Política de Seguridad de la Información

CONTROL DE REVISIONES

REDACCIÓN		Comité de Seguridad		
APROBADO POR		Dirección General		
FECHA Ed.1		18/02/2025		
VERSIÓN	**FECHA**	**RESPONSABLE CAMBIOS**	**DESCRIPCIÓN DE CAMBIOS**	**APROBADO POR**
Ed.1	08/07/2025	Comité de Seguridad	Elaboración versión inicial	Dirección General

ÍNDICE

1. OBJETO

El objeto de la presente Política de Seguridad de la Información es establecer las directrices y principios que regirán el modo en que Ente Vasco de la Energía (en adelante EVE) gestionará y protegerá su información y sus servicios, dentro del marco regulatorio legal y vigente como el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), siendo su aplicación en el ámbito de la administración electrónica del sector público, que exige el establecimiento de los principios y requisitos de una política de seguridad de la información en la utilización de medios electrónicos que permita la adecuada protección de la información.

2. INTRODUCCIÓN

EVE depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

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

Las diferentes áreas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación y en la solicitud de ofertas para proyectos de TIC.

3. MARCO NORMATIVO

El marco normativo de las actividades de EVE en el ámbito de esta Política de Seguridad de la Información está integrado por las siguientes normas:

- Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Igualmente, se deberán tener en cuenta las posibles modificaciones normativas y avances técnicos que puedan afectar al ámbito de esta Política de Seguridad de la Información.

4. ORGANIZACIÓN DE LA SEGURIDAD

Con el fin de garantizar la correcta implantación de la presente Política, EVE se organizará con el objeto de definir las medidas de seguridad que deben aplicarse a los activos de información, y que deben ser implantadas por el área de Sistemas de Información.

Dicha organización de la seguridad cuenta con la participación de la Dirección General de EVE, quien aprobará la Política de Seguridad de la Información y asignará y/o delegará responsabilidades en las personas que considere idóneas, y periódicamente será informada para asegurar el seguimiento de la implantación efectiva de la misma.

Igualmente, la organización implicará en distinta medida a todo el personal de EVE, con el objeto de extender la implantación de las prácticas de seguridad idóneas.

4.1. ESTRUCTURA ORGANIZATIVA: FUNCIONES Y RESPONSABILIDADES

Las funciones y responsabilidades principales de seguridad de la información se definen en el documento Manual de gestión.

4.1.1. COMITÉ DE SEGURIDAD

La organización contará con un Comité de Seguridad en el que participan la persona Responsable de Seguridad de la Información, Responsable de Sistemas, Responsable de Servicio y Responsable de la Información. Este comité tendrá una doble función, tratar los temas relacionados con la protección de datos y gestionar la seguridad de la información. La composición, funciones y responsables de este comité se recoge en el documento Manual de gestión.

Se prevé la celebración de 3 sesiones ordinarias del Comités de Seguridad anualmente, pudiendo celebrarse sesiones extraordinarias cuando así se requiera.

Las sesiones del Comité de Seguridad quedarán conformadas mediante quórum de 2/3 de sus miembros en primera convocatoria y por la mitad + 1 de miembros en segunda convocatoria.

La persona Responsable de Seguridad de la Información comunicará una agenda de temas a tratar al menos una semana antes del comité. De la misma forma, una vez finalizado el mismo, se elaborará un acta de la que será comunicado a todos los miembros. El acta será aprobada en la celebración del siguiente comité.

5. REQUISITOS MINIMOS DE SEGURIDAD

Atendiendo al cumplimiento del ENS, se garantizará el cumplimiento de los siguientes requisitos mínimos:

- ***Organización***: diseño e implantación del proceso de seguridad de la información.
- ***Análisis y gestión de los riesgos***: tratamiento adecuado de los riesgos de ciberseguridad.
- ***Gestión de personal***: implantando seguridad en los procesos de incorporación y baja del personal, así como acciones relativas a formación y concienciación.
- ***Profesionalidad***: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida (instalación, mantenimiento, gestión de incidentes y desmantelamiento). El personal de EVE recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.
- ***Seguridad por terceros***: EVE exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados. Además, se estará a lo dispuesto en el ENS relativo a contratación de terceros.
- ***Autorización y control de los accesos***: el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.
- ***Protección de las instalaciones***: los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas permanecerán cerradas y dispondrán de un control de llaves.
- ***Adquisición de productos de seguridad y contratación de servicios de seguridad:*** se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio de la persona Responsable de Seguridad de la Información.
- ***Seguridad por defecto mínimo privilegio***: los sistemas se diseñarán y configurarán de manera que garanticen la seguridad por defecto y mínimo privilegio:
    - El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- 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, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.
- Se garantizará que el uso ordinario del sistema sea sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- ***Integridad y actualización del sistema***: todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se conocerá en todo

momento el estado de seguridad de los sistemas, con relación a 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 seguridad de estos.

- ***Protección de la información almacenada y en tránsito***: en la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, tabletas, teléfonos móviles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.
- ***Soporte Papel***: toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.
- ***Prevención ante otros sistemas de información interconectados:*** el sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. 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.
- ***Registro de actividad y detección de código dañino***: con la finalidad exclusiva de lograr el cumplimiento del objeto del ENS con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, 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 , así como facilitar la denegación de 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.
- ***Gestión de incidentes de seguridad y Continuidad de la actividad***: los sistemas de EVE dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, dentro de niveles aceptables, en caso de pérdida de los medios habituales de trabajo.
- ***Mejora continua del proceso de seguridad***: el proceso integral de seguridad implantado será actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

6. CATEGORIZACIÓN DEL SISTEMA

La categorización del sistema se establece en función de la valoración de servicios e información que hacen cada uno de las personas responsables de estos.

Para la valoración de servicios e información se seguirán las indicaciones del Real Decreto 311/2022, Anexo I, punto 1 Fundamentos, para la determinación de la categoría de seguridad de un sistema de información que establece que para lograr el cumplimiento de los principios

básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

- Las dimensiones de seguridad relevantes en el sistema a proteger.
- La categoría de seguridad del sistema de información a proteger.

Como soporte adicional se podrá utilizar la guía "CCN-STIC 803 - ENS Valoración de sistemas".

7. NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

El EVE establece un marco documental estructurado en diferentes niveles, de forma que las directrices marcadas por el presente documento tengan un desarrollo específico. En cualquier caso, las diferentes políticas, normativas y regulaciones específicas que se desarrollen deben estar alineadas con la presente Política de Seguridad de la Información y derivarse de la misma.

La composición del citado marco documental es la siguiente:

- **Política de Seguridad de la Información**: Está constituido por el presente documento y es de obligado cumplimiento. Será aprobada por la Dirección General.
- **Normativas**: Emanan de la presente Política de Seguridad de la Información y soportan los diferentes ámbitos de la seguridad. Serán aprobadas por Comité de Seguridad.
- **Procedimientos de seguridad**: Emanan de la presente Política de Seguridad de la Información y soportan los diferentes ámbitos de la seguridad. Serán aprobados por la persona Responsable de Seguridad de la Información de EVE.
- **Guías específicas de TI o instrucciones técnicas**: Conjunto de documentos que describen las pautas específicas a seguir a la hora de realizar una determinada actividad técnica relacionada con la seguridad de la información. Serán aprobados por la persona Responsable de Seguridad de la Información de EVE.
- **Otros documentos**: Además de los documentos citados, la documentación de seguridad podrá contar con otros adicionales, como recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, presentaciones, etc.

La *Política de Seguridad de la Información* (primer nivel) será aprobada por la Dirección General a propuesta del Comité de Seguridad.

Las *normas de carácter general* (segundo nivel) serán aprobadas por el Comité de Seguridad de EVE, a propuesta de la persona Responsable de Seguridad de la Información.

Los *procedimientos* y *guías de seguridad* o *instrucciones de seguridad* (tercer y cuarto nivel) son aprobadas por la persona Responsable de Seguridad de la Información en colaboración con las personas responsables de los servicios y la persona responsable de sistemas.

La presente Política de Seguridad de la Información debe estar accesible en Internet, y las normativas que se aprueben deben ser comunicadas a todos las personas responsables de los servicios afectados. El resto de documentación específica deberá estar accesible en la intranet de EVE siempre que su aplicabilidad pueda afectar a todas las personas usuarias. Su incumplimiento puede dar lugar a la correspondiente responsabilidad disciplinaria.

8. GESTIÓN DE INCIDENTES

Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

8.1. PREVENCIÓN

Las áreas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de esta Política de Seguridad de la Información, las áreas deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

8.2. DETECCIÓN

EVE establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS (reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 8 del ENS. Líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a las personas responsables regularmente.

8.3. RESPUESTA

Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

8.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios, EVE dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos. Se trata de los procedimientos y las normas contenidas en la Normativa de Seguridad de EVE.

9. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN

La Dirección General de EVE se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del ENS de la entidad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente Política de Seguridad de la Información y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de EVE.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de la compañía.
- Asegurar que los recursos necesarios para el ENS estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
- Asegurar que el ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

10. CONCIENCIACIÓN Y FORMACIÓN

Corresponde al Comité de Seguridad promover la formación y concienciación en materia de seguridad de la información en el ámbito de EVE.

Se desarrollarán actividades específicas orientadas a la formación y concienciación de todo el personal en materia de seguridad de la información, así como a la difusión de la Política de Seguridad de la Información y de su desarrollo normativo, y estarán dirigidas en particular a personal de nueva incorporación. A estos efectos, los planes de formación de EVE incluirán actividades específicas sobre seguridad y privacidad de la información.

11. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Todos los sistemas de información sujetos a esta Política de Seguridad de la Información deberán realizar un análisis de riesgos de seguridad de la información, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año.
- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

Las personas Responsables de los Servicios y la Información responden de los riesgos que afectan a su departamento, y asegurarán su seguimiento y control. Para ello, podrán contar en el proceso con la participación y asesoramiento de quienes sean Responsable de la Seguridad y Responsable de los Sistemas.

Para la realización del análisis de riesgos se tendrán en cuenta las guías elaboradas por el Centro Criptológico Nacional (CCN). Esta evaluación de los riesgos se repetirá regularmente para los sistemas de información teniendo en cuenta las recomendaciones formuladas por dicho Centro.

Existe un compromiso por parte de EVE, y una obligación por parte de las personas Responsables de los Servicios y la Información, de realizar análisis de riesgos y atender a sus conclusiones.

12. TERCERAS PARTES

Cuando EVE preste servicios o maneje información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación del Comité de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando EVE utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la Información y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha Normativa de Seguridad, 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 esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad de la Información.

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

13. OBLIGACIONES DEL PERSONAL

Todas las personas usuarias de la organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa e instrucciones de seguridad desarrolladas a partir de ella, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todas las personas usuarias de EVE atenderán a una sesión de concienciación en materia de seguridad informática al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todas las personas usuarias de EVE, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas informáticos y de telecomunicaciones recibirán 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.

El cumplimiento de la presente Política de Seguridad de la Información es obligatorio por parte de todas las personas usuarias internas o externas que intervengan en los procesos de EVE, constituyendo su incumplimiento infracción grave a efectos laborales.

14. APROBACIÓN Y PROCESO DE REVISIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Se revisa y promueve la actualización de la presente Política de Seguridad de la Información y de la Normativa de Seguridad que de esta deriva por parte de EVE.

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que deberán ser inferiores a dos años o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. La propuesta de revisión, en su caso, se aprobará y difundirá para que la conozcan todas las partes interesadas.

Los cambios sobre el presente documento deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 12 del ENS. Dada la naturaleza de EVE, es imprescindible tener en cuenta y velar por la coherencia en la organización.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

En Bilbao, a 8 de julio de 2025

FIRMA DIRECCIÓN