TERMINALES CANARIOS

1ª Versión

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

TERMINALES CANARIOS

Contenido

TERMINALES CANARIOS

Control de versiones.

Versión	Fecha	Descripción	Autor
1.0	17/11/2025	Versión Inicial del Documento	Responsable de Seguridad de la Información

TERMINALES CANARIOS

1. Objeto

Esta política tiene por objeto facilitar las directrices que deben seguirse para proteger la información de Terminales Canarios S.L. frente a una amplia gama de amenazas, con el fin de:

- Garantizar la seguridad de las operaciones realizadas mediante los Sistemas de Información.
- Minimizar los riesgos de daño.
- Asegurar el cumplimiento de los objetivos de Terminales Canarios S.L.

Terminales Canarios S.L. tiene la voluntad de lograr que los principios de la Política de Seguridad de la Información formen parte de su cultura, para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información basado en un estándar reconocido internacionalmente.

La Dirección de Terminales Canarios S.L. respalda esta Política de Seguridad de la Información y se compromete a proporcionar los recursos necesarios para su correcta implantación y cumplimiento

2. Alcance

Esta política aplica a toda la información que trata y servicios que presta Terminales Canarios S.L. Es de obligado cumplimiento para todo el personal que acceda a los sistemas de información de Terminales Canarios S.L.

La política de seguridad de la información es vinculante para todo el personal externo a Terminales Canarios S.L., a través de los contratos de prestación de servicios o acuerdos con terceros.

3. Marco Normativo

La presente política de seguridad se desarrolla en el marco normativo establecido por las siguientes leyes y normas:

- 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).
- Directiva (UE) 2022/2555 del Parlamento Europeo del 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de

ciberseguridad en toda la Unión
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- ISO 27001:2022 – Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de Gestión de la Seguridad de la Información – Requisitos.

4. Misión y servicios prestados

Terminales Canarios, S.L. es una empresa constituida en 1993 y dedicada a la prestación de servicios logísticos de recepción, almacenamiento y suministro de combustibles y lubricantes en las Islas Canarias.

Terminales Canarios desempeña un papel fundamental en la cadena logística vinculada a las soluciones de movilidad en el Archipiélago, operando con un firme compromiso hacia la sostenibilidad y con la aspiración irrenunciable de convertirse en una compañía de “Cero Emisiones Netas”.

Misión en materia de Seguridad de la Información

La misión de Terminales Canarios en el ámbito de la Seguridad de la Información es garantizar la confidencialidad, integridad, disponibilidad y protección de la información que gestiona. Para ello, la compañía se compromete a asegurar la continuidad operativa, el cumplimiento normativo y la confianza de clientes, proveedores, empleados y otros grupos de interés, mediante la implementación de controles, procesos y buenas prácticas alineados con los estándares nacionales e internacionales.

5. Cumplimiento Principios Básicos y aplicación de Requisitos Mínimos

Terminales Canarios se compromete a alinear su Sistema de Seguridad de la Información con los requisitos establecidos por la Directiva NIS2, la Ley de Coordinación y Gobernanza de la Ciberseguridad que la transpone al ordenamiento jurídico español y las buenas prácticas definidas por la norma ISO 27001. Para ello, la organización adoptará las medidas técnicas, organizativas y de gestión necesarias que garanticen un nivel adecuado de protección, resiliencia y continuidad, integrando estos marcos normativos y estándares como referencias para la mejora continua de su seguridad.

Los principios básicos constituyen las directrices fundamentales que deben considerarse en toda actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Seguridad como proceso integral:** La seguridad de la información se abordará como un proceso transversal e integrado en todas las operaciones de la compañía.
- **Gestión de la seguridad basada en los riesgos:** La toma de decisiones en materia de seguridad se fundamentará en un enfoque de gestión de riesgos.
- **Prevención, detección, respuesta y conservación:** Se establecerán medidas para prevenir incidentes, detectar actividades anómalas, responder de forma eficaz y conservar las evidencias necesarias.
- **Existencia de líneas de defensa:** La seguridad incorporará diferentes niveles de control y verificación que actúen como líneas de defensa complementarias.
- **Vigilancia continua:** Se realizará una supervisión continua de los sistemas y servicios con el fin de identificar amenazas y garantizar su protección.
- **Reevaluación periódica:** Los riesgos, controles y procesos de seguridad se revisarán periódicamente para asegurar su adecuación y eficacia.
- **Diferenciación de responsabilidades:** Se definirán roles, funciones y responsabilidades específicas para garantizar una gestión ordenada y eficaz de la seguridad de la información.

Y por ello, se desarrollará aplicando los siguientes requisitos mínimos:

- **Organización e implantación del proceso de seguridad:** Terminales Canarios establecerá la estructura y los procedimientos necesarios para implantar un proceso de seguridad eficaz.
- **Análisis y gestión de los riesgos**: Se realizarán análisis de riesgos periódicos y se aplicarán medidas proporcionales para su tratamiento.
- **Gestión de personal**: La compañía garantizará que el personal conozca sus responsabilidades y recibirá la formación necesaria en materia de seguridad de la información.
- **Profesionalidad**: Se promoverá un comportamiento profesional y ético en el uso y manejo de los activos de información.
- **Autorización y control de los accesos**: Se aplicarán controles de acceso basados en la necesidad de uso y se revisarán periódicamente las autorizaciones concedidas.
- **Protección de las instalaciones**: Las instalaciones serán protegidas mediante medidas físicas y operativas que eviten accesos no autorizados y salvaguarden los activos críticos.
- **Adquisición de productos de seguridad y contratación de servicios de seguridad:** La adquisición de tecnologías y servicios incluirá criterios de seguridad que garanticen su idoneidad y fiabilidad desde su origen.
- **Mínimo privilegio:** Los accesos a los sistemas e información se concederán únicamente con los privilegios estrictamente necesarios para el desempeño de cada función.
- **Integridad y actualización del sistema**: Los sistemas serán mantenidos

actualizados y protegidos para preservar su integridad y reducir vulnerabilidades.

- **Protección de la información almacenada y en tránsito**: La información será protegida mediante controles que garanticen su confidencialidad, integridad y disponibilidad tanto en reposo como durante su transmisión.
- **Prevención ante otros sistemas de información interconectados**: Se adoptarán medidas preventivas para mitigar los riesgos derivados de la interconexión con terceros y otros sistemas de información.
- **Registros de la actividad y detección de código dañino**: Los sistemas generarán registros de actividad y dispondrán de mecanismos para detectar código malicioso o comportamientos anómalos.
- **Incidentes de seguridad**: Se implantará un proceso estructurado para la notificación, gestión y resolución de incidentes de seguridad de forma rápida y eficaz.
- **Continuidad de la actividad**: Se establecerán medidas de continuidad operativa que permitan mantener o restablecer los servicios esenciales ante incidentes o contingencias.
- **Mejora continua del proceso de seguridad:** El proceso de seguridad será objeto de una revisión y mejora continua para garantizar su adecuación frente a cambios tecnológicos, normativos y operativos.

6. Modelo de Gobernanza

La estructura organizativa de la gestión de la seguridad de la información está compuesta por los siguientes roles:

- **Comité de Seguridad de la Información**: Se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información y está formado por:
  - Presidente: Director General.
  - Secretario: Responsable Seguridad de la Información
  - Vocales:
    - Responsable del Sistema
    - Director de Recursos Humanos y Asesoría Jurídica
    - Director de Operaciones
- **Responsable de Seguridad de la Información**: encargado de definir, supervisar y coordinar la implementación de las medidas de seguridad de la información, así como de garantizar la adecuada gestión de riesgos y el cumplimiento de la normativa aplicable en materia de ciberseguridad.
- **Delegado de Protección de Datos**: debe supervisar el cumplimiento del

reglamento y cooperar con la Agencia Española de Protección de Datos.

- **Responsable del Servicio:** encargado de determinar los requisitos de seguridad de los servicios prestados.
- **Responsable de Sistemas:** será el encargado de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
- **Responsable de la Información:** encargado de determinar los requisitos de la información tratada.

Como parte integral de este modelo, se ha definido un proceso formal de seguimiento y evaluación continua mediante la Revisión por el Comité de Seguridad, donde se analiza el estado de la seguridad en base a indicadores, evaluación de riesgos y cumplimiento de objetivos.

6.1 Funciones del Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Seguridad de la Información, en adelante Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad que coordinará las actividades y controles de seguridad establecidos en Terminales Canarios S.L. y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad de la información. Es el encargado de impulsar la implementación de la presente Política de Seguridad.

El Comité de Seguridad **se reunirá con carácter ordinario al menos dos veces al año**, y con carácter extraordinario cuando existan razones de urgencia debidamente justificadas, o a solicitud de su Presidencia o del responsable de Seguridad.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones, así como invitar a dicho personal a las reuniones con voz y sin voto.

El responsable de Seguridad de la Información actuará como secretario, con voz y voto, y como tal:

- Convocará las reuniones del Comité de Seguridad de la Información
- Levantará actas de las reuniones del Comité de Seguridad de Información.
- Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Se convocará al resto de personas con responsabilidades según las necesidades del Comité de Seguridad de la Información.

Sus funciones son:

- Atender las inquietudes del Consejo de Administración y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información al Consejo de Administración.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la Información.
- Elaborar y aprobar los requisitos de formación.
- Monitorizar y aprobar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

6.2 Funciones del responsable de Seguridad de la Información

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la 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 y/o 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, 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.
- Aprobar la Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas.
- 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.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por Dirección.
- Actuará como Secretario del Comité de Seguridad de la Información, realizando las siguientes funciones:
    - Convocar las reuniones del Comité de Seguridad de la Información.
    - Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
    - Elaborar el acta de las reuniones.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Coordinación con Autoridades y Gestión de Incidentes

- Gestionar los incidentes de ciberseguridad, desde su detección hasta su resolución, incluyendo la colaboración en su investigación.
- Informar de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad del sistema.
- Notificar sin dilación indebida a las autoridades de control, a través de los CSIRT nacionales de referencia, los incidentes que tengan efectos perturbadores en la prestación de servicios y las vulnerabilidades detectadas.
- Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emitidas por la autoridad de control, tanto para la operativa habitual como para la subsanación de deficiencias.
- Recopilar, preparar y suministrar información o documentación a la autoridad de control y a los CSIRT nacionales, ya sea por solicitud o por iniciativa propia.

Formación, Supervisión y Relación con Terceros

- Promover la formación y concienciación en materia de seguridad de la información.
- Supervisar el cumplimiento, por parte de empresas externas y proveedores, de los criterios de seguridad de la información establecidos por la organización.

6.3 Funciones de los Responsables de Información y de los Servicios (RS)

- Establecer los requisitos de seguridad aplicables a la Información (niveles de seguridad de la Información) y a los Servicios (niveles de seguridad de los servicios), 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 y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.
- Tiene la responsabilidad última del uso que se haga de determinados servicios e información y, por tanto, de su protección.

6.4 Responsable del Sistema (RSIS)

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar 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.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al Responsable de Seguridad y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema.

6.5 Funciones del delegado de Protección de Datos

En cumplimiento del artículo 39 del RGPD y 37 de la LOPDGDD, las funciones del Delegado de Protección de Datos (DPO) podrán ser desempeñadas por una figura interna o externa designada por la organización conforme a la normativa vigente.

Sus funciones son:

- Asegurar el cumplimiento de la normativa vigente, mediante la recolección de información, su análisis y revisión del cumplimiento en relación con los tratamientos de datos llevados a cabo en el seno de la organización realizando cuantas recomendaciones fuesen necesarias para garantizar el cumplimiento.
- Informar y asesorar a la organización, y a los usuarios que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de la normativa vigente en materia de Protección de Datos.
- Supervisar el cumplimiento de lo dispuesto en normativa de seguridad y de las políticas internas de la organización, en materia de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Comunicar la existencia de una vulneración relevante en materia de protección de datos a los órganos de administración y dirección de Terminales Canarios S.L., proponiendo las medidas necesarias para evitar la persistencia en esa conducta.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos (en adelante, “EIPD”) y supervisará su aplicación, asesorando entre otras cuestiones sobre:
    - La obligatoriedad o idoneidad sobre la realización de un EIPD.
    - La definición de la metodología a emplear en su desarrollo.
    - La idoneidad de realizar la evaluación por parte de la organización, de forma interna o la posible externalización de esta.
    - La definición de las medidas a implementar.
    - La determinación de la correcta ejecución de la EIPD y el análisis sobre si las conclusiones cumplen con la normativa.
- Cooperar con la Agencia Española de Protección de Datos cuando ésta lo requiera, actuando como punto de contacto con ésta para cuestiones relativas al tratamiento de datos.
- El delegado de Protección de datos desempeñará sus funciones de forma independiente prestando atención a los riesgos asociados a las operaciones de tratamiento. Para ello debe ser capaz de:
    - Recabar información para determinar las actividades de tratamiento.
    - Analizar y comprobar la conformidad de las actividades de tratamiento.
    - Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
    - Recabar información para supervisar el registro de las operaciones de tratamiento.
    - Asesorar en el principio de la protección de datos por diseño y por defecto, en todas las fases del ciclo de vida del dato.

- Asesorar sobre si se lleva a cabo o no las EIPD, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.
- Atender las cuestiones de los interesados en lo que respecta al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del Reglamento General de Protección de Datos.

7. Procedimiento de Designación

Los distintos responsables serán designados por el Consejo de Administración de Terminales Canarios S.L. Se nombrarán y documentarán en las actas de reunión las nuevas designaciones y renovaciones periódicamente cada dos años o de acuerdo con las necesidades de la organización y siguiendo el principio de separación de funciones.

8. Resolución de conflictos

Para la correcta coordinación de la organización de la seguridad entre los responsables se debe establecer una jerarquía, en esta se pueden distinguir los siguientes niveles:

- **Órganos de Gobierno**: determinan los objetivos que Terminales Canarios S.L. se propone alcanzar y responde a que se alcancen.
- **Dirección Ejecutiva**: comprenden las necesidades de los departamentos y cómo se coordinan entre sí para alcanzar los objetivos propuestos por la Dirección.
- **Operaciones**: se centran en realizar y gestionar las actividades.

En caso de que los responsables encargados de la organización de la seguridad de Terminales Canarios S.L. no sean capaces de establecer un objetivo, misión o conclusión en común, con el fin de evitar conflictos y preservar el buen clima de Terminales Canarios S.L., se deberá resolver la situación en el orden jerárquico indicado.

La jerarquía a la que deben atender los responsables es la siguiente:

Gobierno	Comité de Seguridad
Ejecutivo	Responsable de Seguridad de la Información
Operaciones	Responsable de Sistemas / Responsable del Servicio / Responsable de la Información

9. Datos de Carácter Personal

Atendiendo a los tratamientos de datos personales realizados por Terminales Canarios S.L., se ha establecido una Política de Protección de Datos Personales conforme al Reglamento General de Protección de Datos (RGPD) la Ley Orgánica de Protección de Datos (LOPDGDD) y demás normativa aplicable, que define los principios, responsabilidades y medidas aplicables al tratamiento de datos personales. Esta política garantiza la legitimidad, licitud, transparencia y seguridad en el tratamiento de los datos, protege los derechos de los interesados y contempla procedimientos para la gestión de incidentes, transferencias internacionales, evaluaciones de impacto y cumplimiento normativo. Su implementación es obligatoria para toda la organización y está sujeta a revisiones periódicas.

Además, cuenta con un Registro de Actividades del Tratamiento detallando los tratamientos afectados y los responsables correspondientes, junto con los análisis de riesgos y evaluación de impacto realizados sobre los tratamientos. Terminales Canarios S.L. garantiza el cumplimiento de las medidas de seguridad establecidas en esta política para todos los tratamientos que incluyan datos personales, así como la aplicación de los principios de privacidad exigidos por la normativa vigente.

10. Desarrollo de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será complementada con otros documentos (normas, guías y procedimientos de seguridad). El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad. Para su organización se ha definido un procedimiento para la gestión de la documentación, que establece las directrices para Terminales Canarios S.L., gestión y acceso.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de esta, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

11. Terceras partes

Cuando Terminales Canarios S.L. utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, 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 está adecuadamente concienciado en materia

de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el responsable de Información y Servicio antes de seguir adelante.

Los proveedores de servicios externalizados que mantengan relación con la seguridad de los elementos del sistema de información de Terminales Canarios S.L., salvo por causa justificada y documentada, deberán designar una Persona de Contacto (POC) que facilite y promueva una coordinación adecuada entre las partes en materia de seguridad. El POC será el responsable de Seguridad de la empresa contratada, quien deberá canalizar y supervisar tanto el cumplimiento de los requisitos de seguridad del servicio prestado como las comunicaciones relacionadas con la seguridad de la información, la gestión de riesgos y la gestión de incidentes. En su defecto, este rol podrá ser asumido por el jefe del servicio, jefe de proyecto u otra figura equivalente designada por la empresa.

12. Obligaciones del Personal

La Política de Seguridad debe ser leída, comprendida y aplicada en su integridad por todos los empleados de Terminales Canarios S.L. El incumplimiento de cualquier obligación establecida en la presente Política o de la normativa interna, podrá ser objeto de investigación, documentación y reporte al órgano interno competente según el caso y de acuerdo con la legislación vigente de aplicación. En base al resultado de las investigaciones, se podrán adoptar medidas disciplinarias.

70647939N SAMUEL LEONARDO PEREZ (C:B38318572)
Firmado digitalmente por 70647939N SAMUEL LEONARDO PEREZ (C:B38318572)
Fecha: 2026.03.17 09:45:37 Z

42871840R JUAN LUIS SANTANA (R: B38318572)
Firmado digitalmente por 42871840R JUAN LUIS SANTANA (R: B38318572)
Fecha: 2026.03.17 09:58:31 Z

43831748G SARA ORIHUELA (R: B38318572)
Firmado digitalmente por 43831748G SARA ORIHUELA (R: B38318572)
Fecha: 2026.03.17 11:14:29 Z