


# **POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD**



	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 2 de 17

## ÍNDICE

### Tabla de contenido

1.	APROBACIÓN Y ENTRADA EN VIGOR.....	3
2.	INTRODUCCIÓN .....	3
3.	ALCANCE .....	4
3.1.	Alcance Subjetivo.....	4
3.2.	Alcance Objetivo.....	4
4.	REQUISITOS MÍNIMOS DE SEGURIDAD .....	5
5.	PRINCIPIOS BÁSICOS.....	6
6.	OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.....	7
7.	MISIÓN.....	8
8.	DESARROLLO DE LA POLÍTICA.....	9
8.1.	Primer nivel normativo: Política de Seguridad TIC.....	10
8.2.	Segundo nivel normativo: Normas de Seguridad de la Información.....	10
8.3.	Tercer nivel normativo: Procedimientos de Seguridad TIC.....	10
9.	ORGANIZACIÓN DE LA SEGURIDAD .....	10
9.1.	Roles o perfiles de seguridad.....	10
9.2.	Comité de Seguridad de la Información .....	10
9.3.	Responsabilidades.....	11
9.4.	Procedimientos de designación .....	14
9.5.	Matriz RACI: matriz de asignación de responsabilidades .....	14
10.	RESOLUCIÓN DE CONFLICTOS .....	15
11.	DATOS DE CARÁCTER PERSONAL .....	15
12.	TERCERAS PARTES .....	16
13.	MEJORA CONTINUA .....	16
14.	APROBACIÓN DEL DOCUMENTO.....	17

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 3 de 17

## 1. APROBACIÓN Y ENTRADA EN VIGOR


Texto aprobado el día 26 de febrero de 2026 mediante acta del Director General de DIVIDEND REFUND, S.L.. en adelante DIVIDEND REFUND. Esta “Política del Sistema de Gestión Seguridad de la Información”, en adelante Política, será efectiva desde su fecha de aprobación, y se mantendrá vigente hasta que sea sustituida por una nueva Política.

## 2. INTRODUCCIÓN

DIVIDEND REFUND depende en gran medida de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos, y es consciente de que la transformación digital ha supuesto un incremento significativo de los riesgos asociados a la seguridad de la información.

El objetivo de esta gestión de riesgos es proteger los sistemas de Tecnologías de la Información y las Comunicaciones frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada por DIVIDEND REFUND.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por las normas ISO 27001 y 27701, 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.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 4 de 17

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

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

### 3. ALCANCE


#### 3.1. Alcance Subjetivo

Los sujetos obligados por esta Política son todo el personal de DIVIDEND REFUND, y todas aquellas personas o entidades, tanto internas como externas, que presten servicios a DIVIDEND REFUND, tanto en sus propias instalaciones como en remoto.

#### 3.2. Alcance Objetivo

Esta Política se aplicará a los sistemas de gestión de la información de DIVIDEND REFUND que **dan soporte a los servicios de tramitación de exenciones de doble imposición de DIVIDEND REFUND, S.L., en las instalaciones ubicadas en Zurbano 92, 28003 Madrid y los entornos cloud que dan soporte a dicho servicio, en base a la Declaración de Aplicabilidad vigente.**


La identificación y mantenimiento del marco normativo será responsabilidad del Responsable del Sistema de Gestión de Seguridad de la Información de DIVIDEND REFUND y se regulará a través del procedimiento relativo a la identificación y evaluación de requisitos legales.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 5 de 17

#### 4. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política del Sistema de Gestión de Seguridad y Privacidad de DIVIDEND REFUND regula la gestión continua del proceso de seguridad. Esta Política se ha establecido de acuerdo con los siguientes principios básicos:

- a) Organización e implantación del proceso de seguridad
- b) Análisis y gestión de los riesgos
- c) Gestión de personal
- d) Profesionalidad
- e) Autorización y control de los accesos
- f) Protección de las instalaciones
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio
- i) Integridad y actualización del sistema
- j) Protección de la información almacenada y en tránsito
- k) Prevención ante otros sistemas de información interconectados
- l) Registro de la actividad y detección de código dañino
- m) Incidentes de seguridad

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 6 de 17

- n) Continuidad de la actividad
- ñ) Mejora continua del proceso de seguridad
- o) Privacidad desde el diseño y por defecto.
- p) Atención a los derechos de los interesados.


Para dar cumplimiento a estos requisitos mínimos DIVIDEND REFUND aplicará las medidas de seguridad descritas en el Anexo A de la norma ISO 27001 y los controles adicionales de la ISO 27701, teniendo en cuenta:

- Los activos que constituyen el sistema de información de DIVIDEND REFUND.
- Las decisiones que se adopten para gestionar los riesgos identificados.

## 5. PRINCIPIOS BÁSICOS

La Política de Gestión del Sistema de Seguridad de la Información y Privacidad de DIVIDEND REFUND establece los siguientes principios básicos, alineados con el compromiso de la Dirección con el Sistema de Gestión Integrado:

- **Seguridad y privacidad como proceso integral:** ambos atributos abarcan elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información y con los tratamientos de datos personales.
- **Gestión integral basada en riesgos:** el análisis y gestión de los riesgos es parte esencial del proceso de seguridad y de los riesgos para los derechos y libertades de los interesados, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos aceptables.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 7 de 17


- **Prevención, detección, respuesta y conservación:** La seguridad del sistema de información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta.
- **Existencia de líneas de defensa:** El sistema de información de DIVIDEND REFUND debe disponer de una estrategia de protección constituida por múltiples capas de seguridad.
- **Vigilancia continua y reevaluación periódica:** La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente permitirá medir su evolución y las medidas de seguridad se reevaluarán y actualizarán periódicamente adecuando su eficacia a la evolución de los riesgos y sistemas de protección.
- **Privacidad desde el diseño y por defecto:** los nuevos servicios, sistemas y procesos incorporan los requisitos de privacidad desde su concepción y aplican la configuración más protectora por defecto.
- **Responsabilidad proactiva:** DIVIDEND REFUND documenta y demuestra el cumplimiento de sus obligaciones en materia de seguridad y de protección de datos.

## 6. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN Y LA PRIVACIDAD

DIVIDEND REFUND se mantiene como objetivo estratégico documentar, controlar, mantener y mejorar progresivamente el Sistema de Gestión y el cumplimiento de los requisitos de las normas de referencia ISO/IEC 27001:2022 e ISO/IEC 27701:2019.

En particular, DIVIDEND REFUND establece como objetivos de Seguridad de la Información y Privacidad los siguientes:


- Garantizar la **protección de la información.**

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 8 de 17

- **Seguridad física:** DIVIDEND REFUND emplaza los sistemas de información en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad.
- **Control de acceso:** DIVIDEND REFUND limita el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de mecanismos de identificación, autenticación y autorización adaptados a la criticidad de cada activo.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** DIVIDEND REFUND contempla los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información.
- **Garantizar la prestación continuada de los servicios:** DIVIDEND REFUND implanta los procedimientos adecuados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio.
- **Protección de datos:** DIVIDEND REFUND adopta las medidas técnicas y organizativas necesarias para gestionar los riesgos derivados del tratamiento de datos personales.
- **Cumplimiento:** DIVIDEND REFUND adopta las medidas técnicas y organizativas necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

## 7. MISIÓN

La misión de DIVIDEND REFUND es ofrecer soluciones especializadas y eficaces en la documentación en fuente y reclamación de la doble retención sobre dividendos extranjeros, defendiendo con rigor los intereses de sus clientes ante las administraciones fiscales internacionales. DIVIDEND REFUND se mantiene permanentemente actualizada en todos

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 9 de 17

los aspectos regulatorios, garantizando eficiencia, seguridad y cumplimiento normativo en cada paso del proceso de recuperación de retenciones.

## 8. DESARROLLO DE LA POLÍTICA


El Comité de Seguridad de la Información y Privacidad de DIVIDEND REFUND ha aprobado el desarrollo de un sistema de gestión de seguridad de la información y privacidad que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles de las normas ISO 27001 y 27701. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información y Privacidad la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de ésta, para su aprobación por parte del Director General de DIVIDEND REFUND.

La presente Política de SGSI y Privacidad es de obligado cumplimiento y se estructura a nivel documental, en los siguientes niveles jerárquicos:

- **Primer nivel:** Política del Sistema de Gestión Seguridad de la Información y Privacidad.
- **Segundo nivel:** Normativas de Seguridad y Privacidad.
- **Tercer nivel:** Procedimientos de Seguridad y Privacidad.

El personal de DIVIDEND REFUND y terceras empresas, deberán conocer además de esta Política, todas las normativas, procedimientos, instrucciones técnicas, u otra documentación que pueda afectar en el desempeño de sus funciones.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 10 de 17

### 8.1. Primer nivel normativo: Política del SGSI/PIMS.

La Política del SGSI/PIMS constituye el instrumento normativo al más alto nivel en la estructura normativa de la seguridad y privacidad de DIVIDEND REFUND. Deberá ser aprobada por el Director General de DIVIDEND REFUND.

### 8.2. Segundo nivel normativo: Normas de Seguridad y Privacidad.

Las Normas son instrumentos de nivel medio que abarcan un área determinada de la seguridad. El órgano responsable de su aprobación es el Comité de Seguridad y Privacidad de DIVIDEND REFUND.

### 8.3. Tercer nivel normativo: Procedimientos e Instrucciones Técnicas.

Los Procedimientos e Instrucciones Técnicas son instrumentos de nivel inferior, redactados con un mayor nivel de detalle, aplicables a un ámbito específico. El Responsable de su aprobación es el Responsable del SGSI.

## 9. ORGANIZACIÓN DE LA SEGURIDAD

### 9.1. Roles o perfiles de seguridad y privacidad


Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y privacidad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- **Responsable del Sistema de Gestión Seguridad de la Información:** D. Diego Barreno

### 9.2. Comité de Seguridad de la Información y Privacidad

DIVIDEND REFUND ha constituido un Comité de Seguridad de la Información y Privacidad, como órgano colegiado, y está formado por los siguientes miembros:

- Director General: Director General de DIVIDEND REFUND.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 11 de 17

- Miembros:
  - ✓ Responsable del SGSI
  - ✓ Delegado de Protección de Datos

Con carácter opcional, otros miembros de DIVIDEND REFUND podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados ya sean de carácter interno, externo o mixto.


El Comité celebrará sus sesiones en las dependencias de DIVIDEND REFUND o de forma remota con periodicidad semestral previa convocatoria al efecto realizada por el Director General de dicho Comité. En todo caso, el Comité podrá celebrar reuniones extraordinarias cuando existan circunstancias que lo requieran.

### 9.3. Responsabilidades

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

#### **Funciones del Responsable del Sistema de Gestión de Seguridad de la Información (RSGSI)**

- Mantener y verificar el nivel adecuado de seguridad y privacidad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Gestionar, supervisar y mantener la seguridad física de las instalaciones de DIVIDEND REFUND.
- Promover la formación y concienciación en materia de seguridad y privacidad.


	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 12 de 17

- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad y privacidad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Comité de Seguridad de la Información y Privacidad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y privacidad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.


### **Funciones del Comité de Seguridad de la Información y Privacidad**

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información y Privacidad, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad y Privacidad de la Información.
- Asesorar en materia de Seguridad de la Información y Privacidad.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información y Privacidad. Para ello se encargará de:

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 13 de 17

- ✓ Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información y Privacidad, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- ✓ Proponer planes de mejora de la Seguridad de la Información y Privacidad, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- ✓ Velar porque la Seguridad de la Información y Privacidad se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- ✓ Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- ✓ Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- ✓ Elaborar y revisar regularmente la Política del SGSI y Privacidad para su aprobación por el órgano competente.
- ✓ Elaborar las normativas de Seguridad y Privacidad de la Información para su aprobación en coordinación con la Dirección General.
- ✓ Verificar los procedimientos de seguridad de la información y privacidad y demás documentación para su aprobación.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 14 de 17

- ✓ Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y Privacidad y, en particular en materia de protección de datos de carácter personal.
- ✓ Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información y Privacidad.
- ✓ Promover la realización de las auditorías periódicas de seguridad de la información y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.


#### 9.4. Procedimientos de designación

La creación del Comité de Seguridad de la Información y Privacidad, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por el Director General de DIVIDEND REFUND y comunicada a las partes interesadas.

Los miembros del Comité, así como los roles de seguridad serán revisados cada tres años o con ocasión de vacante.

#### 9.5. Matriz RACI: matriz de asignación de responsabilidades

Tarea	DG	RSGSI
Política de Seguridad	A	R
Análisis de Riesgos		A/R
Declaración de aplicabilidad (SOA)		A/R
Normas y procedimientos de S.I		A/R
Respuesta incidentes de seguridad	I	A/R
Seguridad del ciclo de vida de los servicios y sistemas de información		C

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 15 de 17

**A: Accountable (toma la decisión, autoriza y aprueba.**  
**R: Responsable (es responsable de la realización del trabajo**  
**C: Consulted (se le consulta antes de tomar la decisión).**  
**I: Informed (se le informa de las decisiones tomadas)**


## 10. RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad de la Información y Privacidad de DIVIDEND REFUND se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad y privacidad.

## 11. DATOS DE CARÁCTER PERSONAL

DIVIDEND REFUND solo tratará datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso conforme a la Política de Protección de Datos Personales aprobada por la Presidencia de DIVIDEND REFUND.

De conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general 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, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 16 de 17

## 12. TERCERAS PARTES

Cuando preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política del Sistema de Gestión de Seguridad de la Información y Privacidad. DIVIDEND REFUND definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad y/o privacidad, así como el resto de las actuaciones que DIVIDEND REFUND lleve a cabo en materia de Seguridad y Privacidad en relación con otros organismos.


Cuando DIVIDEND REFUND utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política del Sistema de Gestión de Seguridad y Privacidad y de la Política de Uso de Activos existente que atañe a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad y privacidad, al menos al mismo nivel que el establecido en esta Política de SGSI y Privacidad.

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

## 13. MEJORA CONTINUA

DIVIDEND REFUND define un conjunto de indicadores de los diferentes procesos y áreas de la organización cuyo control y seguimiento se efectuará periódicamente. Anualmente,

	<b>Política del Sistema de Gestión de Seguridad de la Información y Privacidad</b>	
	VERSIÓN 1	Pág. 17 de 17

durante la Revisión del Sistema, se establecerán los objetivos de Seguridad y Privacidad de la información, se planificará su seguimiento periódico y el análisis de su cumplimiento.

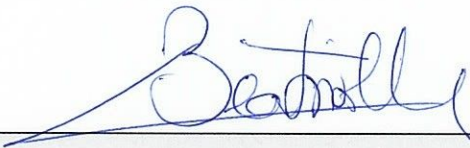
La gestión de la seguridad de la información y privacidad es un proceso sujeto a actualización permanente. Por ello, es necesario que DIVIDEND REFUND implante un proceso de mejora continua que comportará, entre otras, las siguientes actuaciones:

- Revisión de la Política del Sistema de Gestión de Seguridad de la Información y Privacidad.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas y externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de normas y procedimientos.

Para DIVIDEND REFUND, la gestión adecuada de la seguridad de la información y privacidad constituye un reto continuo y colectivo, necesario para la continuidad de la Entidad.

#### 14. APROBACIÓN DEL DOCUMENTO

Declaro aprobada la Política del Sistema de Gestión de Seguridad de la Información y Privacidad de DIVIDEND REFUND que se recoge en este documento, debiendo ser comunicada para el conocimiento general de todos los empleados de la entidad, lo que facilitará su cumplimiento y seguimiento.


26 de febrero de 2026 Director General de DIVIDEND REFUND