Política de Seguridad de la Información de Vicomtech

ÍNDICE

Contents

1. Aprobación y entrada en Vigor

Esta Política ha sido propuesta y revisada por el **Comité de Seguridad de la Información** de Vicomtech y aprobada el 27/11/2025 por la Dirección de **Vicomtech**.

La aprobación de esta Política de Seguridad obliga a Vicomtech tanto internamente como **frente a terceros**. En cumplimiento con el Esquema Nacional de Seguridad (ENS) y para garantizar que todos/as los/as interesados/as conozcan el alcance del compromiso adquirido, esta Política **será objeto de publicación** a través de la página web de **Vicomtech**.

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

La entrada en vigor de la presente Política de Seguridad de la Información de Vicomtech supone la derogación de cualquier otra que existiera anteriormente.

Esta política de Seguridad de la Información **será revisada al menos una vez al año** y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la organización.

En caso de conflictos o diferentes interpretaciones de esta Política de Seguridad de la Información se recurrirá a Dirección para resolución de estos, previa consulta al **Comité de Seguridad de la Información.**

2. Misión, objetivos y Buen Gobierno de Vicomtech

Vicomtech tiene como misión:

- Responder a las necesidades de Investigación Aplicada, Desarrollo e Innovación en Tecnologías de la Información, especialmente la convergencia de Computer Graphics y Computer Vision (Visual Computing), Data Analytics & Intelligence, Interactive Digital Media y Language Technologies, de las empresas e instituciones de nuestro entorno, para afrontar los nuevos retos económicos y sociales, mejorando su competitividad en un mercado global.
- Impulsar la Generación de Conocimiento y la Transferencia de nuestras tecnologías, desarrollando prototipos de nuevos productos y facilitando nuevas líneas de negocio en

cooperación con la industria, y soportados en Propiedad Intelectual original.

- Perseguir la excelencia en los aspectos científicos, técnicos, de organización interna y de servicio al cliente, cumpliendo con los más altos estándares y normativas de calidad reconocidos en los ámbitos científicos e industriales.
- Contribuir al conocimiento universal mediante la formación de personas investigadoras y la publicación de los resultados obtenidos de los trabajos de investigación aplicada en revistas y congresos de prestigio internacional.
- Desarrollar alianzas con socias y socios estratégicos de referencia (académicos, de investigación aplicada e industriales), tanto locales como internacionales, para la promoción de la investigación aplicada en red, la formación de personas investigadoras y generación conjunta de conocimiento.
- Fomentar un entorno de desempeño profesional de excelencia y calidad, que permita a nuestro personal desarrollar las habilidades necesarias para trabajar en equipo y ser promotores del cambio tecnológico, y de la innovación en general, tanto en el propio centro, como en su salida a la industria o a otros ámbitos científico-tecnológicos.

Vicomtech tiene como principales objetivos:

- Contar con una Masa Crítica Investigadora que esté homologada con los criterios establecidos por el Gobierno Vasco y cuente con Perfiles de Investigador Excelente a través de la codirección tesis doctorales en colaboración con Universidades Vascas.
- Fomentar la Publicación de Artículos de Investigación en revistas de primer nivel.
- Transferir el conocimiento generado a la Industria y Sociedad a través de: la contratación de proyectos de investigación aplicada, la protección y transferencia de activos, la transferencia de talento humano o el impacto en nuevas empresas de base tecnológica

El cumplimiento de estos objetivos debe realizarse velando por el **Buen Gobierno** del Centro cuyos pilaren son: la cultura, la ética, la responsabilidad, la transparencia, la eficiencia, la gestión del riesgo y la integridad.

Vicomtech hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

3. Objetivos y misión de la política de Seguridad de la Información

La presente **Política** establece las directrices y líneas de actuación en materia de Seguridad de la Información que rigen el modo en que **Vicomtech** gestiona y protege su información y sus servicios, así como la comunicación con sus clientes y clientas y otros grupos de interés.

Vicomtech ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad**, en adelante **ENS**, y el Sistema de Gestión de Seguridad de la Información **ISO/IEC 27001**, en adelante **SGSI**, integrado dentro del Sistema de Gestión Integral, en adelante **SGI.**

La gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de estos. Para ello, se establecen como **objetivos generales** en materia de seguridad de la información los siguientes:

- Contribuir desde la gestión de la seguridad de la información a cumplir con la misión y Buen Gobierno establecidos por Vicomtech.
- Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos de carácter personal y a la prestación de servicios a través de medios electrónicos.
- Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
- Proteger los recursos de información de Vicomtech y los activos utilizados para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, autenticidad y legalidad de la información.

La **Dirección** de **Vicomtech** se **compromete** manifiestamente a la difusión, consolidación y cumplimiento de la presente **Política de Seguridad de la Información.**

4. Alcance

Esta Política será de aplicación y de obligado cumplimiento para todas las actividades de Vicomtech, a todos sus recursos y centros de trabajo y a los procesos afectados por el ENS/SGSI y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Los diferentes departamentos deben 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.

Cada persona miembro de Vicomtech, afectada por el alcance del ENS/SGSI **tiene la obligación de conocer y cumplir esta Política de Seguridad**, así como los procedimientos de Seguridad de la Información que la complementan, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. Marco Normativo

Esta política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y se desarrollará aplicando los requisitos mínimos establecidos en el ARTÍCULO 12. POLÍTICA DE SEGURIDAD Y REQUISITOS MÍNIMOS DE SEGURIDAD.

El marco de gestión de seguridad de la información abarca igualmente la protección de datos de carácter personal y tiene en cuenta lo dispuesto en el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016**, en adelante **RGPD**, así como lo contemplado en la legislación de carácter nacional en dicha materia.

Así mismo, se ajustará a lo establecido en la ley 59/2003 por el “Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior” y añadir la “Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza”.

Además, resultarán de aplicación cuantas otras normas que regulen la actividad de **Vicomtech** en el ámbito de sus competencias y aquellas otras dirigidas a asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en los medios electrónicos gestionados por el Centro igualmente en el ejercicio de sus competencias.

6. Principios de Seguridad de la información

6.1. Seguridad Integral

La seguridad se entenderá como un proceso integral que aplica a todas las actividades de la organización, y está constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información.

6.2. Gestión de la seguridad basada en riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, permitiendo el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

6.3. Prevención, detección, respuesta y conservación

Vicomtech **prevendrá y evitará**, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad**.** Para ello, sus órganos responsables implementarán las medidas mínimas de seguridad determinadas por el ENS/SGSI y por el RGPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estas medidas y controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidas y documentadas, en el **Manual de Gestión Integral**, asegurando que se garantiza la adecuada prevención, detección, respuesta y conservación para garantizar el cumplimiento de esta **Política de Seguridad de la Información**.

6.4. Líneas de defensa

El sistema dispondrá de una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas falle, permita:

- Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto para asegurar la continuidad del negocio.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa estarán constituidas por medidas de naturaleza organizativa, física y lógica.

6.5. Vigilancia continua y reevaluación periódica

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI/ENS de **Vicomtech** con los

requisitos de la Norma ISO/IEC 27001 para el SGSI y con el Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de las mismas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

Las medidas y controles de seguridad se reevaluarán y actualizarán periódicamente dentro del Sistema de Gestión de Seguridad de la Información, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

6.6. La seguridad como función diferenciada

En consonancia con el artículo 10 del Esquema Nacional de Seguridad se diferenciará la persona responsable de la información, la persona responsable del servicio, la persona responsable de la seguridad de la información y la persona responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La persona responsable de la información determinará los requisitos de la información tratada; la persona responsable del servicio determinará los requisitos de los servicios prestados; y la persona responsable de seguridad de la información determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. La persona responsable del sistema se encargará de la operación del Sistema de información atendiendo a las medidas de seguridad determinadas

6.7. Seguridad por defecto y desde el diseño

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto.

Este principio implica que:

- La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas IT.
- Los sistemas deberán proporcionar la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados

7. Organización de la Seguridad de la información

Vicomtech ha adoptado un modelo de Gobernanza de la Seguridad de la Información basado en la **diferenciación de responsabilidades.**

Este modelo ha sido seleccionado y estructurado de forma motivada para coordinar la seguridad,

tanto en sistemas IT como en otras materias, y para asegurar la correcta distribución de la información y la toma de decisiones corporativas en Vicomtech.

La estructura de gobernanza se articula mediante el **Comité de Seguridad de la Información,** un órgano colegiado esencial para la gestión y coordinación de la seguridad, y la designación de los **roles unipersonales** definidos en el ENS (Real Decreto 311/2022):

7.1. Comités: Funciones y responsabilidades

7.1.1. Comité de Dirección

En materia de seguridad de la información, el **Comité Dirección de Vicomtech** tiene las siguientes funciones:

- Aprobar la Política de Seguridad de la Información de Vicomtech y cualquier otra política sectorial complementaria de la anterior que permita el cumplimiento de los Esquemas Nacionales de Seguridad y el Reglamento General de Protección de Datos.
- Aprobar el desarrollo organizativo propuesto por el **Comité de Seguridad de la Información**.
- Nombrar y cesar a los integrantes del **Comité de Seguridad de la Información**.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del **Comité de Seguridad de la Información**.
- Nombrar al Delegado/a de Protección de Datos de **Vicomtech**.

7.1.2. Comité de Seguridad de la Información

El **Comité de Seguridad de la Información**, será encargado de coordinar la seguridad de la información en Vicomtech.

Estará formado por los siguientes responsables que serán definidos por el Comité Dirección:

- ✓ Responsable de la Información.
- ✓ Responsable del Servicio.
- ✓ Responsable de Seguridad de la Información
- ✓ Responsable del Sistema
- ✓ Administrador/a de la Seguridad del Sistema
- ✓ Técnico/a del Sistema de Gestión Integral

El **Comité de Seguridad de la Información** tendrá las siguientes funciones:

- Elaborar la estrategia de evolución de **Vicomtech** en lo que respecta a seguridad de la información y promover la mejora continua.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por el Comité Dirección.
- **Asegurar la adecuada publicidad de la Política de Seguridad,** velando por su difusión interna y, especialmente, por su **publicación externa** para que sea conocida por todos/as los/as interesados/as, internos/as y externos/as a la organización.
- Elaborar y aprobar los requisitos de formación y calificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad de la información.
- Identificar incumplimientos y proponer sanciones
- Establecer el nivel de riesgo aceptable, aprobar los riesgos residuales y comunicarlos a los responsables de los activos.
- Monitorizar los principales riesgos residuales asumidos por **Vicomtech** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de Vicomtech y en particular, velar por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación.
- 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 al Comité de Dirección.

7.2. Roles: Funciones y Responsabilidades

Las funciones y responsabilidades de cada figura del Comité de Seguridad de la Información serán las siguiente:

7.2.1. Responsable de la Información

La persona responsable de la Información tendrá la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección, siendo la responsable última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

Sus funciones son:

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

7.2.2. Responsable del Servicio

Le corresponde la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, la potestad de determinar los niveles de seguridad de los servicios.

Sus funciones son:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

7.2.3. Responsable de Seguridad de la Información

Cumplirá funciones relativas a la seguridad de los sistemas de información de Vicomtech, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en **Vicomtech**.

Sus funciones son:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos de este.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Gestionar la formación y concienciación en materia de seguridad de la información.

- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar y completar y toda la documentación relacionada con la seguridad del sistema.
- Determinar la categoría del sistema, en colaboración con la persona responsable del sistema, para su eventual aprobación por el Comité de Seguridad de la Información.
- Gestionar los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité de Seguridad de la Información.

7.2.4. Responsable del Sistema

Esta figura será la encargada de las operaciones del sistema y sus funciones son:

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Prestará a la persona responsable de seguridad de la información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspender del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

7.2.5. Administrador/a de la Seguridad del Sistema

Administrará las funcionalidades de seguridad determinadas por las personas responsables anteriores, sus funciones serán:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a las personas Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.2.6. Técnico/a de Gestión Integral

Sus funciones son:

- Revisar, completar y toda la documentación relacionada con la seguridad del sistema.
- Apoyar en la gestión de la formación y concienciación en materia de seguridad de la información.
- 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 de Seguridad de la Información.

7.2.7. Otros posibles roles

Cuando el Comité de Seguridad de la información lo considere oportuno, podrá hacer partícipe a modo consultivo de sus reuniones a otras personas responsables en Vicomtech.

7.2.7.1. Delegado/a de Protección de Datos

Persona encargada de garantizar que los datos personales se tratan y se protegen conforme al

Reglamento General de Protección de Datos (RGPD UE 2016/679).

7.2.7.2. Oficial de Seguridad

En Vicomtech, se maneja en ocasiones Información Clasificada que puede afectar a la seguridad nacional. El/La Oficial de Seguridad es la persona encargada de conocer qué proyectos del centro están clasificados bajo esta categoría y cuáles son los requisitos que deben cumplir.

7.3. Resolución de Conflictos

En el caso de conflictos entre la persona Responsable de la Información, la persona Responsable del Servicio, la persona Responsable de la Seguridad, o la persona Responsable del Sistema, **el Comité de Seguridad de la Información será el órgano encargado de dirimir las discrepancias** y tomar la decisión vinculante. Si el Comité de Seguridad no tuviera suficiente autoridad, **se elevará la discrepancia al Comité de Dirección de Vicomtech** para su resolución definitiva.

7.4. Directrices de Estructuración Documental

La Política de Seguridad de la Información de Vicomtech es un documento de alto nivel que define la postura de la organización sobre la seguridad.

- Para garantizar su correcta aplicación y desarrollo operativo, Vicomtech define los procedimientos que se utilizarán para la implementación de las medidas de seguridad, siendo estos coherentes con esta Política y con el Sistema de Gestión Integral (SGI) de Vicomtech.
- La documentación de seguridad del sistema, su gestión y acceso, se estructurará jerárquicamente en los siguientes instrumentos de desarrollo:

1. Manual de Gestión Integral y P-05.14-Directrices de seguridad de la información:

- Contienen la relación documental relativa a la Seguridad de la Información y su integración dentro del Sistema de Gestión Integral.

2. Procedimientos generales y específicos:

- Son documentos de carácter obligatorio
- Tienen como objetivo uniformizar el uso de aspectos concretos del sistema
- Indican el uso correcto y las responsabilidades específicas de los usuarios
- Su propósito es ayudar a los/as usuarios/as a aplicar correctamente las medidas de seguridad
- Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad.

3. **Instrucciones:**

- Afrontan tareas concretas y repetitivas

- Indican lo que hay que hacer paso a paso para garantizar la operación segura

Toda la normativa de seguridad de desarrollo estará a disposición de todos los miembros de la entidad que necesiten conocerla, especialmente para aquellas personas que utilicen, operen o administren los sistemas de información y comunicaciones. Vicomtech se esforzará en distinguir claramente entre lo que es la política abstracta y su aplicación concreta para mantener la flexibilidad ante el cambio tecnológico y la uniformidad de resultados.

8. Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos.

La gestión de riesgos debe contemplar también los derivados de la normativa de Protección de Datos, contando con la opinión y asesoramiento de la Persona Delegada de Protección de Datos, además se coordinarán los planes del tratamiento del riesgo.

La revisión del análisis de riesgos se realizará con la siguiente periodicidad:

- Al menos una vez al año, que será aprobado por acta en el Comité de seguridad de la Información
- Cuando se produzcan cambios significativos en la información y/o en los servicios prestados.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

El Comité de Seguridad de la Información será el órgano central encargado de **estandarizar la medición del riesgo** y de **asegurar los recursos** para abordar la seguridad de forma global y eficiente en toda la entidad.

9. Clasificación de la Información

La información documentada será clasificada en: pública, interna, restringida, confidencial y clasificada, dando el uso adecuado de acuerdo con dicha clasificación.

- **Información Pública**: Es aquel tipo de información cuya finalidad es la transmisión de cualquier medio a terceras partes como parte de los procesos de negocio, la cual, si se revelase no tendría consecuencias para la organización.

- **Uso Interno**: Es aquel tipo de Información a la que sólo debe tener acceso el personal de VICOMTECH, es decir, no está permitida su circulación pública fuera de la organización. Su revelación no controlada y/o perdida, podría ser un inconveniente para la gestión, aunque no supondría una pérdida económica o un daño de imagen.
- **Información Restringida**: Información sensible, interna de áreas o proyectos a los que sólo debe tener acceso controlado un departamento, participantes del proyecto, un comité, etc. pero no toda la empresa. La divulgación o uso de información restringida por personal no autorizado podría ocasionar pérdidas leves.
- **Información Confidencial**: Información sensible que exclusivamente puede ser conocida y utilizada por un grupo reducido y autorizado de personas para desempeñar sus funciones. La divulgación de información confidencial a personas sin autorización podría ocasionar graves pérdidas, tanto materiales como de imagen o responsabilidades legales a la Organización. Incluye información con datos personales.
- **Información Clasificada**. Afecta a información que puede afectar a la seguridad nacional. Sólo los estados u organizaciones supranacionales pueden determinar que una información queda clasificada y en qué grado. En el caso de Vicomtech afecta a un porcentaje muy bajo de casos por lo que el detalle del protocolo a seguir en estos casos se trata bajo la coordinación del Oficial de Seguridad de Vicomtech. Todo líder o persona miembro de proyecto (incluso en fase de elaboración de propuesta) en el que se sepa, se crea, o se tenga duda de que se pueda estar manejando información que es clasificada debe ponerse en contacto con éste.

10. Datos de carácter personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Vicomtech solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de las normativas de Protección de Datos.

11. Gestión de Incidentes de Seguridad

Para garantizar la continuidad de los servicios y actuar con presteza ante las amenazas, Vicomtech se compromete a disponer de un procedimiento formal y documentado para la gestión ágil de los

eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios:

- Este procedimiento garantizará la detección, contención, mitigación y resolución de los incidentes.
- Se adoptarán las medidas necesarias para que los incidentes detectados no vuelvan a reproducirse.
- Los diferentes departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

11.1. Responsabilidades y Coordinación Interna

La Gestión de Incidentes de Seguridad es una responsabilidad compartida:

1. **Responsable de Seguridad de la Información** (RSI): La persona RSI tiene la función de gestionar los incidentes de seguridad desde su notificación hasta su resolución. Además, debe emitir informes periódicos sobre los incidentes más relevantes al Comité de Seguridad de la Información.
2. **Comité de Seguridad de la Información**: El Comité debe monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones. En particular, el Comité velará por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de la información.
3. **Personal de Vicomtech**: Todo el personal de la organización tiene la obligación de usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.
4. **Técnico/a de Gestión Integral y Administrador/a de Seguridad**: Ambas figuras colaborarán en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

11.2. Integración y Terceras Partes

El procedimiento de gestión de incidentes de Vicomtech se integrará con los requisitos derivados de otras normas sectoriales, como la de protección de datos personales, con el fin de coordinar la respuesta desde los diferentes enfoques.

En el caso de incidentes que involucren a Terceras Partes, Prestadores de Servicios o Proveedores de Soluciones:

- Se establecerán procedimientos específicos de reporte y resolución de incidencias con terceros.

- Estos incidentes deberán ser canalizados obligatoriamente a través del Punto de Contacto (POC) de los terceros implicados.
- Si el incidente afecta a datos personales, la comunicación deberá canalizarse también a través de la Persona Delegada de Protección de Datos (DPD).

Cuando sea necesario, el Comité de Seguridad de la Información coordinará la respuesta y la comunicación para asegurar que se informa a los diferentes organismos de control sin dilaciones indebidas. También se comunicará a las Fuerzas y Cuerpos de Seguridad del Estado o a los juzgados cuando sea preciso.

12. Concienciación y formación

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso de seguridad y a sus responsables jerárquicos, para que, ni la falta de conocimiento, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad de los sistemas de información.

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos de seguridad establecidos.

El personal de Vicomtech recibirá la formación e información específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios que se prestan.

Se establecerá un programa de concienciación continúa dirigido a todo el personal de Vicomtech, en particular a las nuevas incorporaciones.

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: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

13. Terceras Partes / Prestadores de Servicios / Proveedores de Soluciones

Esta sección establece las directrices de seguridad para garantizar que la información y los servicios gestionados por Vicomtech se protejan cuando se involucren terceros, de conformidad con el Real Decreto 311/2022.

13.1. Vicomtech como Prestador de Servicios

Cuando Vicomtech preste servicios a otras entidades o maneje información de otras entidades, se les hará partícipes de esta Política de Seguridad de la Información:

- Se respetarán las obligaciones derivadas de la normativa de protección de datos si Vicomtech actúa como encargado del tratamiento en la prestación de dichos servicios.
- Se establecerán canales específicos para el reporte y la coordinación con los Comités de Seguridad respectivos.
- Se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
- La Persona Responsable de Seguridad de la Información de Vicomtech (a través de incidentes@vicomtech.org) será identificado como el Punto de Contacto (POC) para estas comunicaciones.

13.2. Vicomtech como Cliente de Servicios o Adquisición de Soluciones

Cuando Vicomtech utilice servicios de terceros, ceda información a terceros o adquiera productos y soluciones, estos quedarán sujetos a las obligaciones establecidas en esta Política de Seguridad y en la Normativa de Seguridad que les ataña.

- **Cumplimiento Contractual**: En la contratación de prestadores de servicios o adquisición de productos, se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS
- **Servicios en la Nube:** En la adquisición de derechos de uso de activos en la nube, la entidad tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II del ENS y las Guías de desarrollo correspondientes, el análisis de riesgos, así como el correspondiente análisis de la responsabilidad compartida.
- **Supervisión y Auditoría**: La tercera parte, aunque desarrolle sus propios procedimientos operativos para cumplir con la normativa, quedará sujeta a las obligaciones que permitan a Vicomtech supervisarlos o solicitar evidencias de cumplimiento. Esto incluye la posibilidad de solicitar auditorías de segunda o tercera parte.
- Concienciación: 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 o el que específicamente se pueda exigir en el contrato.

13.3. Gestión de Incidentes con Terceros

Se establecerán procedimientos específicos de reporte y resolución de incidentes con terceros. Estos procedimientos deberán ser canalizados obligatoriamente a través de:

1. El POC (Punto de Contacto) de los terceros implicados
2. La persona Delegada de Protección de Datos (DPO), si el incidente afecta a datos personales.

13.4. Aceptación de Riesgos por Incumplimiento del Tercero

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero (prestador de servicios o proveedor de soluciones), se seguirá un procedimiento formal para la asunción de riesgos:

1. El/la Responsable de la Seguridad emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos
2. Se requerirá la aprobación de este informe por las personas responsables de la información y los servicios afectados.
3. El informe se trasladará al Comité de Seguridad de la Información, quien deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo formalmente los riesgos detectados

13.5. Adquisición y Despliegue de Sistemas de Inteligencia Artificial (IA)

Cuando Vicomtech adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con la normativa vigente (incluyendo el Reglamento (UE) 2024/1689), este proceso deberá contar con:

- En el caso de la adquisición, deberá ajustarse a lo especificado por el Comité de Dirección con respecto a las directrices de Software Empleable dentro del Sistema de Gestión Integral. El/la Delegado/a de Protección de Datos deberá emitir su parecer.
- En el caso, del desarrollo e implantación, , deberá ajustarse a lo especificado por el Comité de Dirección con respecto a las directrices de Desarrollo de Software dentro del Sistema de Gestión Integral.

14. Obligaciones del personal

Todo el personal de la organización y/o partes interesadas que realicen servicios de cualquier clase contratados por Vicomtech o que de alguna manera se presten bajo el control y/o Dirección de Vicomtech tiene la obligación de conocer y cumplir esta **Política de Seguridad de la Información** y la **Normativa de Seguridad** de la Información documentada en el Sistema Integrado de Gestión.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a

tal efecto, en caso de detectar un posible incidente.

En Donostia, a 27 de noviembre de 2025

Fdo. Dirección General

72429210W JULIAN FLOREZ (R: G75051912)

Digitally signed by 72429210W JULIAN FLOREZ (R: G75051912)
Date: 2025.11.27 15:53:55 +01'00'

Fecha	Descripción	Autores	Revisión	Versión
28/03/2025	Creación de la Política de Seguridad de Vicomtech	Comité de Seguridad de la Información	-	1
27/11/2025	Adaptación a la nueva Guía de junio de 2025	Comité de Seguridad de la Información	-	2