POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Referencia	31_Política de Seguridad de la Información_4_2024
Título de la Norma	Política de Seguridad de la Información
Ámbito geográfico	Global
Categoría	Política
Fecha de aprobación	19 de diciembre de 2024
Órgano de aprobación	Consejo de Administración
Versión vigente	19 de diciembre de 2024

Información importante sobre este documento	
Identificación del documento	Política de Seguridad de la Información
Referencia	31_Política de Seguridad de la Información_4_2024
Ámbito geográfico de aplicación	Global
Apartado de otras Normas que desarrolla	Código de Conducta
Normas que sustituye	31_Política de Seguridad de la Información_3_2022
Normas que deroga	31_Política de Seguridad de la Información_3_2022
Responsable principal de su vigilancia	*Director de Inteligencia Artificial y Ciberseguridad (CISO)*
Órgano o Departamento que la propone	*Comisión de Auditoría y Sostenibilidad*
Autor	*Director de Inteligencia Artificial y Ciberseguridad (CISO)*
Órgano de aprobación	*Consejo de Administración*
Fecha de aprobación del texto vigente	19 de diciembre de 2024
Fecha de aplicación	19 de diciembre de 2024
Publicada y accesible en	Extra e Intra-Net

Control de versiones				
Versión	**Fecha**	**Órgano de aprobación**	**Autor**	**Resumen de cambios**
1	19 de diciembre de 2024	Consejo de Administración	*Director de Inteligencia Artificial y Ciberseguridad (CISO)*	Se deroga el texto anterior. Aplicación de Directiva NIS 2 de Ciberseguridad, cuyo plazo de transposición

				venció el 17 de octubre de 2024 y del Código de Buen Gobierno de la Ciberseguridad, aprobado en junio de 2023 por la Comisión Nacional del Mercado de Valores

ÍNDICE

1. Introducción

El Consejo de Administración de ACS, Actividades de Construcción y Servicios, S.A. (en lo sucesivo, "**ACS**" o la "**Sociedad**") en su condición de sociedad cotizada, tiene legalmente atribuida como facultad indelegable la determinación de las políticas y estrategias generales de ACS, facultades que han sido asimismo recogidas en los Estatutos del Consejo de Administración de ACS.

ACS y las sociedades que forman parte del Grupo del que la Sociedad es la entidad dominante (en lo sucesivo, el "**Grupo ACS**" o "**Grupo**") asumen el compromiso de garantizar la seguridad de la información y de las redes y los Sistemas de Información en los que se apoyan los diferentes procesos de negocio, con el fin de reforzar su Resiliencia Operativa Digital, alineando sus prácticas con la normativa vigente aplicable, así como con sus valores corporativos.

En este sentido, ACS se compromete a desarrollar e implantar las máximas capacidades en materia de seguridad de la información, con el fin de reducir las amenazas para la información, los Sistemas de Redes y de Información utilizados en la organización.

De conformidad con lo anterior, el Consejo de Administración de la Sociedad ha aprobado la presente *Política de Seguridad de la Información* (en lo sucesivo, la "**Política**"), que constituye la pieza angular del Sistema de Gestión de Seguridad de la Información de ACS y que se integra en el Sistema de Gobernanza de la Sociedad, teniendo proyección sobre el Grupo ACS.

2. Definiciones

Las siguientes definiciones se aplican a esta Política y a todos los procedimientos asociados con la misma en el seno de ACS, sin perjuicio de su proyección sobre el Grupo:

- ***Comité de Gobernanza y Compliance***: órgano de ACS al que se le asignan funciones propias de Compliance en general, así como específicas respecto de cada uno de los Ámbitos de Compliance identificados y, asimismo, funciones consultivas y de apoyo en materia de gobernanza con fines de coordinación cuando ello resulte necesario al Director de Gobierno Corporativo, al Director de Inteligencia Artificial y Ciberseguridad (CISO), al Director de Sostenibilidad y al Delegado de Protección de Datos (DPO).
- ***Ciberseguridad***: todas las actividades tendentes a garantizar, tanto la seguridad de la información, como la protección de las redes y Sistemas de Información, de los Usuarios de tales sistemas y de otras personas que puedan verse afectadas por las ciberamenazas.
- ***Datos Personales***: toda información sobre una persona física identificada o identificable. Esto incluye cualquier dato que, directa o indirectamente, pueda ser utilizado para identificar a una persona como nombres, fotografías, direcciones de correo electrónico, datos bancarios, información sobre redes sociales, ubicación, o dirección IP de un ordenador, entre otros. Los Datos Personales están protegidos por diversas legislaciones y se deben seguir prácticas

adecuadas para su recogida, tratamiento y almacenamiento de cara a respetar los derechos de privacidad de las personas involucradas.

- ***Director de Inteligencia Artificial y Ciberseguridad (CISO)***: responsable en materia de seguridad de las redes y de los Sistemas de Información.
- ***Control y Gestión de Riesgos*****:** actividades coordinadas para dirigir y controlar en ACS los Riesgos identificados.
- ***Gestión de Incidentes***: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y limitar un Incidente, resolviéndose e incorporando medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
- ***Incidente de Ciberseguridad*** o ***Ciberincidente***: suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por Sistemas de Redes y de Información o accesibles a través de ellos.
- ***Información***: activo principal de cualquier empresa que puede estar en formato físico, o digital y pueden estar determinados en ficheros de todo tipo (texto, imagen, multimedia, bases de datos…), pasando por los programas y aplicaciones que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.
- ***Profesional***: los miembros de los órganos de administración, directivos, trabajadores, colaboradores, estudiantes en prácticas y becarios, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, su nivel jerárquico, su ubicación geográfica o funcional y de la sociedad del Grupo ACS para la que presten sus servicios.
- ***Principio de autenticidad***: persigue garantizar que el origen y las identidades asociadas a la información son realmente los que aparecen en los atributos de esta. Este principio va unido al de no repudio, que consiste en asegurar que un Usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos.
- ***Principio de confidencialidad*****:** procura que la información solo sea accesible para los Usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.
- ***Principio de disponibilidad***: consiste en que la información esté accesible y se pueda utilizar de forma constante, asegurando la continuidad de los procesos y de la actividad. Este principio va unido al de resiliencia, que consiste en asegurar la capacidad de recuperación de los sistemas y la información tras un Incidente que impida el acceso temporal a los mismos.

- ***Principio de integridad***: pretende asegurar que los datos se mantendrán libres de modificaciones no autorizadas y que la información existente no ha sido alterada por personas o procesos no autorizados.
- ***Principio de trazabilidad***: busca la posibilidad de determinar en cada momento la identidad de las personas que acceden a la información y la actividad que desarrollan en relación con la misma, así como los distintos estados y rutas que ha seguido la información.
- ***Resiliencia Operativa Digital*****:** la capacidad de la entidad para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los Sistemas de Información que utiliza la entidad y que sustentan la prestación continuada de servicios y su calidad, incluso en caso de perturbaciones.
- ***Riesgo***: la posible pérdida o perturbación causada por un Incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal Incidente.
- ***Sistema de Gestión de Seguridad de la Información ("SGSI")*****:** conjunto de políticas y procedimientos de seguridad de la información que tratan de componer un sistema de organización y gestión, diseñado para implantar, mantener y mejorar dichas políticas. El SGSI trata de asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los Riesgos de seguridad de la Información teniendo en cuenta los Riesgos analizados dentro de los procesos de negocio de ACS, y cuya base es la presente Política.
- ***Sistema de Información***: un conjunto discreto de recursos de información que soportan aplicaciones o servicios de negocio, los cuales se organizan para obtener, procesar, mantener, utilizar, compartir, distribuir o disponer de la información.
- ***Sistema de Redes y de Información***: i) dispositivos interconectados; ii) sistemas de transmisión (se basan o no en una infraestructura permanente o en una capacidad de administración centralizada), los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos de red que no son activos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.
- ***Tratamiento de datos***: cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, o conjuntos de éstos, ya sea por procesos automatizados o no, como la recogida,

registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

- ***Usuario***: Cualquier persona vinculada a ACS por una relación civil o mercantil, así como clientes, proveedores, subcontratistas, consultores o cualesquiera otras personas o entidades a los que se autorice a utilizar, custodiar o acceder a las HIA Corporativas (tal y como se definen en la *Política de Inteligencia Artificial*).
- ***Vulnerabilidad***: cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado.

Salvo que se disponga expresamente lo contrario en cualquier apartado de la presente Política, las definiciones en singular incluyen el plural y viceversa.

3. Objeto

La presente Política tiene por objeto establecer los principios básicos y las reglas generales que permitan a ACS, con proyección sobre las sociedades del Grupo, desarrollar las estrategias, procedimientos y estándares de seguridad de la información a seguir para mantener un SGSI sólido, fortaleciendo el marco operativo y de control adecuado, alineados con los objetivos de negocio, para la gestión de la seguridad de la información de ACS.

De conformidad con lo anterior, la Política persigue desplegar en ACS con proyección sobre las sociedades del Grupo, procesos y tecnologías que garanticen la seguridad de la información, de las redes y de los Sistemas de Información y operaciones de ACS, minimizando los Riesgos y ciberamenazas a los que están expuestos, de manera que permitan cumplir su objeto social para con los clientes y otros grupos de interés, y por tanto garantizando la continuidad de la prestación de los servicios actuando preventivamente, supervisando la actividad diaria y reaccionando con diligencia a los Incidentes.

4. Ámbito de Aplicación

Esta Política es aplicable a toda la organización de ACS, así como a los proveedores y clientes que presten servicios o se relacionen con ACS, proyectándose además sobre las sociedades del Grupo ACS.

En aquellas sociedades participadas en las que esta Política no sea de aplicación, ACS promoverá en lo posible, a través de sus representantes en sus órganos de administración, el alineamiento de sus políticas con las de ACS.

Esta Política se proyectará también, en lo que proceda, a las uniones temporales de empresas, *joint ventures* y otras asociaciones equivalentes, ya sean estas nacionales o extranjeras, cuando cualesquiera de las sociedades que integran el Grupo ACS tengan el control de su gestión y siempre dentro de los límites legalmente establecidos.

5. Principios Generales de Actuación

ACS entiende la seguridad de la información como un elemento fundamental para proteger los activos de negocio, considerándola como un proceso integral basado en gestión y control de Riesgos con el fin de lograr sus objetivos y cumplir con su misión. En este sentido, ACS se compromete a dotar a las diferentes áreas de la organización de todos los recursos técnicos, humanos, materiales y organizativos necesarios para garantizar una adecuada gestión de la seguridad de las redes y Sistemas de Información de ACS.

Se establecerán procedimientos específicos para que todos los Profesionales y Usuarios conozcan, comprendan y cumplan con la Política y toda su normativa de desarrollo.

De conformidad con lo anterior, todos los Profesionales y Usuarios de ACS deberán respetar y guiar su actuación con base en los siguientes principios:

I. **Proceso integral basado en la gestión y control de riesgos:** ACS lleva a cabo una gestión de la seguridad de la información que se fundamenta en los principios de gestión y control de riesgos que se definen dentro de la política General de Control y Gestión de Riesgos del Grupo, y que se construye sobre la metodología común que se establece en el Sistema Integral de Control y Gestión de Riesgos incluido en dicha política:

- Identificación y evaluación de riesgos
- Definición de los niveles aceptables de riesgo
- Establecimiento de mecanismos de control y mitigación
- Fortalecimiento de la toma de decisiones
- Monitorización y revisión continua

Todo lo cual se refleja en el Plan Director de Seguridad que se actualiza de manera continua.

II. **Definición, desarrollo y mantenimiento**: para lograr la puesta en marcha de los objetivos, valores, estrategia y compromisos asumidos, ACS impulsará el desarrollo de un Sistema de Gestión integrado por los controles técnicos, legales y de gestión de la seguridad de la información necesarios para garantizar en todo momento el cumplimiento de los requisitos legales, reglamentarios y contractuales en la materia que le sean de aplicación.

III. **Promoción de una cultura de seguridad de la información**: ACS se compromete a promover de forma activa una cultura de seguridad de la información entre todos sus Profesionales, y Usuarios, ya sea internamente, o entre sus clientes y proveedores.

IV. **Gestión diaria:** lo cual implica el compromiso de ACS de proteger la seguridad de la información, de las redes y Sistemas de Información, diseñando medidas de seguridad robustas, alineadas con las necesidades de las diferentes partes interesadas, así como de la normativa vigente aplicable en la materia, para lo cual ACS aprobará las políticas y/o procedimientos específicos por materia que desarrollarán los principios y requisitos básicos de seguridad de la información establecidos en la presente Política.

V. **Protección proactiva**: de manera que se persiga proactivamente la salvaguarda de los niveles establecidos de confidencialidad, disponibilidad, autenticidad, trazabilidad e integridad parar sus activos de información y asegurar la Resiliencia Operativa Digital de ACS.

VI. **Mejora continua**: entendiendo la seguridad de la información como un eje transversal integrado en todas las áreas y procesos de negocio, buscando lograr un progreso ininterrumpido de todos los procesos vinculados al SGSI y a la gestión de la seguridad de la información, de las redes y de los Sistemas de Información, de tal forma que contribuya a que toda la operativa de ACS sea digitalmente resiliente.

Los referidos principios generales de actuación se proyectarán sobre las sociedades del Grupo ACS.

6. Requisitos básicos de seguridad de la información

Para llevar a cabo la gestión diaria de la seguridad, se procederá siempre conforme a los siguientes requisitos básicos:

- Establecer requerimientos de seguridad desde el diseño y por defecto.
- Prevención, detección, respuesta y conservación.
- Vigilancia continuada y reevaluación periódica.
- Diferenciación de responsabilidades.
- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los Riesgos.
- Gestión del personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.

- Mínimo privilegio.
- Integridad y actualización del Sistema de Información.
- Protección de la Información almacenada y en tránsito.
- Prevención ante otros sistemas de Información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.
- Seguridad en la cadena de suministro.
- Confiabilidad, seguridad y resiliencia.

Cada uno de estos requisitos se desarrollará por los correspondientes procedimientos y/o políticas específicas aprobadas internamente.

Toda la documentación de seguridad de la información que se desarrolle en ejecución de los mencionados principios y que integra el SGSI, se gestiona, estructura y conserva conforme a los procedimientos documentados que ACS ha desarrollado teniendo en cuenta la normativa, así como los estándares nacionales e internacionales que apliquen en cada caso.

Los referidos requisitos básicos de seguridad de la información y su desarrollo se proyectarán sobre las sociedades del Grupo ACS.

7. Gobernanza

La gobernanza de la seguridad de la Información en ACS es esencial para gestionar y mitigar potenciales Riesgos, para garantizar la toma de decisiones en función del riesgo real de la materialización de las amenazas sobre la organización, así como para la continuidad de las operaciones de negocio, siendo la presente Política una herramienta fundamental para la adecuada gestión y gobernanza de la seguridad de la información.

7.1. Directrices de gestión y supervisión

Corresponde al Consejo de Administración de ACS, a través de la presente Política y, en su caso, de otras normas corporativas en desarrollo de la misma, el establecimiento de la estrategia y directrices de gestión con proyección sobre el Grupo ACS en materia de seguridad de la Información.

A su vez, es competencia de la Comisión de Auditoría y Sostenibilidad a través de sus funciones de supervisión y control, velar por la implementación y desarrollo de la presente Política y de las medidas adoptadas en aplicación de la misma, así como revisar, y en su caso, proponer al Consejo de Administración la actualización de la presente Política.

Asimismo, corresponde a la Comisión de Auditoría y Sostenibilidad la supervisión de la eficacia del SGSI de ACS.

Para el ejercicio de sus funciones de supervisión, la Comisión de Auditoría y Sostenibilidad recibirá periódicamente del CISO información sobre su gestión.

7.2. Director de Inteligencia Artificial y Ciberseguridad (CISO) y del Comité de Gobernanza y Compliance

7.2.1. Principios de actuación

ACS, a través del CISO, observará y promoverá en ACS los siguientes principios en relación con la gobernanza de la seguridad de la información:

a) Principio de alineamiento estratégico y visión de futuro

Se considerará la seguridad de la información como una parte más del negocio, entendiéndose como una herramienta que ayuda a ACS a alcanzar sus objetivos, alineada con la misión y perspectiva del Grupo.

En consecuencia, ACS impulsará un enfoque holístico con el fin de que la seguridad de la información no sea considerada como un obstáculo, sino como parte de un vasto conjunto necesario para el desarrollo de su negocio.

b) Principio de ética y cumplimiento

Deberá guiar el gobierno de la seguridad de la información en ACS, no solo enfocándose en el cumplimiento de la normativa establecida, sino también en las buenas prácticas de seguridad y el uso ético de los recursos del Grupo.

Con el propósito de fomentar una acción ética y responsable, ACS impulsará la colaboración con las mejores prácticas en la materia, tanto dentro de ACS como en cada uno de los mercados en los que se encuentra y en su conexión con los diversos grupos de interés.

c) Principio de responsabilidad

La seguridad de la información es un campo interdisciplinar y complejo que impacta en todas las operaciones de una entidad. Por lo tanto, necesita de un liderazgo apropiado y una estructura que, para ser establecida y administrada correctamente, debe estar conformada por profesionales con la formación y experiencia idóneas.

d) Principio de independencia y autonomía

Deberá actuar con total independencia y autonomía en el desempeño de sus funciones, garantizando así su imparcialidad y objetividad, y dependerá funcionalmente de la Comisión de Auditoría y Sostenibilidad.

7.2.2. Funciones del Director de Inteligencia Artificial y Ciberseguridad (CISO)

Corresponderá al Director de Inteligencia Artificial y Ciberseguridad (CISO):

- Revisar la presente Política, asegurando que cumple con la normativa aplicable a ACS y su Grupo, así como con las mejores prácticas del sector. En este sentido, cuando lo considere conveniente, podrá presentar propuestas de modificación de la presente Política a la Comisión de Auditoría y Sostenibilidad, para su elevación, a su vez, al Consejo de Administración.
- Revisar y promover la mejora continua del SGSI de ACS, incluyendo en su caso, la identificación y evaluación de nuevos Riesgos asociados al SGSI.
- Coordinar los planes de continuidad de los sistemas de información de las diferentes áreas de ACS para asegurar una actuación sin fisuras en el caso de que deban ser activados.
- Informar regularmente a través del Plan Director de Seguridad, a la alta dirección y diferentes áreas de ACS en relación con medidas de seguridad y control adoptadas, recomendando posibles actuaciones al respecto
- Coordinar y monitorizar el desempeño de los procesos de gestión de Incidentes de Seguridad en materia de seguridad de la información.
- Promover procesos de auditorías periódicas para verificar el cumplimiento de la normativa aplicable.
- Promover la formación y el desarrollo de habilidades relacionadas con la seguridad de la información en ACS.
- Velar por el cumplimiento de la normativa de aplicación.
- Aprobar procedimientos, normas o protocolos internos dirigidos al desarrollo e implementación de la presente Política en ACS.
- Establecer y fomentar la seguridad de la información, además de participar en la toma de decisiones y estrategias en este campo, asumiendo la responsabilidad de proporcionar un informe periódico apropiado y a los niveles adecuados, sobre los Riesgos asociados a la seguridad de la información, junto con los mecanismos de mitigación y control que sean requeridos.

Corresponderá asimismo al CISO hacer el seguimiento del desarrollo de estas funciones por los órganos o instancias equivalentes de las sociedades del Grupo con la finalidad de supervisar la implementación de los principios y compromisos que inspiran la presente Política, pudiendo recabar de dichas sociedades cuanta información considere para el cumplimiento de esta función de coordinación a nivel de Grupo.

Para el ejercicio de estas funciones, el CISO contará con el apoyo del Comité de Gobernanza y Compliance.

7.3. Descentralización y coordinación a nivel del Grupo

El Grupo ACS se estructura conforme a un modelo de gestión descentralizado y desarrolla su actividad a través de un amplio grupo de sociedades, que comparten la cultura y valores del Grupo ACS, al tiempo que cada una opera de manera independiente en sus respectivos ámbitos funcionales y de responsabilidad.

En este sentido, las estrategias, procedimientos y estándares de seguridad de la información a seguir para mantener un SGSI sólido, corresponden a las distintas sociedades del Grupo en el marco de sus respectivos ámbitos funcionales y de responsabilidad.

A este respecto, las sociedades del Grupo ACS serán responsables de implementar, supervisar, adecuar y gestionar las estrategias y modelo organizativo en materia de seguridad de la información dentro de sus respectivos ámbitos de actuación, estableciendo sus propias políticas y normas internas en la materia considerando la normativa que en cada caso resulte de aplicación y sus propias características, respetando los principios básicos establecidos en esta Política.

En todo caso, las sociedades del Grupo ACS proporcionarán toda la información necesaria para la definición de la estrategia del Grupo en materia de seguridad de la Información y, asimismo, para el cumplimiento de cuantas obligaciones corresponden a ACS en dicha materia conforme a la normativa aplicable.

8. Control y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los Riesgos a los que están expuestos. ACS realiza de forma periódica y continuada un análisis de riesgos de las amenazas que afectan a la seguridad de la información, tal y como se desarrolla en el procedimiento correspondiente.

9. Gestión de Incidentes

Las áreas que conforman ACS deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por Incidentes de ciberseguridad. Para ello, de

conformidad a lo recogido en el procedimiento correspondiente, dichas áreas deben implementar las medidas mínimas de seguridad determinadas por la normativa aplicable, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

10. Seguimiento, Interpretación y Revisión

10.1. Seguimiento

El cumplimiento de esta Política será supervisado por el CISO. Se establecerán mecanismos de auditoría y revisión periódica para asegurar que el SGSI cumpla con los estándares establecidos.

En caso de tener algún problema, o detectar un Incidente que pueda afectar al funcionamiento o seguridad de los Sistemas de Redes y sistemas, y/o la seguridad de las mismas, este se deberá comunicar inmediatamente al CISO a través de los cauces habilitados a tales efectos y que se determinarán en los procedimientos de SGSI.

A modo de métrica, se documentarán mensualmente los resultados del proceso de gestión de Vulnerabilidades, incluyendo el listado de Vulnerabilidades gestionadas, así como si han podido ser corregidas y, en su caso, las medidas adoptadas.

El incumplimiento de la presente Política puede conllevar responsabilidades legales de diversa naturaleza según dispone la legislación vigente, dando derecho a ACS, si así se estimara necesario, a iniciar las acciones legales que procedan.

10.2. Interpretación

El órgano de contacto para cualquier duda y/o consulta en relación con la interpretación y ejecución de la presente Política será el CISO. La comunicación con el CISO se llevará a cabo por los cauces habilitados al efecto.

10.3. Revisión y Actualización

Esta Política será revisada y, en su caso, actualizada periódicamente para adaptarse a las necesidades y/o cambios regulatorios, organizativos, técnicos y de procesos de ACS y su Grupo, así como para incorporar las mejores prácticas identificadas en el SGSI.

La modificación y/o actualización de la presente Política será aprobada por el Consejo de Administración de ACS, previo informe de la Comisión de Auditoría y Sostenibilidad.

11. Difusión de la Política

Esta Política se publicará en la página web corporativa de ACS con el consiguiente conocimiento y asunción de su contenido íntegro por parte de los Profesionales y Usuarios.

Sin perjuicio de ello, ACS llevará a cabo periódicamente acciones de comunicación, formación y sensibilización para la comprensión y puesta en práctica de esta Política, así como de sus actualizaciones. Asimismo, ACS difundirá esta Política en las sociedades del Grupo ACS.

En todo caso, es responsabilidad de todos los Usuarios y Profesionales leer y comprender el contenido de esta Política, así como observar y cumplir sus directrices, principios y procesos en el desarrollo de su trabajo, en la medida en que el desconocimiento de todo o parte de su contenido no exime de su cumplimiento. En este sentido, se recomienda acceder de forma periódica al contenido de esta Política a través de los canales disponibles para una mejor comprensión de la misma.

12. Entrada en vigor

La presente Política fue aprobada por el Consejo de Administración de ACS en su reunión de fecha 19 de diciembre de 2024, entrando en vigor desde el momento de su publicación en la página web corporativa de ACS.