POLÍTICA DE SEGURIDAD Y DE PROTECCIÓN DE DATOS PERSONALES

Documento de uso público

Contenido

APROBACIÓN Y ENTRADA EN VIGOR

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

Esta es una política que es desarrollada y aplicada en la siguiente empresa:

- **Nombre o Razón Social: ARIETE SEGURIDAD SA**
- **Dir. postal:** C/ INDUSTRIAS, 51 P.I. URTINSA II de Alcorcón CP (28923) Madrid
- **CIF:** A81349474 - **Teléfono:** 916433608
- **Email:** info@arieteseguridad.com - **Web:** https://arieteseguridad.com/

Este documento expone la **Política Seguridad y Protección de Datos personales** (PSPD) de **ARIETE SEGURIDAD SA** como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de los requisitos del RGPD UE 2016/679, el ENS (Esquema Nacional de Seguridad) y de la Norma ISO 27001.

1 INTRODUCCIÓN

ARIETE SEGURIDAD SA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, 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.

ARIETE SEGURIDAD SA debe cerciorarse de que la seguridad de la información 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 y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

ARIETE SEGURIDAD SA debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

ARIETE SEGURIDAD SA aplicará los principios básicos de protección de datos y los demás requisitos del RGPD UE 2016/679 para el procesamiento de todos los datos personales a lo largo del ciclo de vida

de la información mediante la adopción de los principios básicos de protección de datos de la presente política.

Esta Política de Seguridad sigue las indicaciones de la guía **CCN-STIC-805 del Centro Criptológico Nacional**, centro adscrito al Centro Nacional de Inteligencia.

1.1. Prevención

ARIETE SEGURIDAD SA debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD y la LOPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **ARIETE SEGURIDAD SA** debe:

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

1.2. Detección

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

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

1.3. Respuesta

ARIETE SEGURIDAD SA:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad de seguridad y de protección de datos personales.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores o encargados del tratamiento de protección de datos

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **ARIETE SEGURIDAD SA** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

2 MISIÓN

ARIETE SEGURIDAD SA define la presente Política, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información, la protección de datos personales y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información y de los datos personales, de los que se sirve a **ARIETE SEGURIDAD SA** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en **ARIETE SEGURIDAD SA** serán:

- Velar por la seguridad de la información y la protección de los datos personales, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad y la protección de los datos personales, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información y a la protección de los datos personales.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad y de protección de los datos personales, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Está Política:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas qué trabajen con **ARIETE SEGURIDAD SA**.

3 ALCANCE

El alcance de la presente política engloba a los **sistemas de información** que soportan los servicios de **vigilancia y la protección de bienes, establecimientos, espectáculos, certámenes o convenciones** que se realizan por **ARIETE SEGURIDAD SA** ubicado en C/ INDUSTRIAS, 51 P.I. URTINSA II de Alcorcón CP (28923) Madrid propiedad de **ARIETE SEGURIDAD SA**.

La presente es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de **ARIETE SEGURIDAD SA** para los servicios descritos.

Por otro lado, el alcance de la presente política engloba a todos los datos de carácter personal creados, recibidos y tratados en el curso de los negocios de **ARIETE SEGURIDAD SA** en cualquier formato. Los datos personales pueden ser tratados o transmitidos en papel, física y en formato electrónico o comunicarse verbalmente en conversaciones o por teléfono.

4 DEFINICIONES

- **Datos personales:** toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos 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.
- **Datos personales sensibles**: Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales de los interesados, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los mencionados derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliaciones sindicales, datos genéticos, datos biométricos, dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.
- **Responsable del tratamiento**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- **Encargado del tratamiento o encargado**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

- **Destinatario**: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.
- **Tercero**: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.
- **Consentimiento del interesado**: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- **Seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- **Empresa**: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica.
- **Elaboración de perfiles:** toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;
- **Evaluación de Impacto de Protección de datos (EIPD):** La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.
- **Violación de la seguridad de los datos personales**: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- **Transferencia Internacional de Datos**: el tratamiento de datos que suponga una transmisión de los mismos fuera del Espacio Económico Europeo (EEE)
- **Sistema de Información**: conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Riesgo**: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

- **Gestión de riesgos**: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de las actividades, las responsabilidades, las prácticas, los procesos, los procedimientos y los recursos para desarrollar, implantar, llevar a efecto, revisar y mantener al día los compromisos en materia de seguridad de la información.
- **Disponibilidad**: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad**: La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad**: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- **Autenticidad**: Se debe asegurar la identidad u origen de la información.
- **Trazabilidad**: Se debe asegurar para ciertos datos quién hizo qué y en qué momento.

5 DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de esta Política es proteger la información y los servicios de **ARIETE SEGURIDAD SA**.

- En **ARIETE SEGURIDAD SA** se reconoce expresamente la importancia de la información y de los datos personales, así como la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad de la Institución, o al menos suponer daños muy importantes, si se produjera una pérdida total e irreversible de determinados datos.
- **ARIETE SEGURIDAD SA** implementa, mantiene y realiza un seguimiento del Esquema Nacional de Seguridad, del RGPD y de la Ley Orgánica de Protección de Datos, y cumple con todos los requisitos legales aplicables.
- La información y los servicios están protegidos contra pérdidas de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Se cumplen los requisitos del servicio respecto a la seguridad de la información, de protección de datos personales y los sistemas de información.
- Los controles serán proporcionales a la criticidad de los activos a proteger y a su clasificación.
- La responsabilidad de la seguridad de la información y de la protección de datos involucrada en la prestación de los servicios incluidos en el alcance del ENS es de la Dirección, que pondrá los medios adecuados, sin perjuicio de que los empleados o usuarios asuman su parte de responsabilidad respecto a los medios que utiliza, según lo indicado en las normativas y en los procedimientos complementarios. En el punto 6 “Organización de la Seguridad” de este mismo documento se describen las funciones y responsabilidades del Comité de Seguridad y privacidad, que gestionará la seguridad de la información, y de sus miembros.

- Quienes desempeñen la función de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.
- Se ha identificado a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos que la integran, especialmente los de carácter personal o críticos.
- Se establecerá dentro de la normativa un sistema de clasificación de la información, con diferentes niveles.
- Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información y datos personales, y, en general, de cualquier activo de **ARIETE SEGURIDAD SA.**
- Los aspectos específicos más relacionados con la información sobre datos personales están regulados por el conjunto de normas recogidas en esta política y en otra normativa interna o de otra índole a la que pueda remitir o que se cite.
- Quienes no cumplan lo determinado en estas normas y en los procedimientos complementarios podrán ser sancionados de acuerdo con la legislación laboral, o bien con sanciones personalizadas si están vinculados a **ARIETE SEGURIDAD SA** bajo contratos no laborales, de acuerdo con las cláusulas que figuren en dichos contratos en este último caso.
- Deberán realizarse periódicamente evaluaciones de riesgos y, en función de las debilidades, determinar si es necesario elaborar planes de implantación o reforzamiento de controles.
- Se fomentará la difusión de información y formación en seguridad a empleados y colaboradores, previniendo la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar su posible existencia lo antes posible, y en caso de que existieren, procurándose una difusión muy restringida de las indagaciones.
- El personal de **ARIETE SEGURIDAD SA** deberá conocer las normas, reglas, estándares y procedimientos relacionados con su puesto de trabajo, así como sus funciones y obligaciones, además de la separación de funciones y la revisión independiente de los registros, cuando sea necesario, de quién ha hecho qué, cuándo y desde dónde.
- Las incidencias de seguridad serán comunicadas y tratadas apropiadamente.

6 MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a **ARIETE SEGURIDAD SA** en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 Abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.

- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.

ARIETE SEGURIDAD SA cumple con la legislación citada y con todos sus requisitos.

7 ORGANIZACIÓN DE LA SEGURIDAD

7.1 Comité: Funciones y Responsabilidades

El Comité de Seguridad y privacidad y protección de datos coordina la seguridad de la información y la protección de datos en **ARIETE SEGURIDAD SA**.

El **Comité de Seguridad y privacidad** reportará a la organización y estará formado por:

- Responsable del Servicio y de la Información.
- Responsable de Seguridad.
- Responsable del Sistema
- Administrador de Sistemas
- Delegado de protección de datos

El **Secretario del Comité de Seguridad y privacidad** será el Responsable de Seguridad y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad y privacidad.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Responsabilizarse de que se elaboren las actas de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El **Comité de Seguridad y privacidad** tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información y de protección de datos personales.
- Velar por el cumplimiento de la presente política y su normativa de desarrollo.
- Elaborar la estrategia de evolución de **ARIETE SEGURIDAD SA** en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información y protección de datos personales, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la presente Política para que sea aprobada por la organización.
- Aprobar normas y procedimientos para garantizar la seguridad de la información y de los datos personales.
- Promover recursos y medios para la concienciación y formación en materia de seguridad de la información y de protección de datos personales a los Responsables de área, técnicos y usuarios en general.
- Monitorizar los principales riesgos residuales asumidos por **ARIETE SEGURIDAD SA** y recomendar posibles actuaciones respecto de ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de los diferentes departamentos en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad y de protección de datos personales.
- Aprobar planes de mejora de la seguridad de la información y de los datos personales**.** En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar las actuaciones en materia de seguridad y protección de datos personales cuando los recursos sean limitados.
- Velar porque la seguridad de la información y la protección de datos personales 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, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Informar regularmente del estado de la seguridad de la información y de los datos personales a la Dirección.

7.2 Roles: Funciones y Responsabilidades

En el caso de **ARIETE SEGURIDAD SA** todas las responsabilidades recaen en el director, al ser una empresa unipersonal.

Las funciones y responsabilidades se detallan a continuación:

7.2.1 Nivel de Gobierno

Responsable del Servicio y de la Información

La persona con el cargo de Responsable del servicio y de la información asumirá las siguientes funciones:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.
- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad y protección de datos personales
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.
- A proporcionar y dotar de los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora de la presente política y sus normativas vinculadas.

- Demostrar liderazgo y compromiso respecto la presente política.
- Asegurar el cumplimiento de la presente política y que estos sean compatibles con la estrategia de **ARIETE SEGURIDAD SA**
- Promover y fomentar la cultura de la privacidad y de la seguridad de la información.
- Asegurar que la gestión de la privacidad consigue los resultados previstos y apoyar la mejora continua de los procesos de seguridad de la información.
- Aprobar y comunicar la presente Política y otras normas de seguridad y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores
- Dirigir y apoyar a las personas para contribuir a la eficacia de la presente política.
- Reunirse al menos una vez al año, y cuando cualquier evento o solicitud extraordinaria lo demande, con los Responsables de Seguridad, de Sistemas y DPO para ser informado sobre el Sistema de Gestión de Seguridad de la Información y Protección de Datos y actualizar la estrategia en materia de privacidad y Seguridad de la Información
- Definir los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto destinado al programa de privacidad y a la seguridad de la información.
- Aprobar los planes de formación y las mejoras y proyectos relacionados con la privacidad y la seguridad de la Información.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad y de protección de datos.
- Promover la mejora continua.

7.2.2 Nivel de Supervisión

Responsable de Seguridad

La persona con el cargo de Responsable de Seguridad de la Información asumirá las siguientes funciones:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del Esquema Nacional de Seguridad y de la Norma UNE-ISO/IEC 27001.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS o el SGSI para verificar el cumplimiento de los requisitos del mismo y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y para los derechos y libertades para los interesados.
- Realizar con la colaboración del Responsable del Sistema o el Delegado de Protección de Datos, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema y Delegado de Protección de Datos, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por el Responsable del servicio y de la información, siguiendo en todo momento lo exigido en el Anexo II del ENS o el ANEXO I de la ISO 27001, en su caso, declarando la aplicabilidad de dichas medidas.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas (ISO 27001 y ENS), en colaboración con el Responsable de Sistemas
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad.
- Elaborar y firmar el documento de Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS o el ANEXO I de la ISO 27001.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad y privacidad, en coordinación con el Responsable del Sistema, aportando información puntual para la toma de decisiones.

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

- Proponer a la Dirección y al Responsable de Sistemas para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información) y firmar dicha documentación.
- Aprobar la documentación de seguridad de tercer nivel (Procedimientos Operativos e Instrucciones Técnicas).

- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Delegado de Protección de Datos (DPO)

El Delegado de protección de datos a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, deberá llevar a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa estatal de protección de datos personales.

En el desempeño de sus funciones, la delegada o el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento.

El Delegado de Protección de Datos es responsable de:

- informar y asesorar a los usuarios de los datos personales de sus obligaciones que les incumben respecto del RGPD.
- Monitorear el cumplimiento del RGPD y otras leyes relevantes de protección de datos, las políticas en materia de protección de datos y el asesoramiento de las actividades de capacitación y formación relacionadas con el cumplimiento de GDPR.
- Proporcionar asesoramiento cuando se solicite sobre evaluaciones de impacto de protección de datos.
- Cooperar y actuar como punto de contacto ante la Agencia Española de Protección de Datos.
- Realizar consultas basadas en el artículo 36 del RGPD y, en su caso, consultas sobre cualquier otro asunto.
- El Delegado de Protección de Datos deberá, en el desempeño de sus tareas, tener debidamente en cuenta los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.

7.2.3 Nivel Operativo.

Responsable del Sistema

La persona con el cargo de Responsable de Sistema asumirá las siguientes funciones:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de 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.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos e Instrucciones Técnicas).

Administrador de la Seguridad del Sistema

Su función es realizar las tareas de administración en el sistema, delegadas por parte del Responsable del Sistema (RSIS), para facilitar la operativa diaria. Asumirá las siguientes funciones:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aplicar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los respectivos Responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Asegurar que los controles para empleo de software autorizado en el sistema son cumplidos estrictamente y que no se usa software no autorizado.
- Llevar a cabo regulares comprobaciones de presencia de código malicioso en el sistema, recepcionando los informes de las medidas de protección implementadas al respecto.
- Verificar que todo el hardware está perfectamente etiquetado de acuerdo con la máxima clasificación de la información que soporta.
- Asegurar que tienen lugar efectivos procedimientos de copia de respaldo de la información almacenada, así como la custodia de los soportes de almacenamiento resultantes con medidas de seguridad equivalentes

- Asegurar que la trazabilidad, evidencias de auditoría y otros registros de seguridad son frecuentemente analizados, de acuerdo con la presente política de Seguridad
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

8 PROCEDIMIENTOS DE DESIGNACIÓN

El procedimiento de Designación se detalla a continuación.

El Responsable del servicio y de la información (La dirección) nombra:

- Responsable de Seguridad, que reportará al Comité de Seguridad y privacidad.
- Delegado de Protección de Datos, que reportará al Comité de Seguridad y privacidad.
- Responsable del Sistema, que reportará al Comité de la Seguridad.
- Al Administrador de Seguridad del Sistema, que reportará al Comité de Seguridad y privacidad.
- Responsable del Servicio, que reportará al Comité de Seguridad y privacidad.
- Responsable de la Información. Que reportará al Comité de Seguridad y privacidad.

9 ESTRUCTURACION DE LA DOCUMENTACIÓN DEL SISTEMA, SU GESTIÓN Y ACCESO

Estructurar nuestro sistema de gestión de forma que se fácil comprender. Nuestro sistema de gestión tiene la siguiente estructura:

Política de Seguridad y de protección de datos personales es un documento de alto nivel, La política está escrita a un nivel muy amplio, por lo que, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto.

Procedimientos Generales de Seguridad: Los Procedimientos generales afrontan tareas más genéricas en el marco Organizativo del Sistema de Gestión, indicando lo que hay que hacer, paso a paso. (Por ejemplo, Procedimiento general para auditorias, Procedimiento general para métricas e indicadores, etc)

Normas de Seguridad: Las Normas uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio

Procedimientos Operativos de Seguridad (POS): Los Procedimientos operativos afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Instrucciones técnicas de Seguridad: determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. Una instrucción técnica debe ser clara y sencilla de interpretar.

Registros y evidencias: Los registros, registran evidencias objetivas de la ejecución y terminación de actividades o trabajos realizados para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información alienados con los procedimientos, normas e instrucciones descritos en los apartados anteriores.

La gestión de nuestro sistema se encomienda al Responsable de Sistemas Informáticos y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

10 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACION Y RIESGOS DE PROTECCIÓN DE DATOS

La gestión del riesgo es el conjunto de actividades dirigidas a estimar el riesgo que generan las operaciones de tratamiento de la información y de datos personales, con el fin de seleccionar controles, medidas de seguridad y tomar decisiones, que permitan mantener el riesgo de la información y de los datos personales en un nivel de riesgo que sea aceptable.

El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas técnicas y organizativas apropiadas, que establecerá un equilibrio entre la naturaleza de la información, de los datos personales, de los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

Al evaluar el riesgo se tendrá en cuenta los riesgos que se derivan para la seguridad de la información y los riesgos para los derechos de las personas con respecto al tratamiento de sus datos personales. Como consecuencia del análisis de riesgos, las medidas de seguridad técnicas y organizativas son seleccionadas sobre la base de una evaluación de riesgos tienen en cuenta:

- Los riesgos que afecten a los sistemas de información que soportan los servicios definidos en el alcance de la presente política. Los riesgos pueden ser riesgos sobre activos de la información o riesgos organizacionales que afectan a la Organización en general.
- Los riesgos procedentes del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales objetos de tratamiento, o la comunicación o acceso no autorizados a dichos datos.
- Los riesgos que son susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales en las personas físicas como problemas de discriminación, usurpación de

identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, perjuicio económico o social significativo, etc.

La gestión de riesgos de seguridad de la información y de los datos personales debe realizarse de manera continua conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

El análisis y gestión de riesgos se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para el análisis y gestión de riesgos se empleará alguna metodología reconocida. El análisis y gestión de riesgos quedará documentada en el informe de Análisis y Gestión de riesgos.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección será responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

11 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES

Será misión del Comité de Seguridad y privacidad la revisión anual de esta Política de Seguridad de la Información y de Protección de Datos Personales y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la organización y difundida para que la conozcan todas las partes afectadas.

11.1 Principios de seguridad de la información

Esta Política de Seguridad y de Protección de Datos Personales complementa las políticas de seguridad de en diferentes materias:

- Gestión de Activos
- Uso aceptable de los sistemas de información.
- Seguridad de los equipos
- Autorización y control de accesos
- Adquisición, desarrollo y mantenimiento de los sistemas de información y de los datos personales.
- Mínimo privilegio
- Integridad y actualización del sistema
- Gestión del Cambio
- Protección de información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad del usuario
- Seguridad en la gestión de comunicaciones y operaciones
- Protección de la información almacenada y en tránsito

- Eliminación y Destrucción de Información
- Navegación en Internet
- Uso Correo Electrónico
- Seguridad para la Gestión de Contraseñas
- Pantalla y Escritorio Limpio
- Protección frente a código malicioso y código móvil
- Gestión de la seguridad de la red
- Copias de Respaldo de la Información
- Gestión de la continuidad de los sistemas de información y de los datos personales
- Resiliencia de los sistemas de información y de los datos personales
- Gestión de incidentes de seguridad y de los datos personales
- Cumplimiento
- Profesionalidad
- Acciones Correctivas
- Mejora continua del proceso de seguridad

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará 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.

11.2 Protección de Datos y Privacidad

La Ley Orgánica de Protección de Datos (LOPD) y el RGPD, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

ARIETE SEGURIDAD SA cuando la información bajo su responsabilidad contenga datos de carácter personal, aplicará, además de los principios de seguridad de la información enumerados en el punto anterior, los siguientes principios:

- **Licitud, lealtad y transparencia**: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.
- **Limitación de la finalidad:** Los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines.
- **Minimización de datos**: Los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- **Exactitud de los datos:** Los datos de carácter personal serán exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación aquellos datos que sean inexactos.
- **Limitación del plazo de conservación**: Los datos de carácter personal serán mantenidos de forma que no se permita la identificación de los interesados durante más tiempo del necesario para los fines que justificaron su tratamiento.

- **Integridad y confidencialidad:** Los datos de carácter personal serán tratados de manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Las medidas de seguridad del documento de Declaración de Aplicabilidad obtenidas del ANEXO II del Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679
- Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con ARIETE SEGURIDAD SA.

12 OBLIGACIONES DEL PERSONAL

Todos los miembros de **ARIETE SEGURIDAD SA** tienen la obligación de conocer y cumplir esta Política, siendo responsabilidad del Comité de Seguridad y privacidad disponer los medios necesarios para que la información llegue a los afectados.

La presente Política debe ser conocida por todos los usuarios externos y por las empresas que accedan, gestionen o traten información o datos personales de **ARIETE SEGURIDAD SA**.

El conjunto de Políticas, normas y procedimientos complementarios a esta Política también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso. TERCERAS PARTES

Cuando **ARIETE SEGURIDAD SA** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **ARIETE SEGURIDAD SA** utilice servicios de terceros o ceda información a terceros, se les hará partícipe 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 los responsables de la información y los servicios afectados antes de seguir adelante

13 RESOLUCIÓN DE CONFLICTOS Y CONFLICTOS DE LEGISLACIÓN

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de protección de datos y seguridad de la información corresponderá, en última instancia, a la

Dirección, asistida por el Comité de Seguridad y privacidad de la Información y, cuando proceda, por el delegado de protección de datos, la resolución de conflictos.

Esta política está destinada a cumplir con las leyes y reglamentos en el lugar de establecimiento y de los países en los que opera **ARIETE SEGURIDAD SA**. En caso de conflicto entre esta política y las leyes y reglamentos aplicables, prevalecerá esta última.

14 DESARROLLO NORMATIVO Y REVISIÓN DE LA PRESENTE POLÍTICA

Corresponderá a la Dirección de **ARIETE SEGURIDAD SA**, a propuesta de los miembros que integran la estructura organizativa de la presente política y asistida por el Comité de Seguridad y privacidad de la información y, cuando proceda, por el delegado de protección de datos, la adopción de los procedimientos, guías e instrucciones técnicas necesarios para el desarrollo de la presente Política.

En el proceso de desarrollo normativo podrá requerirse la colaboración de las unidades organizativas que componen la estructura orgánica de la **ARIETE SEGURIDAD SA**.

La presente política se someterá a un proceso de revisión, al menos anual, a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

15 LISTA DE CONTROL DE CAMBIOS

Nueva Edición	Fecha de entrada en vigor del documento	Breve descripción del cambio	Entregado a NOMBRE + FECHA	MODO DE ENTREGA
31/01/2023	31/01/2023	Realización inicial		Sharepoint