seresco

# Política de Seguridad

20/02/2024

# Índice de contenido

# 1. Misión

Seresco, S.A. es una empresa de servicios tecnológicos especializada en la provisión de servicios de:

- ***Infraestructuras, Sistemas y Seguridad a terceros***
- ***Gestión, administración, desarrollo, soporte y mantenimiento de nómina***
- ***Consultoría y Desarrollo de Software***
- ***Cartografía y Catastro***
- ***Transformación Digital***

Seresco Atlântico, Unipessoal, Lda es una empresa de servicios tecnológicos especializada en la provisión de servicios de:

- ***Gestión, administración, soporte y mantenimiento de nómina***

La Dirección de Seresco (entendido como Seresco S.A y Seresco Atlântico, Unipessoal, Lda) en el marco de su Plan Estratégico y acorde a su Misión - *aportar soluciones mediante el uso de la tecnología de forma eficiente y segura* - ha considerado necesario incluir una declaración única y extensible a toda la entidad, en relación a la gestión de la seguridad.

A través del Sistema de Gestión de Seguridad de la Información, la Dirección de Seresco adquiere el compromiso firme de:

- **Mantener el pleno cumplimiento legal y normativo,** alineando los procesos y los servicios, a la normativa vigente en cada momento, y que afecta de manera indirecta o directa, al perfil de cliente (administración pública o sector privado), a la información implicada (*pública, privada, restringida, confidencial o secreta*) o en general a la seguridad de la información y/o servicio.
- **Sensibilizar y concienciar** de manera estable y permanente al usuario de la organización.
- **Fomentar y mantener una buena reputación de la organización,** con relación a la seguridad de los servicios prestados.
- **Disponer de respuestas a los incidentes de seguridad**, mediante acciones preventivas y cuando fuera preciso acciones de respuesta y recuperación, adecuadas y detalladas.
- **Asegurar que los activos de la organización sólo sean utilizados por usuarios autorizados** en el ejercicio de sus funciones, según perfiles definidos o según asignaciones extraordinarias.
- **Tratar los datos personales de manera lícita, leal, transparente, con fines determinados y explícitos, legítimos sin ser usados para fines posteriores incompatibles**. Los datos personales tratados serán adecuados, pertinentes y limitados, exactos y actualizados. Serán tratados durante el tiempo necesario garantizándose la seguridad de los mismos.
- **Considerar la seguridad desde el diseño y por defecto** incluyendo a la Oficina de Protección de Datos siempre en la etapa más temprana del diseño y desarrollo de sistemas de información.
- **Proteger la información** interna y la relacionada con la prestación de los servicios a clientes, considerando las dimensiones de:
  - **Confidencialidad:** Toda la información se protegerá de manera que no se pondrá a disposición, ni se revelará a individuos, entidades o procesos, no autorizados previamente.

- **Integridad:** Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterado de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
- **Disponibilidad:** La información será accesible a aquellos usuarios o procesos que la requieran y cuando lo requieran. Será principio básico de la organización, la restricción de accesos al mínimo necesario.

La organización podrá considerar otras dimensiones relacionadas con la seguridad, derivadas de requerimientos legales (o en su caso, de requerimientos de negocio), considerándose:

- **Trazabilidad:** Toda acción desarrollada en el sistema o sobre la información, puede ser imputada a su autor, en cualquier fase de ciclo de vida o en cualquier fase de proceso.
- **Autenticidad:** Toda información puede ser asignada a una fuente o todo autor puede ser contrastado y acreditar su identidad sin lugar a dudas.

**La organización mantendrá las tres primeras dimensiones de seguridad y las dos añadidas, cuando sea preciso.**

- Entender la seguridad como un proceso integral, constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La seguridad del sistema contemplará los aspectos de **prevención, detección y corrección**, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

## 1.1. Prevención

Seresco considerará los riesgos a los que está expuesto el sistema, tanto en el momento actual como aquellos otros que pudieran presentarse en el futuro. Se considera la necesidad de la revisión y evaluación continua y permanente de la seguridad del sistema y sus activos, permitiendo la mejora continua y la eficacia de las medidas de seguridad acordadas, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario. Obtener un análisis en profundidad de las amenazas, así como de las tácticas, técnicas y procedimientos de los principales ciberatacantes del sector, es fundamental para la preparación y resiliencia del sistema.

## 1.2. Detección

Seresco establecerá controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuará en consecuencia, según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

### 1.3. Respuesta

Seresco establecerá las siguientes medidas de respuesta ante eventos que afecten a los servicios y/o información

- Responder eficazmente a los incidentes de seguridad.
- Desarrollar una reacción adecuada frente a los incidentes, reduciendo al máximo la probabilidad de que el sistema sea comprometido en su conjunto.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información y coordinación necesaria, relacionada con el incidente en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

### 1.4. Recuperación

Seresco establecerá protocolos para garantizar la disponibilidad de los servicios y en su caso, la estrategia de gestión de los medios y técnicas necesarias que permitan garantizar la recuperación de los servicios más críticos, mediante el desarrollo de planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

## 2. Alcance

La política de seguridad de la información, será de aplicación **a toda la información** del sistema con independencia del soporte o medio en el que se encuentre, tipología o categoría, **a todo el personal** de Seresco y también a terceros colaboradores, que accedan al sistema y/o presten servicios a la organización, así como **a cualquier activo** de información propiedad de la organización, o en régimen de uso y que afecte al sistema, considerándose en cualquier momento del ciclo de vida del sistema de seguridad.

Asimismo, la presente política, afecta a los datos personales gestionados y tratados por la organización.

Esta política estará accesible a todos los miembros de la organización, mediante su publicación en la intranet.

## 2.1. Alcance del sistema ENS

Específicamente, en Seresco S.A se aplicarán las **medidas de seguridad de categoría media** recogidas en el Esquema Nacional de Seguridad, al sistema de información que da soporte a:

- ✓ los servicios del Área Técnica de Servicios de Infraestructuras, agrupados en:
  - Consultoría de Sistemas y Servicios
  - Infraestructura como servicio
  - Service Desk
  - Operación y Administración de Sistemas e Infraestructuras
- ✓ los servicios de consultoría, desarrollo, mantenimiento y soporte de aplicaciones de software en organismos públicos, del Área Técnica de producción de software.
- ✓ los servicios de producción de Cartografía y Gestión Catastral.

# 3. Principios básicos de seguridad

Los principios básicos, que se describen a continuación serán las directrices fundamentales presentes en cualquier actividad del sistema de información.

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, requiere estar coordinada e integrada con el resto de las iniciativas estratégicas de la estructura orgánica para conformar un todo coherente y eficaz.
- **Responsabilidad determinada**: Se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la implementación de seguridad y supervisión de la operativa del sistema y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad y supervisará las medidas implantadas.
- **Seguridad integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas de tratamiento
- **Proporcionalidad**: Las medidas adoptadas para gestionar los riesgos deberán estar justificadas y, ser proporcionales entre ellas y los riesgos.
- **Mejora continua**: Existirá un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.

- **Seguridad por defecto y desde el diseño**: Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

## 4. Objetivos de la Seguridad de la Información

Se establecen como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información y los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestionar los activos de información, bajo un inventario, calificación y asignación a un responsable.
- Implementar medidas de seguridad ligada a las personas, incluyendo los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación.
- Desplegar y controlar la seguridad física logrando que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad y frente a amenazas físicas o ambientales.
- Establecer la seguridad en la gestión de comunicaciones y operaciones mediante los procedimientos necesarios logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida, conforme a su nivel de sensibilidad y de criticidad.
- Limitar el acceso a los activos mediante controles de acceso a usuarios, procesos y servicios, por medio de mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, asegurando la trazabilidad del acceso y auditando su uso.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Mantener el control y la seguridad en la adquisición e incorporación de nuevos componentes del sistema, asociado a nuevas tecnologías desplegadas en los servicios de soporte o en su caso, en los servicios de telemedicina e información electrónica.
- Gestionarlos incidentes de seguridad para la correcta identificación, registro y resolución de estos.
- Garantizar la prestación continuada de los servicios de acuerdo con las necesidades de nivel de cada servicio.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación de seguridad y privacidad.
- Mejorar los procesos de identidad digital de las personas implicadas en los procesos sanitarios.
- Adoptar las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

## 5. Marco normativo

Seresco, S.A. se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (Reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- CORRIGENDUM 8088/18, de 19 de abril, sobre corrección de errores en diferentes traducciones del RGPD.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del Patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones

- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley 31/1995 de 8 de noviembre, de prevención de Riesgos Laborales y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Convenio colectivo estatal de empresas de consultoría y estudios de mercado y de la opinión pública
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 17/2001, de 7 de diciembre, de Marcas.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
- Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
- ISO/IEC 27001
- ISO/IEC 20000-1

Seresco Atlântico, Unipessoal Lda se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes:

- DL n.º 7/2004, de 07 de Janeiro (comércio electrónico no mercado interno e tratamento de dados pessoais);
- Lei n.º 41/2004, de 18 de Agosto (protecção de dados pessoais e privacidade nas telecomunicações);
- Lei n.º 58/2019 de 8 de agosto (assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679);
- Lei n.º 102/2009, de 10 de Setembro (Regime jurídico da promoção da segurança e saúde no trabalho);
- Decreto-Lei n.º 110/2018 de 10 de dezembro (Código da Propriedade Industrial);

# 6. Organización de seguridad

## 6.1. Comité Estratégico de Seguridad: funciones y responsabilidades

El Comité Estratégico de Seguridad está formado por los Directores de área, el Responsable del Sistema de Gestión Integrado, el Responsable de Seguridad, el Responsable de Sistemas, y contará con la participación de otros roles necesarios en función del orden del día, como pueden ser el Delegado de Protección de Datos, o el Compliance Officer.

El Comité tendrá las siguientes funciones:

- Determinar la estrategia de seguridad de la información, realizando un seguimiento de su ejecución.
- Revisar y aprobar regularmente la Política de Seguridad de la Información.
- Resolver los conflictos de responsabilidad relacionados con seguridad.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación.
- Aprobar el nivel de riesgo aceptable.
- Aprobar los planes de mejora de seguridad
- Realizar un seguimiento de la gestión de los incidentes de seguridad.
- Aprobar la normativa de Seguridad de la Información.
- Aprobar las propuestas de formación en materia de seguridad
- Aprobar la valoración de los servicios y de la información
- Decidir suspensiones temporales de servicios frente a incidentes de seguridad.

## 6.2. Roles unipersonales: Funciones y Responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados el procedimiento de Roles y Responsabilidades y en la matriz asociada.

## 6.3. Procedimientos de designación de personas

El Responsable de Seguridad de la Información y el Responsable del Sistema serán nombrados por el Comité Estratégico de Seguridad.

El Responsable del Servicio y el Responsable de la Información serán designados por la Dirección.

Los roles de seguridad serán revisados anualmente en el caso de que exista una vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

## 7. Resolución de conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité Estratégico de Seguridad de la Información.

## 8. Datos Personales

Seresco en el tratamiento de los datos personales, cumple con los principios y obligaciones de la normativa vigente, entre otra el Reglamento 679/2016, 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-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

En desarrollo de los principios de la vigente normativa de protección de datos, entre otros, los de minimización, confidencialidad o proactividad, Seresco ha definido un marco de actuación en la Política de Protección de Datos (PCO-12 Política de privacidad y protección de datos), que se encuentra accesible a través del portal del Sistema de Gestión integrado (https://sgi.seresco.es).

## 9. Gestión de riesgos

Todos los sistemas afectados por esta Política estarán sujetos a un análisis periódico de riesgos con el objetivo de evaluar las amenazas a las que puedan estar expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o servicios de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad es el encargado de que se realice el análisis de riesgos y una vez identificadas las carencias y debilidades deberá tomar las medidas necesarias para minimizarlas hasta niveles aceptables.

El proceso de gestión de riesgos comprende las siguientes fases:

- Identificación de activos.
- Análisis de riesgos.
- Selección de medidas de seguridad a aplicar, que deberán de ser proporcionales a los riesgos y estar justificadas.

En particular, para realizar el análisis de riesgos, con carácter general, se empleará una metodología reconocido prestigio en el ámbito de la seguridad de la información para el análisis y gestión de riesgos

## 10. Desarrollo de la Política de Seguridad

Esta Política se desarrolla por medio de Normativa de Seguridad a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Para su organización se ha definido una Sistema de gestión, que establece las directrices para la organización, gestión y acceso, cuya documentación está accesible a través del portal del Sistema de Gestión integrado (https://sgi.seresco.es)

Otras Políticas que complementan esta Política de Seguridad, accesibles a través del mismo portal son:

- PCO-00 Políticas de uso aceptable de los activos TIC
- PCO-10 Política de metadatos
- PCO-12 Política de privacidad y protección de datos
- PCO-14 Política de Teletrabajo y Trabajo en Movilidad

## 11. Concienciación y formación

Seresco desarrollará actividades específicas en materia de formación y concienciación en Seguridad de la Información, así como sensibilización de los riesgos a los que están expuestos los Sistemas de Información, cuyos destinatarios deben ser todas las personas con responsabilidades en materia de Seguridad.

Las personas con responsabilidad en el uso, operación o administración de sistemas deberán recibir formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Desde Seresco se dispondrá de los medios necesarios para publicar, difundir y facilitar el conocimiento de esta política de seguridad, así como de sus documentos de desarrollo.

## 12. Obligaciones del personal

Todos los usuarios de los sistemas de información de Seresco tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad del Comité Estratégico de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

## 13. Seguridad con terceras partes

Seresco desarrollará los servicios a terceros conforme a la presente política y a su procedimiento de Homologación de proveedores. Cuando se trate de Administraciones Públicas, les hará participes de la presente, y de cuantos procesos y procedimientos afecten a la seguridad de la información y /o servicio. En particular, definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que Seresco lleve a cabo en materia de Seguridad en relación con otros organismos

Seresco gestionará el acceso y tratamiento por parte de terceros, con acceso a datos personales.

Cuando se establezca una cadena de suministro en la gestión o administración de soluciones a terceros, se mantendrá la presente política aplicable a todos los eslabones presentes.

## 14. Proceso de revisión de la política de seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por Comité de Seguridad.

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

## 15. Aprobación de la Dirección

La Dirección de Seresco asume el compromiso de proveer todos los recursos y medios para la implementación del Plan de Seguridad de la Información y Privacidad, de las Políticas, Procedimientos, Instrucciones y Normas desarrolladas al efecto y de velar por su cumplimiento.

La Dirección demuestra su compromiso, mediante la revisión y aprobación de las Políticas y otras normas que desarrollan el sistema, revisando los riesgos y aprobando el riesgo residual, considerando el informe de evaluación de impacto, participando en el Comité Estratégico de Seguridad, promoviendo la cultura de seguridad y especialmente, dotando de asignación efectiva a esta política mediante recursos y medios.

A tales efectos aprueba y publica esta política para su correcta difusión.

Esta Política de Seguridad de la Información es efectiva desde su fecha de aprobación y publicación y hasta que sea reemplazada por una nueva Política.

En Oviedo, a 20 de Febrero de 2024

Alejandro Blanco Urízar
Director de Organización y Relaciones Institucionales