POLITICA

POLÍTICA DE SEGURIDAD DE LA INFORMACION

REGISTRO DE MODIFICACIONES Y APROBACIÓN

Rev.	Fecha	Elaborado	Revisado	Aprobado	Descripción modificaciones
0	Feb 2026				Primera edición
1	Mar 2026	Lucía Lacalle Firmado digitalmente por Lucía Lacalle Fecha: 2026.03.17 11:19:46 +01'00' Lucia Lacalle Responsable Sistema Gestión QHSE	38119873H JULIAN MENDOZA (R: A46194528) Firmado digitalmente por 38119873H JULIAN MENDOZA (R: A46194528) Fecha: 2026.03.17 11:54:58 +01'00' Julian Mendoza Responsable de Seguridad de la Información	DOMINGUIS PEREZ HECTOR JERONIMO - 44850331D Digitally signed by DOMINGUIS PEREZ HECTOR JERONIMO - 44850331D DN: C=ES, CN=DOMINGUIS PEREZ HECTOR JERONIMO - 44850331D, GN=HECTOR JERONIMO, SN=DOMINGUIS PEREZ, serialNumber=IDCES-44850331D Reason: I am approving this document Location: Date: 2026.03.25 09:51:58+01'00' Foxit PDF Reader Version: 2025.3.0 Héctor Dominguis Presidente y CEO	Adaptación a los requisitos de la ISO 27001 apartado 5.2

INDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política. Será revisada, junto a las propuestas de actualización o mantenimiento de la misma, con una periodicidad mínima anual.

La presente Política será comunicada a todo el personal y estará disponible para todas las partes interesadas pertinentes. GDES garantizará que su personal comprende sus obligaciones derivadas de esta política y participará activamente en su cumplimiento.

2. OBJETO

La finalidad de la presente política es proporcionar la orientación para la gestión de la Seguridad de la Información de GDES, identificando los roles y responsabilidades y estableciendo un marco normativo que permita identificar, desarrollar e implantar las medidas necesarias para garantizar la seguridad y protección tanto de la información de GDES, como de los sistemas que la gestionan.

Para ello, establece un marco de trabajo que permite identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección tanto de la información de GDES como de los sistemas que la gestionan.

GDES se compromete a la mejora continua del Sistema de Gestión de Seguridad de la Información, revisando con regularidad la eficacia de los controles, los resultados del análisis de riesgos, las auditorías, los incidentes y los cambios relevantes en los servicios y en el entorno tecnológico.

3. ALCANCE

Esta política es de aplicación a todo el ámbito de actuación que emplee los Sistemas de Información de GDES.

Abarca a toda la información utilizada por GDES para el desarrollo de sus actividades y es aplicable, con carácter obligatorio, tanto para GDES, así como para las entidades colaboradoras involucradas en la utilización de la información y los sistemas de GDES. La información a que se refiere esta política es la contenida en cualquier tipo de soporte, tanto la producida por GDES como la recibida, ya sea en formato digital o físico, y también la verbal.

Las relaciones con dichas entidades colaboradoras están amparadas por los contratos de prestación de servicios correspondientes, incluyendo cláusulas de garantías en el uso de la información.

La política aplica y es de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en GDES incluyendo el personal externo, cuando sean usuarios de los Sistemas de Información de la organización.

En el ámbito de la presente política, se entiende por usuario cualquier empleado perteneciente o ajeno a GDES, así como personal de organizaciones privadas externas, entidades colaboradoras o

cualquier otro con algún tipo de vinculación con la organización y que utilice o posea acceso a los sistemas de información de la organización. Siendo también de aplicación a usuarios externos, en términos del Esquema Nacional de Seguridad.

4. INTRODUCCIÓN

Con el objetivo de garantizar la calidad de la información y la prestación continuada de los servicios de la organización, GDES actúa de forma preventiva tomando las medidas adecuadas para proteger los sistemas frente a daños accidentales o deliberados, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Para defender los sistemas y la información frente a las amenazas que ponen en riesgo su confidencialidad, integridad, disponibilidad, autenticidad y/o trazabilidad se requiere de una estrategia que implique a todo el personal que maneja la información de la organización.

Siguiendo los requisitos definidos por el Esquema Nacional de Seguridad (en adelante, ENS), así como otras iniciativas de seguridad adicionales, en GDES se considera la seguridad de la información de una manera global.

Por ello, se define la presente Política de Seguridad que se comunica a todo el personal trabajador para su conocimiento y cumplimiento. Tanto esta política como las normativas y procedimientos que de ella se derivan serán revisados, actualizados y divulgados periódicamente (y siempre que sea necesario) para dar respuesta a posibles nuevos riesgos y amenazas y para mejorar de forma continuada la eficacia de los métodos de seguridad de la información aplicados.

Para la elaboración de este documento, se ha tomado como referencia la guía “CCN – STIC 805 Política de Seguridad de la Información” y la guía “CCN – STIC 801 Esquema Nacional de Seguridad Responsabilidades y funciones”, elaboradas por el Centro Criptológico Nacional.

4.1. Prevención

GDES debe 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 debe implementarse 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 la política, GDES:

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

4.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que pueden ir desde una simple desaceleración hasta su detención, debe monitorizarse la operación de los servicios de manera continua para detectar posibles anomalías en los niveles de prestación de los mismos y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables afectados regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.3. Respuesta

Para responder de forma eficaz ante eventos de seguridad, tales como incidentes, GDES realiza las siguientes acciones:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa el punto de contacto para las comunicaciones con respecto a incidentes detectados a las posibles partes interesadas (clientes, proveedores, grupos inversores, etc.).
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) y, si fuera necesario, con las FF.CC.S.E. y con la Agencia Española de Protección de Datos.

4.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, GDES ha desarrollado diversas medidas y estrategias, como identificar y evaluar los riesgos para adoptar medidas preventivas y mitigarlos de manera oportuna.

5. VISIÓN, PROPÓSITO Y COMPROMISOS DE LA ORGANIZACIÓN

La visión, el propósito y los compromisos bajo los que actúa GDES se encuentran definidos en el Manual Corporativo del sistema Integrado de Gestión.

La Dirección de GDES expresa su compromiso firme con la seguridad de la información, proporcionando los recursos necesarios, impulsando el cumplimiento del Esquema Nacional de Seguridad, de la ISO/IEC 27001 y del resto de requisitos legales, regulatorios y contractuales aplicables o voluntariamente adquiridos.

La Dirección asume el liderazgo en la implantación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando que esta Política se comunica,

comprende y aplica en toda la organización. Así mismo, establece objetivos de seguridad de la información, cuya aprobación y seguimiento se realiza a través del Comité de Seguridad de la Información.

6. MARCO NORMATIVO Y LEGAL

GDES se compromete a cumplir con todos los requisitos legales, reglamentarios, contractuales y de negocio relacionados con la seguridad de la información, incluyendo el Esquema Nacional de Seguridad, la ISO/IEC 27001, el RGPD, la LOPDGDD y cualquier normativa aplicable a la organización.

La normativa aplicable a GDES en el ámbito de la Seguridad de la Información y de la Ciberseguridad viene recogida en la herramienta de Identificación de requisitos legales interna.

7. ORGANIZACIÓN DE LA SEGURIDAD

El gobierno de la Seguridad de la Información de GDES se basa en una estructura piramidal, en la cual encontramos el Comité de Seguridad en la cúspide. A este Comité le acompañan, reportan y da soporte una serie de roles, con responsabilidades asociadas. La Dirección de GDES promueve la composición del Comité de Seguridad de la Información, en aras de establecer una vía definida y de apoyo a las iniciativas de seguridad

En términos generales, la responsabilidad trasversal de establecer los mecanismos necesarios para garantizar la seguridad de la información de GDES recae en la Dirección de Sistemas de Información, la cual debe realizar las siguientes tareas:

- Revisar la Política Corporativa de Seguridad de la Información, del marco normativo asociado y de las responsabilidades principales y proponerla al Comité de Seguridad para su aprobación.
- Supervisar y controlar los cambios significativos en los sistemas de información y en la organización de GDES que puedan afectar, desde el punto de vista de la seguridad, a los activos de información.
- Revisar y gestionar las incidencias de Seguridad de la Información.
- Aprobar las iniciativas principales para mejorar la Seguridad de la Información e implantar los controles necesarios para garantizar la seguridad de la información.
- Coordinar las acciones que requieran intervención de otras áreas de GDES.
- Someter periódicamente a auditorías internas y externas, cuando sean necesarias, con la finalidad de verificar el correcto funcionamiento de los planes de seguridad, determinando grados de cumplimiento y recomendando medidas correctoras.
- Reportar al Comité de Seguridad y a Dirección de las principales acciones desarrolladas durante el año, así como de la situación en materia de seguridad de la información de GDES.
- Realizar, mantener y actualizar el análisis de riesgos que permita la toma de decisión sobre la base del riesgo, así como, proponer el plan de tratamiento de los mismos.

Así mismo, la gestión del SGSI se encomienda al Responsable de Sistemas, que, en coordinación con el Departamento QHSE, vela por su correcta aplicación y adecuación. La documentación correspondiente se encuentra debidamente estructurada en el gestor documental de GDES, al cual se puede acceder según los perfiles de acceso establecidos.

7.1. Comité de Seguridad

El Comité Seguridad Información es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que las decisiones más importantes relacionadas con la seguridad de la información que afectan a GDES se acuerdan por este Comité.

El Comité es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones dentro de su ámbito que no tiene que subordinar su actividad a ningún otro elemento de la compañía dentro de sus responsabilidades.

7.1.1. Composición del Comité de Seguridad

Los miembros del Comité de Seguridad Información son propuestos y aprobados por la Dirección de GDES. La composición será la siguiente:

- Presidencia del Grupo
- Dirección General (como Responsable de los Servicios y de la Información)
- Dirección de Sistemas de Información
- Responsable de Sistemas
- Director Calidad y Seguridad (como Responsable de Seguridad y Protección de Datos Personales)

La Dirección General actuará como Presidente del Comité de Seguridad de la Información y será el responsable último de las decisiones adoptadas. El Director de Calidad y Seguridad actuará como Secretario, dirigiendo las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

El Comité podrá tener la participación de asesores externos y/o otros miembros de la Organización cuando se considere conveniente.

7.1.2. Funciones del Comité de Seguridad

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

- Revisión de la Política Corporativa de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.

- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como: riesgos, incidentes, vulnerabilidades críticas, o cualquier otro asunto que requiera de actuaciones por el Comité.
- Control y seguimiento de los riesgos identificados y sus planes de acciones asociados.
- Control y seguimiento de los KPIs de seguridad.
- Revisión y aprobación de planes de continuidad.
- Cumplimiento y difusión de las Políticas de Seguridad.
- Proponer los candidatos para cubrir los roles de responsables del Comité de Seguridad de la información cuando sea necesario.
- Realizar seguimiento de los riesgos identificados y sus planes de acción asociados.

7.1.3. Funcionamiento del Comité de Seguridad

El Comité de Seguridad se reunirá de manera cuatrimestral de forma ordinaria, pudiéndose convocar sesiones extraordinarias cuando sean necesarias aprobaciones urgentes. Antes de cada sesión el Secretario deberá elaborar una orden del día con los asuntos a tratar y, al finalizar, se elaborará y enviará un acta oficial de la sesión donde se recoja como mínimo:

- Fecha y hora de la sesión
- Convocados y asistentes
- Puntos del orden del día tratados
- Puntos adicionales tratados
- Acuerdos alcanzados en el Comité.

Tales actas serán oficiales y aprobadas por los miembros del Comité.

Los acuerdos del Comité de Seguridad se aprobarán por mayoría.

7.2. Responsable de Sistemas

Las funciones del responsable del Sistema son las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o demás miembros del Comité de Seguridad de la Información.

- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.

7.3. Responsable de Información

Las funciones del responsable de Información son las siguientes:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a la información.
- Aceptar los niveles de riesgo residual que afectan a la información.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de la que es responsable, especialmente la incorporación de nueva Información a su cargo.

7.4. Responsable de Servicio

Las funciones del responsable de Servicio son las siguientes:

- Establecer y elevar para su aprobación al Comité de Seguridad de la Información los requisitos de seguridad aplicables a los Servicios (niveles de seguridad de los servicios), dentro del marco establecido en el Anexo I del RD ENS, pudiendo recabar una propuesta al Responsable de Seguridad y teniendo en cuenta la opinión del Responsable del Sistema.
- Dictaminar respecto a los derechos de acceso a los servicios.
- Aceptar los niveles de riesgo residual que afectan a los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios a su cargo.

7.5. Responsable de Seguridad

Las funciones del responsable de Seguridad son las siguientes:

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

- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Analizar los informes de autoevaluación y de auditoría, así como elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctivas adecuadas.

7.6. Responsable de Protección de datos personales

Las funciones del responsable de Protección de datos se encuentran definidas en la política de Protección de Datos Personales.

7.7. Procedimiento de designación y revocación

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección de GDES a propuesta del Comité de Seguridad de la Información. De igual forma, la Dirección es la encargada de la designación de los distintos miembros que formarán el Comité de Seguridad de la Información.

Asimismo, la Dirección se reserva el derecho de la revisión y renovación de las asignaciones y responsabilidades en cualquier momento.

8. GESTION DE RIESGOS

Las decisiones y acciones acordadas en materia de seguridad de la información y ciberseguridad de GDES se basará en una perspectiva del riesgo. De modo que todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis de riesgos, identificando las amenazas y evaluando 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.

Para cada riesgo identificado por encima del apetito de riesgo establecido por el Comité de Seguridad se deberá elaborar un plan de acción que se someterá a aprobación del Comité de Seguridad. Igualmente, se deberá reportar los avances y actualizaciones de estos planes de tratamiento del riesgo.

En el caso de que se decida asumir el riesgo, será el Comité de Seguridad el órgano encargado de aprobarlo y reportarlo a Dirección.

9. OBLIGACIONES DEL PERSONAL

Todo el personal de GDES, interno o externo, que utilice o tenga acceso a la información y/o a los sistemas tecnológicos o de información corporativos, tiene las siguientes obligaciones:

- Conocer, cumplir y hacer cumplir esta Política de Seguridad de la Información y las Normativas de Seguridad y procedimientos que la desarrollan y que le afecten.
- Atender a las acciones de concienciación en materia de seguridad de la información que se realicen.
- Utilizar los servicios y sistemas de información, así como la información en ellos contenida y a la que tengan acceso, con una finalidad profesional acorde a las tareas encomendadas en función de su puesto de trabajo y a los fines y propósitos que motivaron la concesión del acceso.
- Velar por la confidencialidad de la información a la que tenga acceso según la clasificación y características de la misma.
- Notificar eventos que puedan suponer una brecha de seguridad o evidencien una debilidad que pueda implicar posteriores brechas.
- Colaborar en la resolución de brechas de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación.
- Participar en la estructura de gestión de la seguridad de la información cuando corresponda según las competencias y funciones de su puesto de trabajo.
- No realizar acciones intencionadas o negligentes que puedan perjudicar la seguridad de los sistemas tecnológicos o la información que contienen.

Asimismo, queda bajo la responsabilidad de los usuarios hacer un uso proporcional, adecuado y justificado de los medios puestos a su disposición para el desarrollo de sus funciones. Cualquier uso indebido, podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

10. RELACIONES CON TERCEROS

Cuando GDES preste servicios a otras organizaciones o maneje información de otras organizaciones, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos comités de seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando GDES utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de las Normativas de Seguridad aplicables a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

11. DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistemas de información se seguirá en todo momento lo desarrollado en el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD) así como lo exigido de las medidas de seguridad en el tratamiento de datos de carácter personal exigido en la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDDGG).

El Registro de Actividades de Tratamiento recoge los tratamientos de datos personales que realiza GDES, así como el resto de información pertinente, como la base jurídica del tratamiento, las finalidades, los plazos de conservación y los destinatarios (cesiones de datos personales).

Todos los sistemas de información de GDES se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el registro de actividades de tratamiento. Las medidas de seguridad implementadas dependerán del análisis de riesgos realizado y tendrán como objetivo reducir el nivel de riesgo mediante la aplicación de medidas técnicas de seguridad relacionadas con las directrices del ENS y medidas legales relacionadas con los artículos del RGPD.

12. DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

El sistema documental está formado por la presente Política de Seguridad y las Normativas y Procedimientos de Seguridad de GDES. Adicionalmente, puede que algunos procedimientos internos (de gestión de RR.HH., procedimientos operativos, etc.) también incluyan aspectos relacionados con los requisitos de seguridad marcados por el ENS. El Manual QHSE es el documento que describe el sistema de gestión de la organización, adaptado a los requisitos de los referenciales normativos de aplicación y es un marco de referencia permanente para la implantación y mantenimiento del Sistema Integrado de Gestión y una guía de funcionamiento para todos los puestos de trabajo involucrados en el mismo. También da a conocer la estructura documental del Sistema y la interrelación existente entre ella y los elementos del Sistema.

Todos estos documentos se encuentran dentro del repositorio documental de GDES, accesible únicamente para el personal autorizado. La última versión aprobada se encuentra disponible en dicho repositorio documental para todo el personal en modo lectura.