POLÍTICA DE SEGURIDAD, CONTINUIDAD Y DE PROTECCIÓN DE DATOS PERSONALES

Realizado Por	Revisado Por	Aprobado Por
Fecha: 31/01/2023	Fecha: 15/02/2023	Fecha: 15/02/2023

Contenido

APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información y Continuidad de Negocio 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, Continuidad 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 las Normas ISO 27001 e ISO 22301.

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 y continuidad de negocio 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 con el 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 y Continuidad 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, la continuidad del negocio o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD, la ISO 22301 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 y continuidad 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, continuidad de negocio 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 específicos, entre ellos, de los sistemas TIC como parte de su plan general de continuidad del negocio 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 del negocio y 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 y Continuidad del Negocio en **ARIETE SEGURIDAD SA** serán:

- Velar por la seguridad de la información, continuidad de negocio y la protección de los datos personales, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad, la continuidad del negocio y la protección de los datos personales, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de continuidad específicos que se definan para los distintos escenarios de riesgos en relación con los riesgos detectados de cara a la continuada prestación de los servicios ofrecidos por la organización y por tanto de la continuidad del negocio.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información, continuidad del negocio y a la protección de los datos personales.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, continuidad y de protección de los datos personales. Así como 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, así como los recursos humanos, infraestructura, procesos operativos y comunicaciones,** que soportan los servicios de **vigilancia y la protección de bienes, establecimientos, espectáculos, certámenes o convenciones** que se realizan por **ARIETE SEGURIDAD SA** en el centro de trabajo ubicado en C/ INDUSTRIAS, 51 P.I. URTINSA II de Alcorcón CP (28923) Madrid, propiedad de **ARIETE SEGURIDAD SA**.

La presente se aplica 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.
- **Seudoanimización**: 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 estos 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 y Continuidad de Negocio (SGSICN):** 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 y asegurar la continuidad del negocio. 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 y continuidad de negocio.
- **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 Y CONTINUIDAD DE NEGOCIO.

El propósito de esta Política es proteger la información y los servicios de **ARIETE SEGURIDAD SA**, así como la continuidad del negocio.

- 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 continuidad de negocio, 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, de la continuidad de negocio 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 "**Organización de la Seguridad y la Continuidad del Negocio"** 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 y del Comité de Continuidad del Negocio que gestionará la continuidad del negocio, y de sus miembros.

- Quienes desempeñen la función de Seguridad de la Información y Continuidad y otras de administración relacionadas, serán quienes administren la seguridad y los servicios.
- 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. Así como a los responsables de continuidad del negocio que deberán prevenir los riesgos detectados, así como actuar en el supuesto de la materialización de alguno de ellos.
- 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 servicios esenciales, información y datos personales, y, en general, de cualquier activo de **ARIETE SEGURIDAD SA.**
- Los aspectos específicos más relacionados con los servicios, la información y con los 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 contingencia o continuidad específicos 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 y continuidad 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.
- 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 Y CONTINUIDAD DEL NEGOCIO

7.1 Comité de Seguridad y privacidad:

7.1.1 Funciones y Responsabilidades del Comité

El Comité de Seguridad y privacidad 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:

- Dirección
- Responsable de Seguridad
- Responsable de TIC
- Delegado de Protección de Datos

El **Secretario del Comité de Seguridad y privacidad** será el Responsable de Seguridad 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, Continuidad de Negocio y de protección de datos personales en materia de seguridad de la información.
- 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, en materia de seguridad de la información.
- 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 cualquier servicio esencial y por supuesto de la 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 para asegurar, el fortaleciendo 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.

7.1.2 Roles: Funciones y Responsabilidades

Las funciones y responsabilidades se detallan a continuación:

7.1.2.1 Nivel de Gobierno

Dirección

La persona con el cargo de Dirección 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 tanto a niveles generales de los servicios como 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 y de la protección de los servicios de la entidad.
- 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 la Información y DPO para ser informado sobre el Sistema de Gestión de Seguridad de la Información, Continuidad de Negocio 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, 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.

7.1.2.2 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 las Normas UNE-ISO/IEC 27001 e ISO 22301.
- 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 SGSICN para verificar el cumplimiento de los requisitos del mismo y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable de TIC 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 de los derechos y libertades para los interesados.
- Realizar con la colaboración del Responsable de TIC 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 de TIC 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 la Dirección, 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 TIC.
- 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 TIC.
- 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 de TIC, aportando información puntual para la toma de decisiones.

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

- Proponer a la Dirección 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 de TIC.

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.

7.1.3 Nivel Operativo.

Responsable de Sistemas

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

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, incluyendo especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y el sistema de gestión de Seguridad Información y Continuidad de Negocio, 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.
- Realizar el seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida.
- Implementar, previa autorización del Responsable de Seguridad y Continuidad, toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el tratamiento de una determinada información o la prestación de un servicio electrónico en caso de detectar deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y Continuidad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad y Continuidad, los preceptivos análisis de riesgos, de seleccionar las salvaguardas a implantar y de revisar el proceso de gestión del riesgo.
- Elaborar en colaboración con el Responsable de Seguridad y Continuidad, la documentación de seguridad de tercer nivel (Procedimientos Operativos e Instrucciones Técnicas).
- Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.
- Gestionar, configurar y actualizar el hardware y software que sustentan los mecanismos y servicios de seguridad del Sistema de Información.
- Gestionar las autorizaciones concedidas a los usuarios, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad.
- Implementar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad se cumplen estrictamente y que se aplican los procedimientos aprobados para el manejo del sistema.
- Supervisar las instalaciones de hardware y software, así como sus modificaciones y mejoras, para garantizar que la seguridad no se vea comprometida y que se ajusten a las autorizaciones correspondientes.
- Monitorizar el estado de seguridad del sistema mediante herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados.
- Informar a los responsables correspondientes de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Asegurar el cumplimiento de los controles para el uso de software autorizado y evitar el uso de software no autorizado.

- Realizar comprobaciones periódicas para detectar la presencia de código malicioso en el sistema.
- Verificar que todo el hardware esté inventariado y etiquetado según la clasificación de la información que soporta.
- Asegurar la realización efectiva de copias de respaldo de la información almacenada y garantizar la custodia segura de los soportes resultantes.
- Asegurar que la trazabilidad, las evidencias de auditoría y otros registros de seguridad son analizados con regularidad conforme a la presente Política.

7.2 Comité de Continuidad

7.2.1 Funciones y Responsabilidades

El Comité de Continuidad es el órgano que dirige la respuesta estratégica ante incidentes graves que afectan la continuidad del negocio. Su función principal es tomar decisiones rápidas, coordinar recursos y proteger a **ARIETE SEGURIDAD SA**.

El **Comité de Continuidad** estará formado por:

- Dirección (Líder)
- Responsable de Continuidad
- Responsable de Sistemas TIC
- Gestor del Sistema de Continuidad de Negocio
- Director Financiero

El **Comité de Continuidad** tendrá las siguientes funciones:

- Dirección estratégica de la crisis:
  - Evaluar la situación inicial del incidente y su impacto en la organización.
  - Determinar el nivel de gravedad y declarar oficialmente la crisis.
- Toma de decisiones críticas:
  - Priorizar procesos y servicios esenciales.
  - Autorizar uso extraordinario de recursos.
  - Definir cambios operativos necesarios (traslado de operaciones, teletrabajo, proveedores alternativos, etc.).
- Coordinación de equipos de respuesta.
- Coordinar a los diferentes equipos de gestión de incidentes:
  - equipo de continuidad
  - equipo de recuperación de TI
  - seguridad
  - operaciones
  - recursos humanos
- Gestión de la comunicación
  - Definir y aprobar la comunicación hacia:
    - empleados
    - clientes
    - proveedores
    - autoridades
    - medios de comunicación

- Evaluación continua de la situación:
  - Recibir informes periódicos de los equipos operativos.
  - Analizar evolución del incidente.
  - Ajustar las estrategias de respuesta.
- Protección de personas, activos y reputación
  - Priorizar la seguridad de las personas.
  - Minimizar pérdidas económicas.
  - Proteger la imagen corporativa.

- Decidir el retorno a la normalidad. Cuando el incidente está controlado, el comité:
  - autoriza el retorno a operaciones normales
  - desactiva los planes de contingencia
  - inicia la fase de recuperación total.

- Análisis posterior a la crisis. Después del evento:
  - realizar lecciones aprendidas
  - evaluar la eficacia del plan
  - proponer mejoras al SGCN

7.2.2 Roles: Funciones y Responsabilidades

En el caso de **ARIETE SEGURIDAD SA** todas las responsabilidades recaen en ~~el director~~ la Dirección General.

Las funciones y responsabilidades se detallan a continuación:

7.2.2.1 Nivel de Gobierno

Director del Comité de Crisis

Es el Líder del Comité y responsable de la gestión estratégica de la crisis. Sus Funciones son:

- Declarar formalmente la situación de crisis.
- Activar los planes de continuidad de negocio.
- Dirigir las reuniones del comité.
- Tomar decisiones estratégicas críticas.
- Coordinar a todos los miembros del comité

Responsable de Continuidad de Negocio y Operaciones.

Es el experto en continuidad de negocio y el enlace con el SGCN. Sus Funciones son:

- Asesorar al Comité sobre los planes de continuidad.
- Proponer la activación de planes de continuidad específicos.
- Coordinar con los equipos de recuperación.
- Informar sobre el impacto en procesos críticos.
- Garantizar que sigan los procedimientos definidos.
- Evaluar el impacto de la crisis en las operaciones.
- Priorizar los procesos críticos.
- Garantizar que se sigan los procedimientos definidos

Responsable de TIC

Encargado de la continuidad tecnológica y recuperación de sistemas. Sus Funciones son:

- Evaluar el impacto en infraestructura tecnológica.
- Activar planes de recuperación de TI.
- Informar sobe disponibilidad de sistemas.
- Priorizar restauración de servicios tecnológicos.

Secretario del Comité y Responsable de RRHH

Apoya la gestión administrativa y documental del comité, gestiona la comunicación interna y externa durante la crisis y gestiona los aspectos relacionados con el personal. Sus Funciones son:

- Registrar decisiones y acuerdos.
- Elaborar actas de las reuniones.
- Gestionar la documentación de la crisis.
- Preparar comunicados oficiales.
- Coordinar mensajes para empleados y clientes.
- Gestionar la disponibilidad de personal crítico.
- Coordinar medidas laborales especiales.
- Apoyar la comunicación interna.

7.3 Tareas

DIR: Responsable de tratamientos
DIR: Responsable de la Información
DIR: Dirección
RSGSICN: Responsable de la Seguridad de la Información y Continuidad del Negocio.
RSIS: Responsable de Sistemas
DPO: Delegado de Protección de Datos

Tarea	Responsable
Hacer un registro de los tratamientos	DIR + DPO
Garantizar el cumplimiento de los deberes de secreto y seguridad.	DIR
Garantizar derechos LOPD/RGPD	DIR + DPO
Determinación de los niveles de seguridad requeridos en cada dimensión	DIR o el Comité de Seguridad y privacidad
Determinación de la categoría del sistema	RSGSICN
Análisis de riesgos	RSGSICN + RSIS + DPO
Declaración de aplicabilidad	RSGSICN
Medidas de seguridad adicionales	RSGSICN + DPO
Configuración de seguridad	Elabora: RSGSICN Aplica: RSIS
Implantación de las medidas de seguridad	RSIS
Aceptación del riesgo residual	DIR
Documentación de seguridad del sistema	RSGSICN

Política de seguridad	Elabora: Comité de Seguridad y privacidad Aprueba : Organización
Normativa de seguridad y privacidad	Elabora RSEGCN y DPO Aprueba: Comité de Seguridad y privacidad
Procedimientos operativos de seguridad	Elabora y aprueba: RSGSICN Colabora: RSIS y DPO Aplica: RSIS
Estado de la seguridad del sistema	Monitoriza: RSIS Reporta: RSGSICN
Planes de mejora de la seguridad	Elaboran: RSIS + RSGSICN Aprueba: Comité de Seguridad y privacidad
Planes de concienciación y formación	Elabora: RSGSICN + RSIS + DPO Aprueba: Comité de Seguridad y privacidad
Notificación de brechas de datos personales e incidentes de seguridad a la AEPD	Elabora: RSGSICN + DPO Notifica a la AEPD: DIR
Notificación de brechas de datos personales e incidentes de seguridad a los interesados	Elabora: RSGSICN + DPO Notifica a la AEPD: DIR
Planes de continuidad	Elabora: RSIS Valida: RSGSICN Coordina y aprueba: Comité de Seguridad y privacidad Ejercicios: RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	Elabora: RSIS Aprueba: RSGSICN

8 PROCEDIMIENTOS DE DESIGNACIÓN

El procedimiento de Designación se detalla a continuación.

El Dirección nombra:

- Responsable de Seguridad, que reportará al Comité de Seguridad y privacidad.
- Responsable de Continuidad, que reportará al Comité de Continuidad.
- Delegado de Protección de Datos, que reportará al Comité de Seguridad y privacidad.
- Responsable de Sistemas, que reportará al Comité de la Seguridad y privacidad y al Comité de Continuidad.
- Al Gestor del Sistema de Gestión de Seguridad de la Información y Continuidad de Negocio, que reportará a ambos Comités.

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, Continuidad 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 y Continuidad: 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, CONTINUIDAD DE NEGOCIO 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 continuidad de negocio, 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 de los servicios esenciales, así como los derivados 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 la entidad, tanto en los servicios esenciales, como los relativos a la 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, CONTINUIDAD DE NEGOCIO Y DE PROTECCIÓN DE DATOS PERSONALES

Será misión de ambos Comités la revisión anual de esta Política de Seguridad de la Información, Continuidad de Negocio 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 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.

11.1.1 Gestión de Activos.

Los activos de información involucrados en todos los procesos de **ARIETE SEGURIDAD SA**, son propiedad de esta, y se proporcionan a los usuarios para cumplir con sus funciones profesionales.

La información gestionada en todos los procesos **ARIETE SEGURIDAD SA** debe cumplir con lo siguiente:

- Los activos de información se encontrarán inventariados, categorizados, protegidos y estarán asociados a un responsable.
- La clasificación de los activos se realizó de acuerdo al tipo de activo, por ejemplo, hardware, software, servicio, personas, la cual debe revisarse periódicamente o cuando se presenten cambios en la información o en la estructura que puedan afectarla.
- Los activos de información que contienen datos personales deben estar en cumplimiento con el RGPD UE 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

11.1.2 Uso aceptable de los sistemas de información.

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- Los usuarios son responsables de un adecuado y racional uso de los activos de información que se utilizan en **ARIETE SEGURIDAD SA**. Es decir, no se pueden usar para propósitos diferentes para los cuales fueron definidos o para temas personales.
- Se implementarán medidas adecuadas y se fortalecerá una cultura para reportar cualquier anomalía o incidencia identificada, al responsable de Seguridad de la Información, de acuerdo con los procedimientos establecidos, con el objeto de gestionar los riesgos e incidentes de seguridad que se puedan presentar para **ARIETE SEGURIDAD SA**.
- Se establece que los datos de acceso son un elemento personal e intransferible, los usuarios asumen la responsabilidad sobre el buen o mal uso que se dé sobre los sistemas de información del **ARIETE SEGURIDAD SA**.
- **ARIETE SEGURIDAD SA** proporciona el hardware y el software requerido para el desempeño adecuado de los servicios prestados por la entidad. Los datos e información creados, almacenados y recibidos, serán propiedad de la **ARIETE SEGURIDAD SA**.

- La copia, sustracción, daño intencional o utilización para fines distintos del desempeño de las funciones laborales serán sancionadas de acuerdo con las normas y legislación vigentes aplicables.

No se considera aceptable entro otras:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Compartir las contraseñas o permitir el acceso no autorizado a las cuentas otorgadas y así mismo es responsable por el tratamiento adecuado de la información y las acciones que por mal uso se deriven de esos accesos
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de los equipos están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso intencionadamente. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

11.1.3 Seguridad física y del entorno.

11.1.3.1 Áreas seguras.

ARIETE SEGURIDAD SA tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

Los activos de información y de los datos personales serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

La totalidad de las instalaciones de **ARIETE SEGURIDAD SA** cuentan con las barreras físicas para asegurar los recursos que éstas alberguen; en concreto un control el visitante y el acompañamiento del personal durante la estancia en las instalaciones.

11.1.3.2 Seguridad de los equipos.

Los equipos informáticos de **ARIETE SEGURIDAD SA** están protegidos contra posibles fallos de energía (ordenador portátil con batería, SAIs, etc.).

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal autorizado podrá acceder al equipo para proceder a su reparación o mantenimiento. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.

11.1.4 Autorización y control de accesos.

Se limitará el acceso a los sistemas de información y a los datos personales por parte de usuarios, proceso, dispositivos u otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

11.1.5 Adquisición, desarrollo y mantenimiento de los sistemas de información y de los datos personales.

Las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios, sistemas de información y datos personales, acompañadas de los correspondientes procedimientos de control y garantizando su seguridad por defecto.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en las condiciones contractuales para proyectos de TIC.

11.1.6 Mínimo privilegio.

Los sistemas de información se diseñan y configuran con los mínimos privilegios necesarios para su correcto desempeño, lo que implica:

- Proporcionar la funcionalidad imprescindible para alcanzar los objetivos.
- Que las funciones de operación, administración y registro de actividad serán las mínimas necesarias.
- La eliminación o desactivación de las funciones que sean innecesarias o inadecuadas.

11.1.7 Integridad y actualización del sistema.

ARIETE SEGURIDAD SA se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

11.1.8 Gestión del Cambio.

ARIETE SEGURIDAD SA garantiza que cualquier cambio en sistemas de información se realicen de manera gestionada y controlada, evaluando los riesgos previamente y acorde a las necesidades y requerimientos de la entidad.

ARIETE SEGURIDAD SA garantiza que la implementación de los cambios se lleve a cabo sin generar discontinuidad en la operatividad.

Los responsables de los cambios deben informar antes de la implementación de un cambio a las dependencias o partes interesadas, que puedan verse afectados, con el fin de evitar falta de operatividad.

Todo cambio critico realizado a un recurso informático y/o sistemas de información debe quedar documentado.

11.1.9 Protección de información almacenada y en tránsito.

ARIETE SEGURIDAD SA establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

11.1.10 Prevención ante otros sistemas de información interconectados.

ARIETE SEGURIDAD SA establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

11.1.11 Registro de actividad del usuario.

ARIETE SEGURIDAD SA, registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Los objetivos principales de la Gestión de incidentes son los de:

- Establecer un sistema de detección y reacción frente a código dañino.
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.
- Este registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente. Velar por la integridad de los sistemas en el caso de un incidente de seguridad.

- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

Todo ello con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales y demás disposiciones que resulten de aplicación.

11.1.12 Seguridad en la gestión de comunicaciones y operaciones.

Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información y los datos personales que se transmitan a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

11.1.13 Protección de la información almacenada y en tránsito.

ARIETE SEGURIDAD SA asegura que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

ARIETE SEGURIDAD SA define modelos de acuerdos de confidencialidad y/o de intercambio de información con los proveedores (terceras partes), que incluyan los compromisos adquiridos y penalidades por el incumplimiento de dichos acuerdos.

ARIETE SEGURIDAD SA define y establece procedimientos para el intercambio de información segura con las diferentes partes interesadas, teniendo en cuenta la utilización de medios de transmisión confiables y la adopción de controles y herramientas seguras, con el fin de proteger la confidencialidad e integridad de la información.

11.1.14 Eliminación y Destrucción de Información.

ARIETE SEGURIDAD SA establece los directrices para que la eliminación, destrucción o borrado seguro de la información, se realice de forma adecuada en el activo de información que la contenga. La eliminación segura de información es un mecanismo de control para prevenir la divulgación de información confidencial de la entidad.

La eliminación segura de medios físicos (USB, Discos duros, entre otros), se puede realizar con diversos mecanismos técnicos tales como: sobreescritura, desmagnetización o destrucción física. De acuerdo con el medio, se establece la herramienta adecuada y el procedimiento a seguir, tanto de información en medio físico o lógico.

11.1.15 Navegación en Internet.

ARIETE SEGURIDAD SA permite el acceso a servicio de internet, estableciendo directrices que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

11.1.16 Uso Correo Electrónico

Toda comunicación por correo electrónico entre las partes interesadas debe efectuarse mediante el uso del sistema aprobado por **ARIETE SEGURIDAD SA** (correo corporativo). Toda información transmitida por este medio es considerada como propiedad de la **ARIETE SEGURIDAD SA**.

Las partes interesadas, no podrán enviar correos internos o externos, que puedan perjudicar la imagen de **ARIETE SEGURIDAD SA**. Así mismo, éstos son responsables del contenido de las comunicaciones enviadas, por lo cual se debe revisar y validar la información a enviar a través del correo electrónico corporativo.

Todo correo saliente debe ir con firma de pie de página del remitente sin excepción.

En el caso de que se reciba una comunicación o correo electrónico sospechoso, de alguien desconocido o spam, debe reportarlo de inmediato, sin abrirlo, al responsable de seguridad de la información.

11.1.17 Seguridad para la Gestión de Contraseñas.

Ningún usuario deberá acceder a la red o a los sistemas de información de **ARIETE SEGURIDAD SA** utilizando una cuenta de usuario o clave de otro usuario.

Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó la clave.

El departamento TI y/o Responsable de Seguridad suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

11.1.18 Pantalla y Escritorio Limpio.

ARIETE SEGURIDAD SA establece las pautas, durante y fuera de la jornada laboral, para preservar la información por medio de buenas prácticas en el manejo de documentos físicos y lógicos, medios de almacenamiento externos y pantallas de los dispositivos de procesamiento de información.

Los usuarios deben conservar el escritorio libre de documentos o dispositivos de almacenamiento con el fin de evitar acceso no autorizado, pérdida y daño de la información de la entidad.

La información confidencial, ubicada en medios físicos o impresos debe ser guardada bajo llave cuando no está siendo utilizada, especialmente cuando la oficina se encuentre vacía.

Los usuarios deben bloquear la pantalla de su computador con el protector de pantalla, cuando no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los documentos que contienen información confidencial deberán ser retirados inmediatamente de la impresora, fotocopiadora o fax, por las partes interesadas responsables, no se deben dejar sin custodia o abandonadas, si esto sucede será tratado como un incidente de seguridad de la información.

11.1.19 Protección frente a código malicioso y código móvil.

ARIETE SEGURIDAD SA asegura el uso herramientas informáticas adecuadas la no propagación o instalación de software con código malicioso el cual pueda comprometer la disponibilidad, integridad y confidencialidad de los servicios soportados por la Infraestructura tecnológica de **ARIETE SEGURIDAD SA**

Queda totalmente prohibida la instalación de software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de **ARIETE SEGURIDAD SA.** Cualquier software que requiera ser instalado para trabajar sobre la red deberá ser evaluado y autorizado por el Responsable de Seguridad y Continuidad.

11.1.20 Gestión de la seguridad de la red.

Los elementos de red (switch, router...etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad del sistema.

Existirá una gestión gráfica de la red de forma que su mantenimiento pueda resultar más cómodo.

11.1.21 Copias de Respaldo de la Información.

ARIETE SEGURIDAD SA garantiza la generación continua de copias de respaldo y almacenamiento seguro de la información crítica, proporcionando los recursos necesarios para establecer sistemas de respaldo adecuados y estableciendo los procedimientos y mecanismos para la realización de estas actividades de manera efectiva, con el fin de asegurar que toda la información esencial de la entidad pueda ser restaurada en caso de ser necesario.

Las copias de respaldos se deben almacenar en un sitio lejano con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño causado por desastres. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Se definen procedimientos de restauración para los medios de respaldo, se verificarán y probarán a intervalos regulares para garantizar la disponibilidad de la información en caso de contingencia o desastre.

11.1.22 Gestión de la continuidad de los sistemas de información y de los datos personales.

Se garantizarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y de los datos personales y se dotarán de planes y medidas necesarias para asegurar la continuidad de los procesos de negocio y la recuperación ante posibles contingencias graves.

11.1.23 Resiliencia de los sistemas de información y de los datos personales.

Se garantizará un nivel apropiado de resiliencia de los sistemas de información y de los datos personales, de forma que permita asegurar y mantener la confiabilidad persistente de los procesos de negocio y de las operaciones de tratamiento de datos personales ante irrupciones relacionadas fallos o ataques informáticos.

11.1.24 Gestión de incidentes de seguridad y de los datos personales.

Cualquier empleado que sospeche u observe una incidencia de seguridad y de los datos personales, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Servicio de Informática para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

ARIETE SEGURIDAD SA dispondrá de mecanismos de detección, notificación interna, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones.

11.1.25 Cumplimiento.

Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos de carácter personal.

11.1.26 Profesionalidad.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de **ARIETE SEGURIDAD SA**.

ARIETE SEGURIDAD SA exigirá que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

11.1.27 Acciones Correctivas.

Se integran en el plan de acciones de mejora las acciones correctivas para eliminar la causa de no conformidades asociadas a las respectivas auditorias y a los requisitos de la política de seguridad con el fin identificar, registrar, controlar, desarrollar, implementar y realizar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

Las acciones correctivas deben ser puestas en conocimiento del Comité de Seguridad y privacidad de la Información. La dirección puede hacer el seguimiento al cumplimiento de las mismas.

11.1.28 Mejora continua del proceso de seguridad.

ARIETE SEGURIDAD SA establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO 27001.

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.

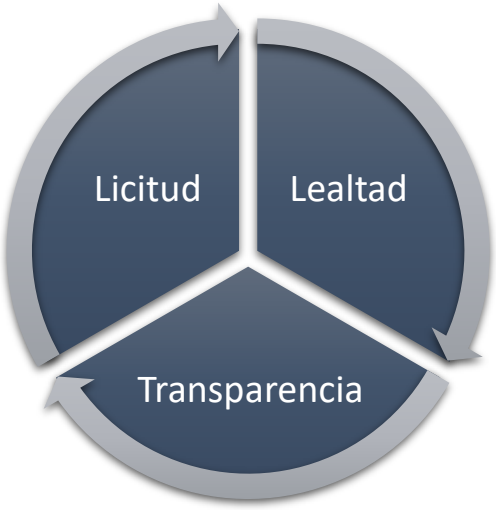
ARIETE SEGURIDAD SA cuando la información bajo su responsabilidad contenga datos de carácter personal, aplicará, además de los principios de seguridad de la información enumerados en el punto anterior, los siguientes principios:

- **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.

11.2.1 Principio de legalidad, lealtad y transparencia

Los principios de licitud, lealtad y transparencia se aplican a todo tipo de tratamiento de datos personales.



Licitud del Tratamiento: sólo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD UE 2016/679.

- **Lealtad del tratamiento.** El interesado deberá ser informado del riesgo para garantizar que el tratamiento no tenga efectos negativos imprevisibles.

- **Transparencia del tratamiento.** El interesado, antes de proceder al tratamiento de sus datos, deberá conocer la finalidad del tratamiento y la identidad del responsable del tratamiento, entre otros detalles. Las normas de información sobre privacidad que deben conocer los interesados se encuentran en los artículos 12, 13 y 14 del RGPD UE 2016/679. Deberá de utilizase un lenguaje claro y sencillo e informarse claramente de los derechos de los interesados en el momento de la recogida o antes de recoger datos personales
- Todos los formularios utilizados para recopilación de datos personales (electrónicos o en papel) deben incluir una información breve de privacidad con un enlace a una declaración de privacidad más extensa y aprobados por el Delegado de Protección de Datos o por el Responsable de Protección de Datos, en su caso**.**

La información que debe facilitarse al interesado debe incluir, como mínimo:

- la identidad y los datos de contacto del responsable del tratamiento y, en su caso, del representante del responsable del tratamiento.
- los datos de contacto del Delegado de Protección de datos, en su caso.
- los fines del tratamiento a que se destinan los datos personales, así como el fundamento jurídico del mismo.
- el período durante el cual se almacenarán los datos personales.
- la existencia de los derechos de acceso, rectificación, cancelación u oposición al tratamiento, y las condiciones (o ausencia de ellas) relativas al ejercicio de estos derechos, como por ejemplo si se verá afectada la legalidad del tratamiento anterior;
- las categorías de datos personales de que se trate.
- los destinatarios o categorías de destinatarios de los datos personales, en su caso.
- en su caso, que el responsable del tratamiento tiene la intención de transferir datos personales a un destinatario en un tercer país y el nivel de protección de los datos
- cualquier otra información necesaria para garantizar un tratamiento justo.

ARIETE SEGURIDAD SA es responsable de informar y establecer los canales adecuados para que los interesados reciban la información sobre sus tratamientos.

11.2.2 Limitación de la Finalidad.

Los datos personales deben de ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

La finalidad del tratamiento de datos deberá definirse antes de que comience el tratamiento e implica que cualquier tratamiento de datos personales debe realizarse con un fin perfectamente definido y solo con fines adicionales especificados que sean compatibles con el original, previa “Evaluación de la compatibilidad” entre ambos fines.

11.2.3 Minimización de datos.

Los datos personales deben de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

- **ARIETE SEGURIDAD SA** debe procurar que no recopile información que no sea estrictamente necesaria para el propósito para el cual fue obtenida.
- Todos los formularios utilizados para recopilación de datos personales (electrónicos o en papel) deben incluir una información breve de privacidad con un enlace a una declaración de privacidad más extensa y ser aprobados por el Delegado de Protección de Datos.

- Siempre que sea posible **ARIETE SEGURIDAD SA** debe aplicar la seudoanimización de los datos personales como garantía para reducir el riesgo concerniente a los interesados. **ARIETE SEGURIDAD SA** debe indicar quienes son sus personas autorizadas para llevar a cabo seudoanimización.

El tratamiento de datos no puede constituir una injerencia desproporcionada en los intereses, derechos y libertades que se ponen en juego.

Las categorías de datos recogidos deberán limitarse estrictamente a aquella información que esté directamente relacionada con el fin específico que persiga el tratamiento, asegurándose que no se recopile información que no sea estrictamente necesaria para el fin específico

Todos los métodos de recolección de datos deben de ser revisados regularmente para asegurar el principio de minimización de los datos.

11.2.4 Exactitud

Los datos personales deben ser exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

ARIETE SEGURIDAD SA es responsable de asegurar que todos los usuarios de los datos personales estén capacitados de la importancia de recoger datos precisos y mantenerlos, así como de que existan procedimientos y políticas apropiadas para mantener los datos personales exactos y actualizados, teniendo en cuenta el volumen de datos recopilados, la velocidad con la que podrían cambiar y cualquier otro factor relevante.

Por otro lado, es responsabilidad de los usuarios de los datos personales asegurarse de que los datos que obran en poder **ARIETE SEGURIDAD SA** sean exactos y que hayan adoptado todas las medidas razonables para que los datos estén actualizados.

No será imputable al responsable del tratamiento, la inexactitud de los datos personales, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, con respecto a los fines para los que se tratan, cuando los datos inexactos:

- Hubiesen sido obtenidos directamente del afectado.
- Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.
- Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.
- Fuesen obtenidos de un registro público por el responsable.

De forma periódica, **ARIETE SEGURIDAD SA** revisará las fechas de retención de todos los datos personales procesados en referencia a los indicado en el Registro de Actividades del Tratamiento e identificará cualquier dato que ya no sea necesario en el contexto de la finalidad registrada.

11.2.5 Conservar los datos personales sólo durante el tiempo que sea necesario.

Los datos personados no deben ser conservados más tiempo del necesario para los fines para los cuales los datos personales son tratados.

- El principio de limitación del plazo de conservación obliga a suprimir o anonimizar los datos personales en el momento en que dejen de ser necesarios para los fines para los que fueron recabados.
- Cuando los datos personales se conserven más allá de la fecha de tratamiento, se reducirán al mínimo, se cifrarán o seudoanimizarán, a fin de proteger la identidad del interesado en caso de violación de los datos o de posibles usos ilícitos.
- Los datos personales se conservarán de acuerdo con el procedimiento de conservación de registros y, una vez transcurrida la fecha de conservación, deberán ser destruidos de forma segura.
- El período de conservación de los datos personales debe ser coherentes con la información contenida en los Avisos de privacidad y cláusulas de transparencia.
- **ARIETE SEGURIDAD SA** debe aprobar específicamente cualquier retención de datos que supere los períodos de retención definidos en el procedimiento de conservación de registros, y debe asegurarse de que la justificación esté claramente identificada y sea conforme a los requisitos de la legislación sobre protección de datos. Esta aprobación debe ser por escrito.
- Los plazos de conservación de los datos se ceñirán a lo estrictamente necesario (extensión del tratamiento) y solo se conservarán más allá, para atender posibles responsabilidades nacidas del tratamiento en base a los plazos legales de conservación.
- De forma periódica, se revisarán los plazos de conservación de todos los datos personales procesados en referencia a los indicado en el Registro de Actividades del Tratamiento e identificará cualquier modificación de estos como consecuencia de nuevos requisitos contractuales o legales.

11.2.6 Seguridad del tratamiento de los datos personales.

Teniendo en cuenta el estado de la tecnología, las medidas de seguridad disponibles, el coste de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, los datos personales serán tratados de tal manera que se garantice un nivel de seguridad adecuada de los datos personales.

Las medidas de seguridad técnicas, organizativas y las medidas de cumplimiento legal son seleccionadas sobre la base de una evaluación de riesgos determinado en el punto anterior donde se tienen en cuenta:

- 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.

ARIETE SEGURIDAD SA y los usuarios de los datos personales deben de comprometerse firmemente en cumplir con todos los aspectos aplicables de la presente política, todas las medidas de seguridad técnicas, organizativas y las medidas de cumplimiento legal determinadas por **ARIETE SEGURIDAD SA**

dentro de su plan de tratamiento de riesgos y aquellas las políticas y normas de seguridad y privacidad implementadas y comunicadas por **ARIETE SEGURIDAD SA** para garantizar una seguridad apropiada.

La gestión de riesgos de seguridad de la información debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

11.2.7 Evaluación de Impacto de Protección de Datos (EIPD)

Aquellas operaciones de tratamiento en los que sea probable que se derive un alto riesgo para los derechos y libertades de las personas físicas, debe corresponder a **ARIETE SEGURIDAD SA** la realización de una Evaluación de Impacto relativa a la Protección de Datos (EIPD), que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo.

Previamente, **ARIETE SEGURIDAD SA** deberá realizar y documentar un análisis previo de las características específicas de cada uno de los tratamientos o actividades de tratamiento para determinar la obligatoriedad de llevar a cabo la evaluación (EIPD). El análisis previo se denomina "Análisis de la Necesidad de hacer la Evaluación de Impacto de Protección de Datos". El resultado de dicho análisis previo determinará si existe un alto riesgo para los derechos y libertades de las personas físicas, y por lo tanto, si realmente las operaciones de tratamientos analizados deben recorrer el proceso de la EIPD, o por el contrario, en caso de no existir un alto riesgo realizar un análisis básico de riesgos

Cuando del resultado del "Análisis de la Necesidad de hacer la Evaluación de Impacto de Protección de Datos" se deriva un alto riesgo, entonces **ARIETE SEGURIDAD SA** deberá realizar la EIPD que deberá incluir como mínimo:

- una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando proceda, el interés legítimo perseguido por el responsable del tratamiento
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad
- una evaluación de los derechos y libertades afectados de los interesados
- las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

En la práctica, **ARIETE SEGURIDAD SA** debe evaluar continuamente los riesgos creados por sus actividades de tratamiento a fin de identificar cuando es probable que un tipo de tratamiento entrañe "un alto riesgo para los derechos y libertades de las personas físicas".

Aunque no exista la obligatoriedad de realizar una EIPD, la **ARIETE SEGURIDAD SA** debe considerar su realización voluntaria ya que es un mecanismo que establece medidas o acciones preventivas, que permite demostrar el cumplimiento del RGPD UE 2016/679 y que se conecta con el concepto de privacidad en el diseño

Delegado de Protección de Datos ofrecerá asesoramiento y supervisión sobre los análisis de riesgo de los tratamientos realizados y sobre las evaluaciones de impacto relativa a la protección de datos que se precisen.

11.2.8 Consulta Previa a la Autoridad de Control (AEPD)

Si una evaluación de impacto relativa a la protección de datos (EIPD) muestra que las operaciones de tratamiento entrañan un alto riesgo que ARIETE SEGURIDAD SA no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes proceder al tratamiento.

11.2.9 Delegado de Protección de Datos

ARIETE SEGURIDAD SA determinará necesidad y obligación de disponer de un Delegado de Protección de Datos según los supuestos previstos en el artículo 37.1 del RGPD UE 2016/679 y en el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDDG)

En el caso de que se determine la obligación de designar un Delegado de Protección de Datos (DPO), deberá procederse a su inscripción al Registro de Delegados de Protección de Datos de la Agencia Española de Protección de Datos.

En el caso de no tener la obligación legal de designar un Delegado de Protección de Datos, **ARIETE SEGURIDAD SA** podrá determinar su nombramiento de forma voluntaria atendiendo a criterios propios (mejora de la responsabilidad proactiva, mejora de la imagen ante terceros, como elemento negociador en caso de conflictos con particulares, etc.)

11.2.10 Protección de Datos desde el diseño y por defecto

La privacidad en el diseño supone aplicar las necesarias garantías de protección de datos desde la fase inicial en el diseño de una nueva actividad del tratamiento, sobre todo cuando esta consiste en desarrollo tecnológico como, por ejemplo, una aplicación o programa, una app, un desarrollo de comercio electrónico, el IoT o internet de las cosas, etc.

La privacidad en el diseño confluye en una actitud proactiva (previene, no remedia) de forma que actúa antes de iniciar las operaciones de tratamiento y busca la protección en todo el ciclo de vida del producto o servicio (de punto a punto).

La privacidad por defecto consiste en ofrecer las máximas garantías de privacidad por defecto. La privacidad por defecto implica, además:

- La minimización de datos, es decir, se recogerán los mínimos datos posibles para que el producto o servicio sea posible y pueda cumplir su finalidad.
- El control de accesos, solo el personal que realmente necesite acceder a los datos para el desarrollo de sus labores profesionales tendrá acceso a dicho datos y por supuesto no se cederán a terceros si esta cesión no es necesaria, no es obligatoria o no está explícitamente informada y consentida por el interesado. Para ello se pueden aplicar técnicas de seudoanimización.
- Los plazos de conservación de los datos deberán estar informados, se ceñirán a lo estrictamente necesario (extensión del tratamiento) y solo se conservarán más allá, para atender posibles responsabilidades nacidas del tratamiento en base a los plazos legales de conservación.
- Transparencia, entendida como proceso de información al interesado sobre los tratamientos de sus datos personales. información clara, concisa y entendible.

En cualquier caso, antes de iniciar cualquier nueva actividad del tratamiento deberán de implementarse los principios de la privacidad desde el diseño y por defecto. El personal o departamento que promocione o impulse la nueva actividad del tratamiento debe solicitar asesoramiento al Delegado o Responsable de Protección de Datos.

11.2.11 Gestionar y revisar las relaciones con terceros que procesan datos personales

Las contrataciones y adquisiciones de proveedores de servicios que supongan o requieran acceso o tratamiento de datos de carácter personal, y que se realice por encargo de **ARIETE SEGURIDAD SA**, la relación se regirá por un contrato u otro acto jurídico con arreglo al Derecho que vincule al proveedor (que pasará a ser encargado del tratamiento) respecto de **ARIETE SEGURIDAD SA** estableciendo el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

ARIETE SEGURIDAD SA recurrirá únicamente a aquellos proveedores de servicios externos que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento.

Previa a la contratación del proveedor de servicios externos se procederá a su evaluación y valoración para determinar si aporta las garantías suficientes que permita el cumplimiento del Reglamento RGPD UE 2016/679

Como mecanismo para demostrar el cumplimiento de las obligaciones (responsabilidad proactiva) es recomendable y valorable positivamente que el proveedor del servicio externo este adherido a un código de conducta aprobado o a un mecanismo de certificación aprobado.

Los proveedores de servicios que accedan a información personal deberán conocer la PSPDP y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación, asimismo, garantizarán la confidencialidad de los mismos.

Antes de iniciar cualquier nuevo acuerdo que implica el tratamiento de datos personales por una organización externa, o se altere un acuerdo existente, el personal o departamento oportuno debe obtener la aprobación del Delegado de Protección de Datos o, en su caso, del responsable de la protección de datos o del responsable de seguridad.

11.2.12 Gestionar y mantener actualizado el Registro de actividades del tratamiento.

ARIETE SEGURIDAD SA gestiona y mantiene actualizado un inventario de todos los tratamientos para los que actúa como Responsable del tratamiento como aquellos tratamientos para los que actúa como Encargado del Tratamiento.

El Registro de Actividades del Tratamiento es un importante instrumento de rendición de cuentas. De hecho, permite obtener un conocimiento profundo de los tratamientos que se producen en **ARIETE SEGURIDAD SA** ya que permite conocer:

- Quien es el Responsable del Tratamiento.
- Porque se procesan los datos personales. Finalidad del tratamiento y base legitima del tratamiento.
- De quién se tratan los datos personales. Categorías de Interesados.
- Que datos personales se tratan. Tipología de datos personales tratados.
- Con quién se comparten los datos personales. Destinatarios.

- Hasta cuándo debo mantener los datos personales. Plazo de conservación de los datos o criterio para determinar el plazo
- Cómo protegemos los datos. Que medidas de seguridad se aplican.
- Si una Actividad del Tratamiento se fundamenta en la base legal del consentimiento debe de mantenerse los registros de los Consentimientos de los interesados y los procedimientos para obtener los Consentimientos.

Todos los responsables de los departamentos pertinentes, la dirección, el Comité de Seguridad y privacidad y protección de datos, el Delegado de Protección de Datos, o en su caso, el responsable de la protección de datos, deben participar en la construcción de los registros de las actividades de tratamientos que deben ser escritos en un lenguaje claro y claro que pueda ser fácilmente comprendido en toda la organización.

Para obtener un resultado óptimo, es necesario involucrar en la confección de los registros a aquellos usuarios y responsables que día a día están manejando, utilizando y manipulando los registros, ya que estos son los mejores conocedores cual es el flujo de la información, cual es el propósito del tratamiento, que datos se están tratando, etc.

En el caso, de que un departamento o usuario precise realizar un nuevo tratamiento para unos propósitos distintos de los identificados en el propio registro, deberá comunicarlo al Delegado de Protección de Datos, en su caso, el responsable de la protección de datos, para estudiar y verificar si el tratamiento es conforme a los principios del RGPD UE 2016/679 y para determinar previamente las medidas de transparencia, limitación, minimización y seguridad a aplicar.

11.2.13 Gestionar cualquier violación de la seguridad de los datos de forma rápida y adecuada.

ARIETE SEGURIDAD SA adoptará todas las medidas necesarias para impedir que se produzcan violaciones de la seguridad de los datos personales. Sin embargo, en el caso de que se produzca una violación de la seguridad de los datos personales **ARIETE SEGURIDAD SA** adoptará todas las medidas necesarias para reducir o mitigar el impacto de los incidentes relacionados con los datos personales mediante el seguimiento del Procedimiento de incidencias y gestión de brechas de seguridad definido por **ARIETE SEGURIDAD SA**

Cuando una violación de la seguridad de los datos personales pueda suponer un riesgo para los derechos y libertades de los interesados, el Delegado de Protección de Datos o, en su caso, el responsable de la protección de datos se pondrá en contacto con la Agencia Española de Protección de Datos e informará de la violación, de conformidad con los requisitos reglamentarios, en un plazo de 72 horas a partir de su descubrimiento.

El Delegado de Protección de Datos o, en su caso, el responsable de la protección de datos también recomendará, cuando sea necesario, medidas para informar a los interesados y reducir los riesgos para su intimidad derivados de la violación.

La pronta notificación de la violación de la seguridad de los datos personales por parte de los usuarios de los datos personales es de vital importancia para atenuar o reducir el impacto y daño de la violación de la seguridad de los datos personales y, por lo tanto, para los derechos de derechos y libertades de los interesados. En tal caso, puede ponerse en contacto con el Delegado de Protección de Datos o, en su caso, al responsable de la protección de datos o al responsable de seguridad.

11.2.14 Gestionar las Transferencias Internacionales de Datos.

El RGPD restringe las transferencias de datos a países no pertenecientes a la UE para garantizar que el nivel de protección de datos que ofrece el RGPD a las personas no se vea afectado. Los datos personales que se transmitan fuera del **Espacio Económico Europeo (EEE)** serán considerada una Transferencia Internacional de Datos (TID).

Sólo podrá transferir datos personales fuera del **del Espacio Económico Europeo (EEE)** si se cumple alguna de las siguientes condiciones:

- La Comisión Europea ha emitido una decisión confirmando que el país al que transferimos los datos personales garantiza un nivel adecuado de protección de los derechos y libertades de los interesados. Los países actualmente aprobados se pueden encontrar aquí:

  https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Existen garantías adecuadas y los interesados cuenten con derechos exigibles y acciones legales efectivas, como normas empresariales vinculantes, cláusulas contractuales tipo aprobadas por la Comisión Europea o por la Autoridad del Control correspondiente (Agencia Española de Protección de Datos), un código de conducta aprobado o un mecanismo de certificación.
- El interesado ha dado su consentimiento explícito a la transferencia propuesta tras haber sido informado de cualquier riesgo potencial; o
- La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado,
- Por razones de interés público,
- Para Establecer, ejercer o defender demandas legales o
- Para proteger los intereses vitales del interesado cuando éste se encuentre física o jurídicamente incapacitado para dar su consentimiento.

ARIETE SEGURIDAD SA cuenta con una amplia gama de acuerdos y cláusulas para garantizar que las transferencias internacionales se realicen bajo la legalidad del RGPD UE 2016/679. Cualquier usuario de los datos personales o departamento antes de realizar o de proceder a realizar una Transferencia Internacional de Datos, bien porque va a proceder a la contratación de un proveedor de servicios externo o bien porque se trata en una transmisión a un nuevo destinatario, deberá previamente solicitar asesoramiento al Delegado de Protección de Datos o, en su caso, al responsable de la protección de datos o al responsable de seguridad.

11.2.15 Responsabilidad proactiva

ARIETE SEGURIDAD SA adoptara los mecanismos e instrumentos necesarios para demostrar el cumplimiento de los principios básicos sobre el tratamiento de datos personales.

ARIETE SEGURIDAD SA aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento (UE) 2016/679. Dichas medidas se revisarán y actualizarán cuando sea necesario.

ARIETE SEGURIDAD SA tiene el deber de cumplir y demostrar el cumplimiento de los principios del RGPD UE 2016/679.

11.3 Gestión de Proyectos

Todos los proyectos relacionados o que afecten a los sistemas de información y/o al tratamiento de datos personales deberán incluir la seguridad de la información y la protección de datos personales en los proyectos como una actividad adicional.

Para la gestión de proyectos se tendrá en cuenta los siguientes puntos:

- Conocer los estándares y normativas de seguridad que aplica al proyecto.
- Identificar responsabilidades de los integrantes del proyecto y de quienes lo supervisan.
- Incluir objetivos de seguridad de la información en los objetivos del proyecto.
- Identificar los activos e información sensible que están involucrados en el proyecto.
- En las fases iniciales de un proyecto se analizarán los riesgos Seguridad de la Información y del tratamiento de datos personales para identificar amenazas/vulnerabilidades y riesgos de seguridad y de protección de datos.
- Se tratarán los riesgos y se implementarán medidas de seguridad para mitigar los riesgos de seguridad y de protección de datos personales.
- Establecer el nivel de sensibilidad de la información que en la gestión del proyecto se utilizará y las medidas de seguridad y control requeridas.
- Contar con la seguridad en todas las fases del proyecto donde se tendrán en cuenta y se aplicarán los conceptos de seguridad y privacidad desde el diseño, codificación segura y los controles y medidas de seguridad que proceda según los riesgos y la sensibilidad de la información.
- Se implementarán planes de acción para la corrección de las desviaciones en riesgos.

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.

12.1 Seguridad ligada a las personas

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información confidencial.

Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información y a los datos de carácter personal, conozca sus responsabilidades, las políticas y procedimientos en materia de seguridad, así como sus obligaciones con arreglo a la legislación en materia de protección de datos y normativa de seguridad, y de este modo, se reduzca el riesgo derivado de un uso indebido de dichos activos.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

12.2 Concienciación y formación.

Todos los miembros de **ARIETE SEGURIDAD SA** recibirán concienciación en materia de seguridad y protección de datos al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **ARIETE SEGURIDAD SA,** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El delegado de protección de datos supervisará las acciones de concienciación y formación del personal que participa en las operaciones de tratamiento con datos personales, a fin de garantizar el cumplimiento de la presente Política.

12.3 Líneas de responsabilidad de los usuarios de la información y de los datos personales.

Para garantizar un nivel de seguridad adecuada de la información y de los datos personales, es esencial una activa implicación de los usuarios donde:

- Tengan concienciación de su papel en el cumplimiento de las medidas de seguridad, garantías y mecanismos que aseguren la seguridad de la información y el cumplimiento de la normativa de protección de datos personales.
- Utilicen y empleen todos los procedimientos y tecnologías puestas en marcha para mantener la seguridad de la información y de todos los datos personales (garantizar el secreto de las claves, bloqueos de sesión, garantizar la confidencialidad, mantener escritorio y pantalla limpio, etc.)
- Transfieran la información de **ARIETE SEGURIDAD SA** y de los datos personales únicamente a los proveedores de servicios que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas adecuadas y que estén de acuerdo por escrito en cumplir con las políticas y procedimientos necesarios para garantizar un tratamiento seguro para los derechos y libertades de las personas físicas.
- Mantengan la seguridad de los datos mediante la protección de la confidencialidad, integridad, disponibilidad, integridad y autenticidad de la información y de los datos personales, que se define de la siguiente manera
- Notifiquen, sin dilación indebida, cualquier incidencia[1] o brecha de seguridad que pueda afectar a los datos personales de la que tenga conocimiento el Delegado de Protección de Datos o Responsable de Seguridad.

13 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

[1] Se entiende por incidencia, cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

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

14 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.

15 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.

16 LISTA DE CONTROL DE CAMBIOS

Versión	Fecha de entrada en vigor	Breve descripción del cambio
01	15/02/2023	Realización inicial
02	24/01/2026	Se Restructura el punto de Organización de la Seguridad y modificaciones en el texto por la integración de la norma ISO 22301
03	09/03/2023	Se modifica el redactado de los capítulos 7 y 8 para identificar claramente las diferencias entre el Comité de Seguridad y Privacidad y el Comité de Continuidad.