VadilloAsesores GRUPO +70 años

Proceso de Apoyo de Información y Digitalización

PA-IN-PO-01

Política de seguridad de la información

Revisión y publicación

VERSIÓN	FECHA	MOTIVO DEL CAMBIO
01	14/11/2008	Primera Emisión
02	15/05/2009	Modificar alcance.
03	Abril 2011	Implementar requisitos de clientes Cambio del esquema de la red Actualizado del esquema de la norma
04	Diciembre 2011	Adaptación del apartado Evaluación de Riesgos según la metodología Magerit. Enfoque a las características del negocio, repasar el cumplimiento legal y mejorar la redacción.
05	Septiembre 2013	Actualización
06	Octubre 2014	Revisión
07	Julio 2015	Actualización del apartado 7 comunicación
08	Diciembre 2016	Actualización del apartado 1.4.2 suprimiendo la oficina de Bilbao, ampliación del alcance a las oficinas físicas especialmente en cuanto a documentación física
09	Septiembre 2017	Revisión
10	Mayo 2018	Seguridad de los Recursos Humanos. Comunicación interna y externa. Infraestructura informática. Responsable de Seguridad y Administrador de los sistemas.
11	Junio 2019	Actualización contexto de la organización y grupos de interés. Actualización Política SGSI
12	Abril 2020	Actualización infraestructura de red. 1.1. Contexto de la Organización 1.2. Empresas participadas 1.3. Análisis del contexto 1.4. Misión, visión y valores Grupos de Interés

13	Junio 2020	Actualización del apartado 1.9. Requisitos Legales Se incluye en el apartado 4.1.5. Propietario de Riesgos Se actualiza el apartado1.5 relativo a los Requisitos y Expectativas de los Grupo de interés Introducción del apartado 1.11 Seguimiento, medición y mejora
14	Marzo 2022	Adecuación a nuevo formato y numeración. Cambio de responsable de seguridad. Actualización mapa red. Revisiones y cambios menores. Se revisan las referencias a otros procedimientos o documentos.
15	Julio 2022	Adaptación a la normativa ENS. Reorganización del documento y las referencias a los distintos procedimientos.
16	Octubre 2022	Se arreglan referencias a otros procedimientos.
17	Abril 2023	Se revisa el capítulo “Objetivos” para evitar redundancias con la Normativa de seguridad (PA-IN-MA-01).
18	Diciembre 2023	Se modifica el marco normativo
19	Marzo 2024	Se revisa la política. Sin cambios.
20	Abril 2024	Se revisa cumplimiento con art.11 y 12.6 de RD 311/2022.
21	Julio 2025.	Revisión de la estructura y el contenido del documento y alineación a la estrategia de la empresa

REALIZADO Y REVISADO		FIRMA
Versión:	21	
Nombre:	Olatz y Susana.	
Fecha:	Julio 2025	

APROBADO		FIRMA
Nombre:	José Antonio Gómez Vadillo	GOMEZ VADILLO JOSE ANTONIO - 16259199Q Firmado digitalmente por GOMEZ VADILLO JOSE ANTONIO - 16259199Q Fecha: 2025.10.06 13:22:55 +02'00'
Fecha:	06/10/2025	

PUBLICACIÓN EN	FORMATO	RUTA
SharePoint	PDF	PROYECTOS > PA INFORMACION Y DIGITALIZACION > MODO DE FABRICACIÓN > POLÍTICAS
SharePoint	PDF	DOCUMENTACION NORMATIVA > SEGURIDAD
Web corporativa	PDF	www.grupovadillo.com

ÍNDICE

1. Introducción

El propósito de esta Política de la Seguridad de la Información es proteger, en todos los ámbitos, los activos de información de Vadillo Asesores (VA). La Seguridad de la Información debe velar, teniendo en cuenta los requisitos internos y externos de la organización, para la correcta operación de la organización y la satisfactoria ejecución de los servicios a los clientes y demás grupos de interés.

Vadillo tiene implantado, y mejora continuamente, un Sistema de Gestión de la Seguridad de la Información acorde con la norma UNE-ISO/IEC 27001:2022 y con el Esquema Nacional de Seguridad.

Esta Política de Seguridad se aplica en todas las empresas de Vadillo Asesores en todas sus instalaciones, y en especial a todos los empleados, que deben seguir las directrices en la medida que afecten a su trabajo. También aplica a los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información.

Todos los procesos internos y externos quedan adscritos a la presente política o cuantas políticas transversales se desarrollen para dar cumplimiento a la misma.

Esta Política de Seguridad tiene vigencia desde la aprobación por la Dirección de Vadillo Asesores y mientras no se apruebe una posterior, se mantendrá vigente. La Política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

Cualquier violación de esta política o de cualquier procedimiento u otro documento que la desarrolle, por parte de personal interno o colaboradores externos, estará sometida a procedimiento disciplinario.

1.1 Alcance

El Sistema de Seguridad de la Información de Vadillo Asesores (VA), se ha asociado a los sistemas y procesos empleados en los servicios de outsourcing y gestión de sistemas de información y telecomunicaciones conforme a la declaración de aplicabilidad en vigor, desarrollados en las instalaciones de Vadillo Asesores en Vitoria-Gasteiz (Araba/Alava).

1.2 Compromiso de la dirección

La Dirección de Grupo Vadillo Asesores está comprometida con el desarrollo, implantación, mantenimiento y actualización del Sistema de Gestión de la Seguridad de la Información a través de un Comité de Cumplimiento, para el control de este.

Esta política es aprobada por la dirección de Vadillo Asesores como muestra del compromiso existente, así como para favorecer el cumplimiento y conocimiento de esta a toda la organización.

Tanto Dirección como el Comité de Cumplimiento validarán las cuestiones de definición del Sistema y realizarán las oportunas supervisiones de la operativa. Estos trabajos se resumen en:

- Comunicar a la organización la Política de Seguridad, así como de las modificaciones a la misma.
- Establecer el alcance del sistema, los niveles de riesgo aceptables, roles y nombramientos y cualquier otro parámetro que afecte significativamente al sistema.
- Verificar que se realizan todas las auditorías internas, externas y los trabajos que estén planificados.
- Proporcionar los recursos necesarios.

La Seguridad de la Información está implícita en cada uno de los puntos de esta Política, e integrada en los procesos de negocio de Vadillo Asesores. Esta política queda alineada plenamente con los objetivos de negocio e integrada en la estrategia de la organización.

1.3 Objetivos Generales

La gestión de la Seguridad de la Información debe de estar alineada a:

1. La visión estratégica de Resiliencia; estableciendo medidas preventivas, adaptativas y controles, que mitiguen los riesgos y permitan una recuperación rápida ante los incidentes.

2. La responsabilidad Social Corporativa, como garantía de la reputación de la marca de VA, teniendo como principio básico el cumplimiento normativo.

3. La gestión por Gerencia de Riesgos y oportunidades, identificando como activo crítico los datos y la información. Y como riesgo critico la ciberseguridad.

4. La mejora continua.

Para alcanzar una gestión eficiente, se establecen anualmente objetivos específicos (Seguimento de objetivos 2025 (1).xlsx) en relación a la Seguridad de la Información, que garantizan la mejora continua del SGSI, siendo estos consistentes con los presentes objetivos.

1.4 Objetivos específicos

Los objetivos específicos del Sistema de Gestión de la Seguridad de la Información son:

- Proteger la información como una de las principales materias primas de la organización en todas sus dimensiones:

    - Confidencialidad: disponible únicamente para las personas autorizadas y durante el tiempo mínimo necesario. Cualquier acceso lógico o físico a la información estará controlado.

    - Integridad: evitar la manipulación no autorizada y mantener la veracidad de la información.

    - Disponibilidad: debe estar accesible cuando se necesita

- Trazabilidad: posibilidad de imputar a un autor concreto cualquier acción realizada
- Autenticidad: garantizar la identidad del usuario que accede

- Mejorar la confianza de todos los grupos de interés para Vadillo Asesores
- Implantar de un proceso de digitalización en la organización
- Asegurarse de que el equipo, los aliados y proveedores, conoce y comprende los problemas asociados a la seguridad de la información. Que asumen y son conscientes de sus responsabilidades en este tema.
- Proporcionar una guía para establecer los estándares, procedimientos y medidas de seguridad para desarrollar un Sistema de Seguridad de la Información.
- Maximizar la disponibilidad y calidad de los servicios prestados a nuestros clientes, garantizando la continuidad del negocio.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo a su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos.
- Reducir o eliminar los peligros y riesgos inherentes a nuestras actividades, por medio de la mejora continua del desempeño en seguridad, en nuestros procesos, productos y servicios.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información. El personal debe estar formado para poder gestionar el Sistema de Gestión de la Seguridad de la Información y aplicar sus contenidos.
- Mantener a disposición de las partes interesadas nuestra Política presente, así como los futuros desarrollos de esta.
- Establecer los objetivos anuales referidos a la Seguridad de la Información, manteniendo una actualización y mejora continua del sistema.
- Asegurar que los activos de la organización solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información.
- Reflejar en la Declaración de Aplicabilidad del SGSI (RG_SOA_27001) los objetivos de control definidos para el SGSI de Vadillo Asesores, basados en los controles recogidos en el Anexo A de la norma 27001.
- Reflejar en la Declaración de Aplicabilidad del ENS (RG_SOA_ENS) las medidas de seguridad y dimensiones definidos en el Esquema Nacional de Seguridad.
- Mantener la coordinación con los distintos Sistemas de Gestión (Compliance y LOPD).

Y todo ello dentro del marco de los objetivos estratégicos de la organización y de toda la legislación aplicable.

1.5 Principios de la seguridad

El SGSI de VA se rige por los siguientes principios de seguridad:

- La gobernanza del dato y la privacidad son dos activos críticos.
- La seguridad de la información será un criterio clave en cualquier cambio o adición de cualquier sistema o proceso de la organización: seguridad por defecto. La continuidad de los servicios es prioritaria.
- La seguridad se gestionará en base a los procesos existentes en la organización.
- La seguridad implica a toda la organización de una u otra manera.
- La información será accesible según el principio de mínimo privilegio, incluyendo el marco temporal.
- La concienciación, información y formación es imprescindible para mitigar la fuente de amenazas que son las personas.
- Tener un sistema certificado y auditado externamente es una garantía para mitigar el riesgo de los procesos y controles.
- Garantizar un cumplimiento normativo en:
    - Tratamiento de datos personales.
    - Propiedad Intelectual.
    - Comercio electrónico.
    - Uso responsable de la Inteligencia Artificial.
- Los incidentes de seguridad deben ser gestionados con eficacia para resolverlos en el menor tiempo posible y posibilitar la obtención de lecciones aprendidas.

2. Marco normativo

En el documento RE-01 LEGISLACIÓN APLICABLE GVA.xlsx se presenta el marco legal y regulatorio en el que se desarrollan las actividades de la organización, identificándose las obligaciones legales aplicables a la misma en relación a la seguridad de la información. Este registro es revisado anualmente, actualizándose además en el caso de que se produzcan cambios en la legislación considerada, o que se requiera incluir nuevas obligaciones.

Además, se consideran los requisitos contractuales establecidos en contratos de clientes o proveedores que requieren de requisitos específicos en materia de seguridad.

Asimismo, Vadillo Asesores se obliga a la implantación eficiente del Sistema de Gestión de la Seguridad de la Información certificado externamente bajo la ISO 27.001 y bajo el ENS en grado medio.

Existe un procedimiento específico para el cumplimiento de toda la legislación aplicable:

"PA-IN-PR 01 Procedimiento cumplimiento legislacion .doc

3. Roles y funciones de seguridad

El documento "*PA-IN-MA-02 Estructura de seguridad (1).docx* establece los distintos roles de la organización con respecto a la seguridad de la información, así como los distintos procedimientos para su nombramiento, aprobación y comunicación al personal.

La designación de estos roles debe establecer los requisitos mínimos para garantizar la profesionalidad de las personas designadas, así como garantizar que puedan ejecutar sus tareas con imparcialidad y sin presiones jerárquicas. Estos requisitos se establecen por puesto de seguridad en los registros de *PA-IN-RE-11 Requisitos de perfiles de puestos*

El responsable de seguridad tiene potestad para decidir las medidas de seguridad a implantar y para aprobar o rechazar las solicitudes recibidas. En caso de conflicto, el afectado podrá elevar al comité de seguridad su reclamación para su evaluación. En cualquier caso, Dirección podrá decidir sobre cualquiera de estos supuestos sin necesidad de convocatoria del comité de seguridad.

4. Comité de Cumplimiento

El documento PA-IN-PR-02 Comité de cumplimiento Normativo la composición y calendario de los comités de VA y, en concreto, en lo que aplica a esta política, hace referencia a los Riesgos de la Información.

En concreto, la gestión de los riesgos de la información debe velar por el cumplimiento de esta política, así como de todos los procedimientos y controles que se establezcan como consecuencia de ella y para mantener la operativa de la organización, incluyendo el análisis y gestión de los riesgos que existan.

Los miembros que integran este Comité vienen detallados en el documento PA-IN-PR-02 Comité de cumplimiento Normativo

5. Gestión del riesgo.

El sistema de información sujeto a esta política dispondrá de su correspondiente análisis de riesgos, evaluando las amenazas, los riesgos a los que están expuestos, y desplegando sus planes de tratamiento. Este análisis se repetirá:

- Anualmente.

- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra una incidencia grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de cumplimiento establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Esta metodología se recoge en el procedimiento *PA-IN-PR-15 Analisis de Riesgos.docx*

6. Gestión de incidentes

El proceso de gestión de incidentes de Vadillo Asesores, *PA-IN-PR-09 Gestión de incidencias y reclamaciones* y sus notas técnicas; incluyen la detección y notificación de los incidentes de seguridad, los criterios de clasificación, los procedimientos de análisis y resolución, así como los canales de comunicación a las partes interesadas, especialmente cuando afecta a terceros, y el registro de las actuaciones ejecutadas.

Los incidentes de seguridad permiten la recopilación de evidencias, de manera que se pueda identificar y documentar la recogida, la adquisición y la preservación de la información.

7. Continuidad del servicio.

Vadillo Asesores dispone de un Plan de Continuidad del Negocio (PCN) y un Plan de Recuperación ante Desastres (DRP), desarrollados en el DC-INF-01-02 Plan de Continuidad del negocio -firmado (1) (1).docx cuyo objetivo es garantizar la disponibilidad de los servicios esenciales y la recuperación de los sistemas de información ante incidentes graves.

Estos planes están documentados, se revisan periódicamente y se prueban para asegurar su eficacia.

La política de continuidad está alineada con los requisitos del Esquema Nacional de Seguridad (ENS) y forma parte del Sistema de Gestión de la Seguridad de la Información (SGSI).

8. Desempeño: Desarrollo de la política de seguridad de la información

Esta política se desarrollará por medio de:

- La Normativa de Seguridad ("*PA-IN-MA-07 Normativa de seguridad.docx*" y "*PA-IN-MA-01 PA-IN-MA-01 Manual de seguridad (7).pdf*
- Los procedimientos de Seguridad
- Notas técnicas que afrontarán aspectos específicos de los mismos,

todos ellos elaborados a los efectos del cumplimiento del RD 311/2022, de 3 de mayo y los controles exigidos por la ISO 27001.

La documentación mencionada estará a disposición de las personas autorizadas y, en su caso, de las entidades externas afectadas y ubicada en el sitio de SharePoint de Documentación Normativa.

Tanto la política como la normativa de seguridad deberán ser difundidas para su conocimiento y aplicación por todo el personal. Se realizarán recordatorios anuales o, en períodos inferiores, si se produjeran cambios sustanciales en la misma con anterioridad.

La actividad profesional que demandan nuestros clientes se basa en un atributo que es la confianza. Este atributo, queda enfocado en los valores de la organización, que están reflejados en todos nuestros procesos, en las capacidades y comportamientos de nuestras personas.

Entendemos que “las materias primas”, que gestionamos son:

- La información de nuestros clientes.
- El conocimiento de las personas del equipo.
- Y el tiempo que dedicamos a la actividad.

Por todo ello, marca y materias primas de fabricación, junto con la confianza que es el atributo esencial que demandan los clientes, tienen que estar gestionados con unos criterios que permitan proteger todas las dimensiones referenciadas en esta política: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad. Por tanto, en Vadillo Asesores, se establecen acciones para garantizarlo:

- Dotar de los medios necesarios para una correcta protección contra pérdidas de disponibilidad, confidencialidad e integridad.
- Dotar de los medios necesarios para una correcta protección contra accesos no autorizados.
- Dotar de los medios necesarios para el cumplimiento de los requisitos legales aplicables.
- Dotar de los medios necesarios para el cumplimiento de los requisitos de los clientes, llegado el caso.
- Dotar de los medios necesarios para el cumplimiento de los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
- Tratamiento y comunicación adecuadas en gestión de incidencias de seguridad.
- Establecimiento de procedimientos para asegurar el cumplimiento de esta Política de Seguridad.
- Dotar de los medios necesarios para el cumplimiento de la Política y sus procedimientos, notas técnicas y demás requisitos por parte de la organización

9. Formación y concienciación

Todas las personas de VA tienen la obligación de conocer y cumplir esta política de seguridad de la información, así como de la documentación que la desarrolla en la medida que les afecte, siendo responsabilidad del Comité de Cumplimiento disponer los medios necesarios para que la información les llegue.

Todas las personas de VA atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

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

Todas las personas propias o de terceros al servicio de VA deberán conocer y aplicar la presente política y la normativa de seguridad.

10. Terceras partes

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

Para los servicios prestados por proveedores, VA les hará partícipes de esta política y normativa de seguridad de la información que atañe a dichos servicios o información. Dichos proveedores estarán sujetos a las obligaciones establecidas en esta política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de esta Política de Seguridad 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/as responsables de la información y los servicios afectados antes de seguir adelante.

SAGARDUY ANTUNEZ OLATZ - 79188042P

Firmado digitalmente por SAGARDUY ANTUNEZ OLATZ - 79188042P
Fecha: 2025.10.06 13:50:57 +02'00'