POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

POL.01

versión 1.1

07.09.2026

USO INTERNO

INDICE DE CONTENIDOS

1. CONTEXTO

La presente **Política de Seguridad de la Información** se formaliza con el objeto de dar cumplimiento a los preceptos legales recogidos en el **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS)**, en el ámbito de la Administración Electrónica.

El **ENS** se constituye como la piedra angular para la definición e implantación del **Marco de Gobierno y Gestión de la Seguridad de la Información** formalizado para las distintas entidades del GRUPO EMERA que son gestoras y explotadoras en España de los Centros Residenciales que existen bajo la marca EMERA (en adelante, **EMERA ESPAÑA**).

La finalidad del **ENS** es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de la identificación e implantación de medidas que permitan garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, otorgando a los ciudadanos y a las Administraciones Públicas, el posible ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El **ENS**, en su **artículo 12**, establece la obligación de disponer de una Política de Seguridad, especificando los principios básicos y los requisitos mínimos que debe cumplir la misma.

Esta Política de Seguridad de la información sigue las pautas, instrucciones e indicaciones consideradas por la **guía CCN-STIC-805** del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

EMERA ESPAÑA hace uso de los sistemas TIC (Tecnologías de la Información y Comunicaciones) para alcanzar los objetivos estratégicos que han sido formalizados por los órganos de gobierno (en adelante, la **Dirección**). En consecuencia, estos sistemas deben ser administrados con diligencia, tomando las medidas de seguridad adecuadas para proteger la información frente a daños accidentales o deliberados.

La información constituye para la práctica totalidad de los procesos de negocio y los servicios prestados por **EMERA ESPAÑA**, el hilo conductor imprescindible para la ejecución de los mismos con garantías de eficiencia y calidad, alcanzando, con ello, el cumplimiento de los objetivos estratégicos formalmente establecidos.

Las **dimensiones principales de seguridad de la información** que deben ser garantizadas en la ejecución de cualquier proceso son:

- **Confidencialidad:** Garantiza que la información solo se encuentra accesible a personas, entidades o procesos autorizados.
- **Integridad:** Garantiza que la información solo se genera, modifica y elimina por personas, entidades o procesos autorizados.
- **Disponibilidad:** Garantiza que la información se encuentra accesible cuando las personas, entidades o procesos autorizados lo precisan.

Por otro lado, se presentan otras dimensiones de seguridad, tales como la **autenticación de las partes**, el **no repudio** o la **trazabilidad** que, de igual forma, deben ser garantizadas cuando el valor de seguridad de la información en el contexto del proceso de negocio o el servicio que esté siendo prestado, así lo precise.

Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el **ENS**, así como realizar un seguimiento continuo de los niveles de prestación de los servicios,

monitorizar las vulnerabilidades alertadas, y preparar una respuesta efectiva a los incidentes para garantizar las dimensiones de seguridad señaladas con anterioridad.

EMERA ESPAÑA debe garantizar que la seguridad es parte integral de cada etapa del ciclo de vida de los sistemas TIC, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición, y las actividades propias de explotación.

La **Política de Seguridad de la Información** se basa en la adopción de principios claros y bien definidos que aseguren el cumplimiento de las directrices estratégicas, los requerimientos legales, así como los contractuales formalizados con terceros y, por tanto, se constituye como el instrumento principal en el que se apoya **EMERA ESPAÑA** para la utilización segura de las tecnologías de la información y comunicaciones.

La normativa (estándares, procedimientos e instrucciones de seguridad) que emane de la **Política de Seguridad de la Información** de **EMERA ESPAÑA** pasará a formar parte de la misma una vez haya sido divulgada, siendo de obligado cumplimiento para la totalidad de los empleados y terceras partes que hagan uso de la información propiedad de **EMERA ESPAÑA**.

La **Dirección** de **EMERA ESPAÑA** asegurará que esta **Política de Seguridad de la Información** es entendida e implantada en todos los centros de trabajo, facilitando los recursos técnicos y humanos necesarios para la consecución de los objetivos definidos en este marco de actuación.

2. OBJETIVOS

La **Política de Seguridad de la Información** queda establecida como el documento de alto nivel que formaliza las distintas directrices de actuación en materia de seguridad adoptadas por **EMERA ESPAÑA**, y que serán desarrolladas en mayor detalle en la correspondiente normativa de seguridad (estándares, procedimientos e instrucciones de seguridad) elaborada a tales efectos.

Bajo esta premisa, por tanto, la **Política de Seguridad de la Información** contempla los siguientes objetivos principales:

- Dar cumplimiento a la normativa legal de aplicación en el ámbito de la seguridad de la información.
- Contribuir a cumplir con la misión y objetivos estratégicos formalizados por **EMERA ESPAÑA**.
- Alinear la seguridad de la información con los requerimientos demandados por los servicios prestados mediante la formalización y ejecución del proceso de análisis y evaluación de los riesgos a los que se encuentran expuestos los distintos activos de información, alcanzando la definición de una estrategia para la mitigación de los riesgos relacionados con el entorno de la seguridad de la información.
- Garantizar la protección adecuada de los distintos activos de información en función del grado de sensibilidad y criticidad alcanzado por los mismos (valor de seguridad de los activos de información según las distintas dimensiones consideradas).
- Facilitar el dimensionamiento de los recursos necesarios para la correcta implantación de las medidas de seguridad de índole técnica y organizativa recogidas en la normativa de seguridad documentada a tales efectos.
- Fomentar el uso de buenas prácticas en materia de seguridad de la información, así como crear una cultura de seguridad en el contexto de la estructura organizativa de **EMERA ESPAÑA**.

- Establecer los mecanismos de revisión, monitorización, auditoría y mejora continua con el objeto de mantener los niveles de seguridad oportunos demandados por los servicios prestados por **EMERA ESPAÑA**.

3. ALCANCE

EMERA ESPAÑA aplicará la presente **Política de Seguridad de la Información** sobre todos aquellos sistemas de información y de comunicaciones que se encuentren relacionados con la prestación de servicios que pudieran afectar el ejercicio de derechos y el cumplimiento de deberes por parte de los ciudadanos, mediante el uso de medios electrónicos, así como con el acceso a la información o al procedimiento administrativo a través de tales medios.

4. MARCO NORMATIVO

La formalización de la **Política de Seguridad de la Información**, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la siguiente normativa legal aplicable a la actividad principal de **EMERA ESPAÑA**:

- Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD – Reglamento General de Protección de Datos), 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.
- Ley Orgánica, 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, Ley 3/2018).
- Ley 34/2002, de 11 de julio, de servicios de sociedad de la información y comercio electrónico.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, que adapta el ordenamiento jurídico español al Reglamento (UE) 910/2014 (también conocido como eIDAS).
- Texto Refundido de la Ley de Propiedad Intelectual, aprobado mediante el Real Decreto Legislativo 1/1996, de 12 de abril de 1996. Esta normativa ha sido modificada por varias leyes, incluyendo la Ley 21/2014, que traspone el contenido de las directivas europeas a la legislación española, y la Ley 2/2019, que incorpora la Directiva 2014/26/UE y la Directiva (UE) 2017/1564.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Y demás disposiciones concordantes y de desarrollo de las mencionadas anteriormente.

5. PRINCIPIOS

Con el objeto de garantizar el cumplimiento de los objetivos de seguridad identificados con anterioridad, la **Política de Seguridad de la Información** formaliza la aplicación de determinados principios de seguridad.

5.1. SEGURIDAD COMO PROCESO INTEGRAL

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información utilizados como soporte para la ejecución de los procesos de negocio. En este sentido, por tanto, todas las actividades de seguridad serán ejecutadas bajo esta perspectiva, evitando cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en la ejecución de los procesos de negocio, y la de los responsables jerárquicos con el objeto de evitar que el desconocimiento, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad de la información.

5.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno de información controlado, minimizando los riesgos hasta niveles aceptables formalizados por la **Dirección**.

La reducción del riesgo hasta tales niveles se alcanzará mediante la aplicación de medidas de seguridad, de forma equilibrada y proporcionada a la naturaleza de la información tratada, los servicios a prestar y los riesgos a los que estén expuestos los distintos activos de información utilizados.

5.3. PREVENCIÓN, DETECCIÓN Y RESPUESTA

La seguridad de la información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades existentes, y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información o los servicios prestados.

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

Las medidas de detección estarán orientadas a la alerta temprana de cualquier escenario de materialización de amenazas.

Las medidas de respuesta, que 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.

5.4. EXISTENCIA DE LÍNEAS DE DEFENSA

Se deberá garantizar que la estrategia de protección queda conformada por múltiples capas de seguridad dispuestas de forma que, cuando una de las capas se vea comprometida, se pueda reaccionar adecuadamente frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que puedan propagarse.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

5.5. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

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

Las medidas de seguridad 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, si fuese necesario.

5.6. DIFERENCIACIÓN DE RESPONSABILIDADES

La responsabilidad de la seguridad de la información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información.

6. REQUISITOS

El desarrollo de la **Política de Seguridad de la Información** deberá permitir el cumplimiento de determinados requisitos de seguridad.

6.1. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

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

6.2. GESTIÓN DE RIESGOS

El proceso de gestión de riesgos estará conformado por las actividades de análisis y tratamiento de los riesgos garantizando la aplicación del principio de proporcionalidad.

6.3. GESTIÓN DE PERSONAL

El personal, propio o ajeno, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro de los activos de información se concretará y plasmará en unas normas de seguridad específicas.

6.4. PROFESIONALIDAD

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

Las entidades terceras que presten servicios de seguridad deberán contar con profesionales cualificados, así como niveles idóneos de gestión y madurez en los servicios prestados.

Se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

6.5. AUTORIZACIÓN Y CONTROL DE ACCESOS

El acceso controlado a los sistemas de información deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

6.6. PROTECCIÓN DE LAS INSTALACIONES

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

6.7. MÍNIMO PRIVILEGIO

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) Los sistemas de información proporcionarán la funcionalidad imprescindible para que se alcancen los 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) 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 de los sistemas de información ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

6.8. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La inclusión de cualquier elemento físico o lógico en el registro de activos de información, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas de información 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.

6.9. PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Se 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.

6.10. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se protegerá el perímetro de los sistemas de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad. En todo caso, se analizarán los riesgos derivados de la interconexión de los sistemas de información con otros sistemas, y se controlará su punto de unión.

6.11. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Se registrarán 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. Todo ello, se llevará a cabo en cumplimiento de las disposiciones legales de aplicación en este ámbito de actuación.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de la normativa legal de aplicación, se podrá analizar las comunicaciones entrantes y salientes, y únicamente para 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 del servicio, evitar la distribución malintencionada de código dañino, así como otros daños.

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.

6.12. INCIDENTES DE SEGURIDAD

Se dispondrá de procedimientos de gestión de incidentes de seguridad, así como cauces de comunicación a las partes interesadas, y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad de los sistemas de información.

6.13. CONTINUIDAD DE LA ACTIVIDAD

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

6.14. MEJORA CONTINUA

El proceso integral de seguridad de la información implantado deberá ser actualizado y mejorado de forma continua.

7. ENFOQUE DE RIESGOS

Los sistemas que conforman el alcance de la presente **Política de Seguridad de la Información** se encuentran sujetos a un análisis y evaluación de riesgos, con el objeto de identificar las amenazas a las que se encuentran expuestos, evaluar el impacto asociado a la materialización de tales amenazas, y determinar las situaciones de riesgos que podrían derivarse.

El resultado de este análisis y evaluación de riesgos permitirá la identificación y proposición de las medidas de seguridad oportunas como estrategia para la mitigación de los mismos.

El **Comité de Seguridad de la Información** liderará la ejecución periódica del análisis de riesgos, planificando los recursos técnicos, humanos y económicos necesarios a tales efectos.

8. ESTRUCTURA

El desarrollo de la **Política de Seguridad de la Información** incluirá, basándose en el análisis y evaluación de riesgos efectuado, aspectos específicos de la seguridad de la información, tales como las medidas de seguridad indicadas en el **ENS**.

Estas medidas de seguridad quedarán agrupadas en **tres niveles diferenciados de seguridad** según queda establecido en el **ENS**.

8.1. MARCO ORGANIZATIVO

Orientado a administrar la seguridad de la información en el contexto de la estructura organizativa de **EMERA ESPAÑA**, así como establecer un marco de gestión para controlar su implementación.

8.2. MARCO OPERACIONAL

Constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

- **Planificación:** mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes, entre otros aspectos.
- **Control de acceso:** orientado a controlar el acceso lógico a la información.
- **Explotación:** medidas para la gestión de la seguridad en explotación; partiendo del inventario de activos y controlando la gestión de incidentes, gestión de cambios, gestión de la configuración, registros de actividad, entre otros.
- **Servicios externos:** medidas de seguridad orientadas a garantizar que los proveedores de servicios contratados por **EMERA ESPAÑA**, o que, de alguna manera, se presten bajo el control y/o la dirección de **EMERA ESPAÑA**, cumplan las políticas y normas de seguridad de la información establecidas.
- **Continuidad del servicio:** acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.
- **Monitorización del sistema:** orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos frente al impacto provocado por situaciones de desastre.

8.3. MEDIDAS DE PROTECCIÓN

Para la protección de activos concretos, según su naturaleza, con el nivel requerido para cada dimensión de seguridad.

- **Protección de las instalaciones e infraestructuras:** destinado a impedir accesos no autorizados, daños e interferencias a las instalaciones e infraestructuras de **EMERA ESPAÑA**.
- **Gestión del personal:** orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos.
- **Protección de los equipos:** medidas para la protección física y medioambiental de los equipos.
- **Protección de las comunicaciones:** dirigido a garantizar el intercambio seguro de la información, y los accesos a través de redes de comunicaciones.
- **Protección de los soportes de información:** con el objeto de preservar la información que contienen estas unidades de almacenamiento externo.
- **Protección de las aplicaciones informáticas:** orientado a mantener la visión de seguridad durante todo el ciclo de vida asociado al desarrollo y mantenimiento de las mismas.
- **Protección de la información:** cumpliendo lo dispuesto en el **RGPD**, la **Ley 3/2018**, así como cualquier otra legislación de aplicación en función de la naturaleza de la información.
- **Protección de los servicios:** definiendo las medidas necesarias para mantener la seguridad de los servicios de TI.

9. TERCERAS PARTES

Cuando **EMERA ESPAÑA** requiera de la participación de terceras partes para la prestación de un servicio, les hará participes de la normativa de seguridad que sea de consideración en el contexto de dicha colaboración, quedando éstos sujetos a las obligaciones establecidas en dicha normativa y, formalmente, a los requisitos de seguridad identificados para el alcance de los servicios externalizados.

10. DATOS DE CARÁCTER PERSONAL

La formalización de la **Política de Seguridad de la Información**, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la normativa legal vigente aplicable en materia de protección de datos de carácter personal.

11. REVISIÓN

La **Política de Seguridad de la Información** será revisada anualmente por el **Responsable de Seguridad** o cuando exista un cambio significativo (enfoque de la gestión de la seguridad, circunstancias del negocio, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades de control, tendencias relacionadas con amenazas y vulnerabilidades, etc.) que obligue a ello.

En el caso de que se obtenga una nueva versión de la **Política de Seguridad de la Información**, se precisará la aprobación formal de la **Dirección** con carácter previo a su divulgación.

12. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Dirección el día 7 de septiembre de 2026.

Esta **Política de Seguridad de la Información** es efectiva desde el día siguiente al de su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Su entrada en vigor supone la derogación de cualquier otra Política que existiera a tales efectos.

La Dirección