asegurar los recursos necesarios para operar la seguridad de la organización.
- Dirigir y apoyar a las personas, para contribuir a la eficacia del esquema nacional de seguridad.
- Promover la mejora continua.

Para ello, la dirección asegurará que el personal de Clece cumple con las normativas, políticas, procedimientos e instrucciones relativas a la seguridad.

Mediante el desarrollo e implementación de la Seguridad de la Información, Clece pretende garantizar los siguientes objetivos de seguridad:

- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Cumplir todos los requisitos legales aplicables.
- Todos los empleados son informados de sus funciones y obligaciones de seguridad y son responsables de cumplirlas.
- Gestionar adecuadamente todas las incidencias ocurridas.
- Formar y concienciar a todos los empleados en materia de seguridad.
- Mejorar de forma continua el Sistema de Gestión de Seguridad de la Información (SGSI) y, por ende, la seguridad de la información de la organización.

2 OBJETO

El presente documento tiene por objeto establecer la política de seguridad para Clece en base a los requisitos dispuestos en el ENS, asegurando así la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los sistemas de información de la compañía y por

supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables y minimizando los riesgos y ciberamenazas a los que están expuestos las redes y sistemas de información de Clece, de manera que permitan cumplir su objeto social para con los clientes y otros grupos de interés, y por tanto garantizando la continuidad de la prestación de los servicios actuando preventivamente, supervisando la actividad diaria y reaccionando con diligencia a los Incidentes.

3 ÁMBITO DE APLICACIÓN

La política de seguridad será de obligado cumplimiento para todos los usuarios de los sistemas de Clece y aplicable a los activos empleados para prestar los servicios, afectando a la información tratada.

Será de obligado cumplimiento para todo el personal, proveedores y clientes que accedan tanto a los sistemas de información como a la propia información que sea gestionada por la compañía, con independencia de cuál sea su destino, adscripción o relación con el mismo.

4 MISIÓN Y OBJETIVOS

La misión, visión y los valores de Clece son la base sobre la que trabajamos cada día y que nos permite llegar a ser un referente de calidad realizando una gestión eficiente y profesional de los servicios, al tiempo que nos permite impulsar, través de nuestro Proyecto Social, la inclusión de colectivos socialmente vulnerables. Todo ello, manteniendo la transparencia y el cumplimiento legal en la gestión de nuestras actividades y servicios.

MISION

- Gestión eficiente y profesional de los servicios, buscando una rentabilidad sostenible.
- Impulsar a través de nuestro Proyecto Social, la inclusión de colectivos socialmente vulnerables como personas en riesgo de exclusión social, personas con diversidad funcional, víctimas de violencia de género y jóvenes en desempleo.

VISION

Trabajamos para:

- Ser líderes del sector y un referente de calidad en el ámbito de la prestación de servicios.
- Tener presente la innovación como elemento diferenciador en el mercado.
- Contar con equipos interdisciplinares capaces de dar respuesta a las necesidades de los usuarios.

- Mejorar la calidad de vida de los colectivos más sensibles de nuestra sociedad: mayores, niños, personas con discapacidad y personas en riesgo de exclusión social.

VALORES

- Promover el respeto y dignidad de las personas a las que prestamos algún tipo de atención social.
- Transparencia y cumplimiento legal en la gestión de nuestras actividades y servicios.
- Velar por la confidencialidad de los datos personales de nuestros clientes y usuarios.
- Trabajar en equipo, con profesionalidad y motivación que nos permita mejorar cada día.
- Velar por la Seguridad y Salud de nuestros Trabajadores.
- Fomentar el respeto y preservación de nuestro medio ambiente.

5 MARCO LEGAL Y REGULATORIO

Clece en conformidad con el ENS y el SGSI, tendrá en cuenta los requerimientos dispuestos por el marco legal aplicable y regulatorio en el que se desarrollan las actividades.

Identificando los siguientes reglamentos y normativas principales:

- **RGPD Y LOPDGDD**: Reglamento (UE) 2016/679 de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.
- **ENS**: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que constituye los principios básicos y requisitos mínimos que permitan una protección adecuada de la información y **guías CCN-STIC** aplicables (801, 805, etc.)
- **NIS2:** 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.
- **Reglamento de Inteligencia Artificial:** Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial

Si bien, todos los requisitos de seguridad aplicables en la organización se detallan en el documento correspondiente del sistema de gestión.

6 PRINCIPIOS DE SEGURIDAD

Se establecerán las siguientes directrices fundamentales de seguridad, las cuales ayudarán a evitar comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los servicios e información asociada.

Estableciéndose los siguientes principios:

1. **Proceso integral**. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información, 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. Asegurándose de promover conocimiento y concienciación en Seguridad de la Información entre sus empleados.
2. **Gestión de la seguridad basada en Riesgos**. Se desarrolla el estudio, el establecimiento de la metodología con los criterios, el análisis y la evaluación de los riesgos que puedan poner en peligro la seguridad de la información. Así mismo, se aplicarán las medidas necesarias para mitigar estos riesgos en base a su criticidad realizando evaluaciones periódicas que permitan obtener el estado de la gestión del tratamiento del riesgo y principalmente tras incidentes de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables.
3. **Definición, desarrollo y mantenimiento**: para lograr la puesta en marcha de los objetivos, valores, estrategia y compromisos asumidos, Clece impulsará el desarrollo de un Sistema de Gestión integrado por los controles técnicos, legales y de gestión de la seguridad de la información necesarios para garantizar en todo momento el cumplimiento de los requisitos legales, reglamentarios y contractuales en la materia que le sean de aplicación.
4. **Promoción de una cultura de seguridad de la información**: Clece se compromete a promover de forma activa una cultura de seguridad de la información entre todos sus profesionales, y usuarios, ya sea internamente, o entre sus clientes y proveedores.
5. **Prevención, detección, respuesta y conservación**. La seguridad del sistema contemplará aspectos de prevención, detección y respuesta, para conseguir que las amenazas no afecten a la información y los servicios que se prestan. Para ello, se implantarán medidas de seguridad que limiten la exposición, de prevención de las amenazas y vulnerabilidades, de detección de incidencias, de restauración de la información y servicios, la conservación de los datos, y el mantenimiento de la disponibilidad de los servicios.
6. **Líneas de defensa**. El sistema dispondrá de una estrategia de protección constituida por varias capas de seguridad organizativas, lógicas y físicas, de forma que cuando

una de ellas se vea comprometida, se ofrezca una respuesta para reducir el impacto en cuanto a su alcance y a su duración.

7. **Gestión diaria**: lo cual implica el compromiso de Clece de proteger la seguridad de la información, de las redes y Sistemas de Información, diseñando medidas de seguridad robustas, alineadas con las necesidades de las diferentes partes interesadas, así como de la normativa vigente aplicable en la materia, para lo cual Clece aprobará las políticas y/o procedimientos específicos por materia que desarrollarán los principios y requisitos básicos de seguridad de la información establecidos en la presente Política.
8. **Protección proactiva**: de manera que se persiga proactivamente la salvaguarda de los niveles establecidos de confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad parar sus activos de información y asegurar la Resiliencia Operativa Digital de Clece.
9. **Vigilancia continua y revaluación periódica**. La vigilancia permitirá la detección de actividad anómala y poder proceder a su correspondiente respuesta. Se realizará una evaluación periódica de las medidas de seguridad para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, realizando auditorías y marcándose objetivos como compromiso de mejora continua del sistema.
10. **Diferenciación de responsabilidades**. En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del sistema, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema; el responsable del servicio, que determinará los requisitos de los servicios prestados y el Responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
11. **Mejora continua**: entendiendo la seguridad de la información como un eje transversal integrado en todas las áreas y procesos de negocio, buscando lograr un progreso ininterrumpido de todos los procesos vinculados al SGSI y a la gestión de la seguridad de la información, de las redes y de los Sistemas de Información, de tal forma que contribuya a que toda la operativa de Clece sea digitalmente resiliente.

7 GOBERNANZA, ORGANIZACIÓN E IMPLEMENTACIÓN DEL PROCESO DE SEGURIDAD

La gobernanza de la seguridad de la Información en Clece es esencial para gestionar y mitigar potenciales riesgos, para garantizar la toma de decisiones en función del riesgo real de la materialización de las amenazas sobre la organización, así como para la continuidad de las operaciones de negocio, siendo la presente Política una herramienta fundamental para la adecuada gestión y gobernanza de la seguridad de la información.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

Corresponde al Consejo de Administración de Clece, a través de la presente Política y, en su caso, de otras normas corporativas en desarrollo de ésta, el establecimiento de la estrategia y directrices de gestión con proyección sobre Clece en materia de seguridad de la Información.

A su vez, es competencia de la Función de Auditoría Interna a través de sus funciones de supervisión y control, velar por la implementación y desarrollo de la presente Política y de las medidas adoptadas en aplicación de esta, así como revisar, y en su caso, proponer a la Dirección la actualización de la presente Política.

Asimismo, corresponde a la Función de Auditoría Interna la supervisión de la eficacia del SGSI de Clece.

Para el ejercicio de sus funciones de supervisión, la Función de Auditoría Interna recibirá periódicamente del Responsable de seguridad información sobre su gestión.

La responsabilidad de la seguridad de la información recae, en última instancia, en la Dirección General de la compañía.

La Dirección General es responsable de asignar las funciones y responsabilidades a los roles identificados en la presente política, aprobar la política de seguridad y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La Dirección General establece una serie de roles y responsabilidades en materia de seguridad y gestión de los servicios, desarrollados en el siguiente epígrafe.

8 ROLES Y RESPONSABILIDADES

Responsable de la información.

El Responsable de la Información tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Se asigna al Responsable de la Información la potestad de establecer los requisitos de la información en materia de seguridad o, la potestad de determinar los niveles de seguridad de la información.

Realizará la valoración de la información utilizada en la prestación de los servicios, según los criterios de valoración sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares, establecidos en el sistema.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

La persona designada como responsable de información consta en el correspondiente documento de nombramiento.

Responsable del servicio.

Se asigna al Responsable del Servicio la potestad de establecer los requisitos del servicio en materia de seguridad o la potestad de determinar los niveles de seguridad de los servicios.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

Realizará la valoración del servicio, según los criterios de valoración sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares, establecidos en el sistema.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.

En cuanto al RGPD, por delegación del Responsable del tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto.

La persona designada como Responsable de servicio consta en el correspondiente documento de nombramiento.

Responsable de seguridad.

Sus responsabilidades son las siguientes:

- Mantener y gestionar la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad, alineado con los objetivos de la empresa.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Y sus tareas:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.

- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella. Interlocución con otras empresas, instituciones, reguladores y Fuerzas y Cuerpos de Seguridad del Estado en materia de seguridad de la información.
- Determinación de la categoría del sistema.
- Realización del Análisis y Gestionar los riesgos de seguridad de la información y establecer el plan de acción correspondiente.
- Gestionar los incidentes de seguridad, sea directa, a través de servicios externalizados o a través de otras áreas de la organización.
- Elaborar la normativa de seguridad.
- Aprobar los procedimientos operativos de seguridad.
- En colaboración con el Responsable de Sistemas, gestionar la parte de seguridad en los procesos de adquisición, uso, gestión y finalización de los servicios en la nube.
- Desarrollar la gestión de la continuidad de negocio
- Reportar al comité el estado de la seguridad del sistema.
- Elaborar junto al responsable de sistemas los planes de mejora de la seguridad.
- Elaborar los planes de concienciación y formación.
- Supervisar el cumplimiento de la legislación en los aspectos referidos a su ámbito de actuación.
- Interlocución con la Alta Dirección en materia de seguridad de la información (métricas, reporte de riesgos, planes de acción, amenazas e incidencias)
- Seguimiento y cumplimiento de los planes de formación en materia de Seguridad de la Información.
- Coordinación de la obtención de certificaciones en materia de Seguridad de la Información.
- Velar por que el uso, desarrollo y contratación de sistemas de inteligencia artificial se realice conforme a la Política de IA, al Reglamento Europeo de IA y al resto de normativa aplicable.
- Supervisar los riesgos legales, éticos, de seguridad y de privacidad asociados a los sistemas de IA utilizados por la organización.
- Validar, desde el punto de vista de seguridad de la información y cumplimiento normativo, la incorporación de nuevas herramientas o soluciones basadas en IA.

La persona designada como Responsable de seguridad consta en el correspondiente documento de nombramiento.

Responsable del sistema.

Sus responsabilidades son:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo, para cubrir las necesidades de la Compañía y de sus usuarios.
- 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 tratamiento 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 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 del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de seguridad de la Información.
- En colaboración con el Responsable de Seguridad, gestionar la parte de seguridad en los procesos de adquisición, uso, gestión y finalización de los servicios en la nube.
- 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.
- Propondrá 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) al Responsable de Seguridad de la Información para su aprobación.
- Control de los programas de licenciamiento de las aplicaciones corporativas.
- Cooperar en el diseño de planes de formación en materia de tecnologías de la información y supervisar su implementación.
- Garantizar que los sistemas de información que incorporen inteligencia artificial se diseñen, implanten y operen de forma segura, controlada y alineada con la Política de IA.

- Asegurar la correcta integración técnica de los sistemas de IA en el entorno tecnológico corporativo durante todo su ciclo de vida.

La persona designada como responsable de sistema consta en el correspondiente documento de nombramiento.

Estructura y responsabilidades segregadas y resolución de conflictos.

El artículo 11 del Esquema Nacional de Seguridad recoge el principio de "Diferenciación de responsabilidades". Este principio exige que el Responsable de la Seguridad sea independiente del Responsable del Sistema, asimismo, exige que la responsabilidad de seguridad esté separada de la responsabilidad sobre explotación de los sistemas. Clece ha separado los roles en diferentes personas, no obstante, en caso de conflicto este deberá ser resuelto por el Comité de Seguridad.

La estructura creada en Clece contempla las siguientes responsabilidades:

- Responsabilidades derivadas del tratamiento de datos de carácter personal.
- Responsables de Información, para todas las informaciones manejadas por los servicios prestados dentro del marco de las leyes que puedan resultar de aplicación.
- Responsables de Servicios, para todos los servicios prestados dentro del marco de las leyes que puedan resultar de aplicación.
- Supervisión: una figura, reportando a Dirección, y desarrollando la función de Responsable de la Seguridad.
- Operación: una figura, reportando a Dirección, e integrando las siguientes funciones de Responsable del Sistema y Administrador de Seguridad.

El Responsable de seguridad se asegura de que estos roles son comunicados y aceptados por las personas correspondientes y que éstos han entendido sus funciones y obligaciones para con la organización en materia de seguridad y gestión del servicio.

Comité de seguridad.

Funciones:

- Verificación del cumplimiento de las políticas de seguridad de la información.
- Conocer y revisar el resultado de las auditorías del sistema, así como las incidencias relevantes de seguridad de la información.
- Adoptar las medidas necesarias para que el personal conozca los procedimientos en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Asegurarse de que se han identificado las necesidades de seguridad de la información y que se han integrado en los procesos relevantes de la organización de manera correcta.

- Facilitar todos los recursos necesarios para llevar a cabo la Seguridad de la Información.
- Resolución de conflictos de funciones, obligaciones, segregación y toma de decisiones que se puedan dar.
- El Comité reportará a Dirección todos los asuntos de especial relevancia que sean tratados. Igualmente, se informará a las áreas de la organización que se vean afectadas en la toma de decisiones.

Obligaciones:

Estar concienciados en Seguridad de la Información y conocer los riesgos de la organización que pudieran ponerla en peligro.

- Conocer la normativa interna en materia de seguridad.
- Conocer las consecuencias que se pueden derivar y las responsabilidades en que se pudiera incurrir en caso de incumplimiento de la normativa.

Requisitos:

- La composición del Comité está realizada con el fin de tener una completa visión de los servicios integrados en el alcance.
- El Comité se reunirá tantas veces como lo designen sus integrantes, pero al menos se deberá reunir dos veces al año, de manera ordinaria. En caso de que el Comité lo considere oportuno y debido a circunstancias que así lo requieran, se podrán convocar reuniones extraordinarias.
- El Comité invitará a personal de las áreas de la organización que vayan a ser relevantes en los temas tratados.
- El DPD se considera un órgano consultivo del Comité para todas las cuestiones relacionadas con datos de carácter personal.
- Las conclusiones acordadas en las reuniones del Comité quedarán registradas en un acta, la cual debe ser firmada por todos los integrantes y guardada como evidencia de la asistencia y registro del funcionamiento de este.

Integrantes del Comité:

- Responsable de seguridad.
- Responsable de Sistemas.
- Responsables de Servicio.
- Responsables de información.

Procedimiento de designación.

Todos los roles serán nombrados por la Dirección o representación de la esta y aceptados por las personas designadas. El nombramiento se podrá revisar cuando la Dirección estime necesario o cuando el puesto quede vacante.

Sustituciones y suplencias.

Clece dispondrá de un mecanismo de sustitución temporal de los responsables designados (Responsable de la Información, del Servicio, de Seguridad y del Sistema) para cubrir ausencias de larga duración o ausencias puntuales que puedan afectar a la eficacia de sus funciones. La activación de la suplencia se documentará (p. ej., acta/comunicación interna) e incluirá: responsable suplente, alcance de la suplencia, fecha de inicio y fin.

Para todos los casos será la Dirección de Clece el órgano competente para la designación de la suplencia, pudiendo ser adicionalmente en los casos de los responsables de Servicio o Información, lo dirección operativa competente para cada servicio.

9 GESTIÓN DOCUMENTAL

Clece, en cumplimiento de los requerimientos del ENS, es partícipe de una gestión documentada de creación, actualización y control de la documentación de seguridad. Dicha gestión se estructura mediante a) La presente Política, (b) Normativa de Seguridad (obligatorias), (c) Procedimientos operativos de seguridad, y (d) Guías/Guías de apoyo o instrucciones técnicas específicas.

La documentación se gestiona bajo control de versiones, con responsables de custodia definidos y repositorio corporativo único, asegurando su disponibilidad para quienes necesiten conocerla según su rol, y aplicando controles de acceso acordes a su sensibilidad.

Adicionalmente, se permiten repositorios departamentales para facilitar su acceso y distribución.

10 REQUERIMIENTOS DE SEGURIDAD DESDE EL DISEÑO Y POR DEFECTO

Todos los sistemas, aplicaciones y servicios deben incorporar medidas de seguridad desde su concepción, garantizando que los controles de protección sean inherentes y no opcionales. La evaluación debe realizarse en las fases iniciales de desarrollo y adquisición, estableciendo controles que minimicen vulnerabilidades y aseguren el cumplimiento normativo.

Los sistemas deben desplegarse con los parámetros de seguridad más restrictivos y ajustarse solo cuando sea estrictamente necesario, evitando configuraciones predeterminadas inseguras.

11 ANÁLISIS Y GESTIÓN DE RIESGOS

Clece realizará un análisis de riesgos de todos los sistemas de información sujetos a esta política que soportan los servicios y la información tratada en ellos, conforme a la metodología previamente establecida.

Umbral y aceptación del riesgo residual.

Clece establecerá un umbral corporativo de riesgo asumible y un proceso de aceptación del riesgo residual. La aceptación del riesgo residual requerirá autorización explícita del responsable de Seguridad y se comunicará el resto de Responsable del Servicio, Información, y Sistema la cual quedará registrada como evidencia.

Se revisará el resultado del análisis para gestionar, como mínimo, aquellos riesgos que estén por encima de un nivel de riesgo aceptable (NRA) definido y adoptar las medidas de control que correspondan para proceder a su mitigación.

Periodicidad y disparadores de reevaluación.

El análisis de riesgos se revisará, al menos, con periodicidad anual y siempre que concurra alguno de los siguientes supuestos: (i) cambios relevantes en la información manejada; (ii) cambios relevantes en los servicios prestados o en la arquitectura/tecnología; (iii) incidente grave de seguridad; (iv) reporte de vulnerabilidades graves; (v) cambios relevantes en las evaluaciones de impacto/gestión de riesgos de protección de datos.

12 RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE LOS DATOS PERSONALES

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. El Registro de Actividades del Tratamiento detalla los tratamientos afectados y los responsables correspondientes.

Clece tiene establecida una metodología de análisis de riesgo y evaluación de impacto que se aplica a todos los tratamientos de datos personales, gestionando los riesgos residuales obtenidos.

13 GESTIÓN DEL PERSONAL

Todo el personal implicado en el SGSI contará con la formación necesaria para desempeñar adecuadamente sus funciones. Cuando se detecten carencias o necesidades formativas, se planificará y ejecutará la formación correspondiente para subsanarlas.

Asimismo, el personal que participe en la prestación de los servicios y asuma responsabilidades en materia de seguridad de la información deberá estar concienciado sobre su importancia y conocer la normativa de seguridad aplicable.

Para ello, se implantará un programa de concienciación continua así como una formación específica para nuevas incorporaciones (onboarding).

Se comprobará que el personal con funciones de uso, operación o administración de sistemas cuente o, en su defecto, reciba formación específica antes de asumir nuevas responsabilidades.

14 PROFESIONALIDAD

Todas las actividades relacionadas con la seguridad de los sistemas están atendidas, revisadas y auditadas por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento. Este mismo principio se aplicará a las entidades prestadoras de servicios.

15 AUTORIZACIÓN Y CONTROL DE ACCESOS

Se controlará el acceso a los sistemas de información de Clece para que sólo sea realizado por personal autorizado y en las condiciones de seguridad que la organización haya decidido operar. Se asegurarán los accesos a los usuarios autorizados y se prevendrá el acceso a los no autorizados.

16 PROTECCIÓN DE LAS INSTALACIONES

Se prevendrá todo tipo de acceso físico no autorizado, daños o intromisiones en las instalaciones y en la información de Clece.

Se tomarán las medidas de seguridad necesarias para evitar pérdidas, daños, robos o circunstancias que pongan en peligro los activos o que puedan provocar la interrupción de las actividades.

17 ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS

Clece valorará positivamente la adquisición de productos de seguridad cuya funcionalidad esté certificada, así como de servicios de seguridad de empresas certificadas. Esta certificación deberá estar de acuerdo con las normas y estándares reconocidos internacionalmente, en el ámbito de la seguridad de la información, pero principalmente se considerará la conformidad con el ENS en el nivel de categorización que tiene Clece.

18 MÍNIMO PRIVILEGIO

Los sistemas se configuran de tal forma que:

- Proporcionen la mínima funcionalidad requerida para que la organización alcance sus objetivos y ninguna función adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos autorizados, poniendo si fuera necesario restricciones de horarios y puntos de accesos facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funcionalidades innecesarias o que no sean de interés.
- 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.

19 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Todos los elementos físicos o lógicos de Clece requieren una autorización formal previa a la instalación en el sistema.

Se deberá conocer en todo momento el estado de la seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de la seguridad de estos.

20 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Clece presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, móviles o tablets, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Clece considera como parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos.

La documentación en papel deberá estar protegida aplicando las medidas de seguridad que correspondan para garantizar su adecuada protección y conservación en todo su ciclo de vida.

21 PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se protegerá el perímetro, especialmente si la conexión se produce desde o hacia redes públicas.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

22 REGISTROS DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Clece registrará las actividades de los usuarios, siempre cumpliendo exhaustivamente la legislación aplicable en cada caso, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Igualmente, cumpliendo rigurosamente la legislación aplicable, se podrá 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 poder exigir responsabilidades, cada usuario que accede a los sistemas de información deberá estar identificado de forma única, de modo que se pueda determinar quién ha realizado una determinada actividad.

23 INCIDENTES DE SEGURIDAD

Las áreas que conforman Clece deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por Incidentes de ciberseguridad. Para ello, se aplicarán las medidas mínimas de seguridad determinadas por la normativa aplicable, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Toda incidencia en materia de seguridad deberá comunicarse por defecto al Centro de Atención al Usuario (CAU), y, en caso de considerarse necesario, al Responsable de seguridad para su gestión y coordinación con los procedimientos y obligaciones aplicables (p. ej., protección de datos), incluyendo la comunicación a las autoridades u organismos competentes sin dilaciones indebidas cuando resulte necesario

Una vez recibida, se seguirá el procedimiento que establece una gestión completa de las incidencias de seguridad con mecanismos de detección, análisis, clasificación, resolución, registro y comunicación a las partes interesadas.

24 CONTINUIDAD DE LA ACTIVIDAD

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

25 AUDITORÍAS DE SEGURIDAD Y GESTIÓN DE VULNERABILIDADES.

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá adoptar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección

de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

26 MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

El proceso integral de seguridad 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 las tecnologías de la información.

27 SEGURIDAD EN LA CADENA DE SUMINISTRO

Todos los terceros con acceso a información o sistemas críticos deben someterse a una evaluación de riesgos de seguridad antes de su contratación, verificando las certificaciones que dispongan.

Los acuerdos con proveedores deben incluir cláusulas específicas de seguridad de la información, cumplimiento normativo y notificación de incidentes para garantizar la protección de los activos.

Se deben implementar mecanismos de monitorización para verificar que los proveedores cumplen con los controles de seguridad exigidos y mitigar posibles vulnerabilidades en la cadena de suministro.

Punto de contacto de seguridad.

En las relaciones con proveedores/prestadores (incluidos servicios en la nube) el Responsable de Seguridad, o la persona en quien delegue, actuará como Punto de Contacto (POC) para coordinar requisitos ENS, intercambio de evidencias, y la gestión y reporte de incidentes con terceros

Evidencias y derecho de verificación.

Los acuerdos con terceros podrán requerir la aportación de evidencias de cumplimiento (p. ej., certificaciones, informes de auditoría, declaraciones de aplicabilidad) y, cuando aplique, auditorías de segunda o tercera parte, o mecanismos equivalentes de verificación.

Excepciones en terceros.

Si un tercero no puede satisfacer algún requisito de seguridad aplicable, el Responsable de Seguridad emitirá un informe de riesgos que describa la desviación, el impacto y las medidas compensatorias. Dicho informe requerirá la aprobación de los responsables de la

información y del servicio afectados antes del inicio o continuación de la contratación, quedando registrada la aceptación del riesgo y los planes de acción que se lleven, en su caso, a cabo.

28 CONFIABILIDAD, SEGURIDAD Y RESILIENCIA

Disponibilidad y continuidad operativa: Los sistemas críticos deben diseñarse y gestionarse para garantizar una alta disponibilidad, con planes de continuidad y recuperación ante desastres que minimicen interrupciones en el servicio.

Protección contra amenazas y vulnerabilidades: Se deben aplicar controles de seguridad robustos, como gestión de parches, monitoreo continuo y protección contra ciberataques, asegurando la integridad y confiabilidad de la información.

Capacidad de respuesta y resiliencia: La organización debe contar con procedimientos para detectar, responder y recuperarse rápidamente ante incidentes de seguridad, reforzando su capacidad de adaptación frente a amenazas emergentes.

29 GESTIÓN DE EXCEPCIONES

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al responsable de la Seguridad de la Información de la sociedad de Clece que corresponda. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

30 SEGUIMIENTO Y REVISIÓN.

El órgano de contacto para cualquier duda y/o consulta en relación con la interpretación y ejecución de la presente Política será el Responsable de seguridad. La comunicación con el Responsable de seguridad se llevará a cabo por los cauces habilitados al efecto.

La presente Política de Seguridad de la Información, será revisada anualmente y aprobada si procede por la dirección quedando registrada su aprobación y las evidencias asociadas. No obstante, si tuvieran lugar cambios relevantes en los sistemas de información o se identificaran cambios significativos en la sociedad o en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión

siempre que se considere necesario, asegurando así que la Política permanece adaptada en todo momento a la realidad de Clece.

La aprobación de esta Política implica que su implantación contará con el apoyo de la Dirección para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos.

El cumplimiento de esta Política será supervisado por el Responsable de seguridad. Se establecerán mecanismos de auditoría y revisión periódica para asegurar que el SGSI cumpla con los estándares establecidos.

En caso de tener algún problema, o detectar un Incidente que pueda afectar al funcionamiento o seguridad de los sistemas de redes y aplicaciones, y/o la seguridad de la información, éste se deberá comunicar inmediatamente al Responsable de seguridad a través de los cauces habilitados a tales efectos y que se determinarán en los procedimientos de SGSI.

La Política se redacta con neutralidad tecnológica, evitando referencias a soluciones concretas, y se mantendrá actualizada para prevenir obsolescencia ante cambios técnicos u organizativos.

El incumplimiento de la presente Política puede conllevar responsabilidades legales de diversa naturaleza según dispone la legislación vigente, dando derecho a Clece, si así se estimara necesario, a iniciar las acciones legales que procedan.

31 DIFUSIÓN

Esta política debe ser conocida y asumida por todas las partes interesadas y deben establecerse los procedimientos necesarios para ello, a través de los canales corporativos de comunicación.

Esta Política se publicará en la página web corporativa de Clece con el consiguiente conocimiento y asunción de su contenido íntegro por parte de los profesionales y usuarios. Sin perjuicio de ello, Clece llevará a cabo periódicamente acciones de comunicación, formación y sensibilización para la comprensión y puesta en práctica de esta Política, así como de sus actualizaciones. Asimismo, se difundirá esta Política entre las partes interesadas de Clece y sus filiales.

En todo caso, es responsabilidad de todos los usuarios y profesionales leer y comprender el contenido de esta Política, así como observar y cumplir sus directrices, principios y procesos en el desarrollo de su trabajo, en la medida en que el desconocimiento de todo o parte de su contenido no exime de su cumplimiento. En este sentido, se recomienda acceder de forma periódica al contenido de esta Política a través de los canales disponibles para una mejor comprensión de ésta.

32 ENTRADA EN VIGOR

Esta política fue aprobada en la fecha de firma (indicada en la portada y marca de agua en el margen del documento) por la Dirección General de Clece.

Esta Política de Seguridad es efectiva desde dicha fecha y hasta que sea actualizada o reemplazada por una nueva.