POLÍTICA DE SEGURIDAD DE LA INFORMACION ISO 27001 + ENS

La presente política tiene por objeto establecer el marco de trabajo que permita identificar e implantar las medidas técnicas y organizativas para garantizar la seguridad de la información y la continuidad de los servicios de HISPAVISTA. Para ello, HISPAVISTA aplica las medidas de seguridad establecidas por el Esquema Nacional de Seguridad (ENS), estándar establecido por el Gobierno de España como adecuado para las Administraciones Públicas y las empresas privadas que prestan servicios a las mismas.

HISPAVISTA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para ofrecer sus servicios y cumplir sus objetivos. Estos sistemas deben protegerse garantizando la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de la información y los servicios prestados. La seguridad de la información es un factor crítico para asegurar la calidad y continuidad 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 la información y los servicios. Para defenderse de estas amenazas, el personal de HISPAVISTA debe aplicar los siguientes principios básicos:

- Seguridad como proceso integral
- Gestión de la seguridad basada en riesgos
- Prevención, detección, respuesta y conservación
- Existencia de líneas de defensa
- Vigilancia continua
- Reevaluación periódica
- Diferenciación de responsabilidades

Reflejados en los siguientes requisitos mínimos de seguridad exigidas por el ENS:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.

- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Para asegurarse debe realizarse un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

HISPAVISTA se compromete a que la seguridad TIC sea una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, incluyendo las decisiones de desarrollo o adquisición y las actividades de explotación.

1. ALCANCE

Esta política se aplica a todos los sistemas TIC y a todo el personal de HISPAVISTA sin excepciones. La seguridad de la información está en la mano de todos, es un trabajo en equipo.

2. MISIÓN/OBJETIVOS DE HISPAVISTA

La MISIÓN de HISPAVISTA es hacer crecer los negocios de nuestros clientes y solucionar sus retos digitales a través de soluciones tecnológicas innovadoras, acompañándolos en el camino con nuestra experiencia, dedicación y esfuerzo, desde la cercanía, la honestidad y la orientación a resultados.

Relacionado con esto la VISIÓN de HISPAVISTA es la de ser una empresa pionera y de referencia en iniciativas tecnológicamente disruptivas que supongan un beneficio sustancial en los servicios que prestamos a nuestros clientes/usuarios para conseguir su máxima satisfacción y fidelidad, desde la cercanía, el esfuerzo, la honestidad y la orientación a resultados.

3. MARCO NORMATIVO

HISPAVISTA tiene la obligación de cumplir con las leyes y normas aplicables a su naturaleza y actividad, así como con aquellas obligaciones contraídas con terceros. Para garantizar el cumplimiento normativo, HISPAVISTA dispone de un registro en el que se realiza un seguimiento de los requisitos aplicables, con especial atención a los relacionados con:

- Con la protección de datos de carácter personal
    - RGPD, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016
    - LOPDGDD, Ley Orgánica 3/2018, de 5 de diciembre
- Con la protección intelectual, Ley 2/2019, de 1 de marzo

- Con la seguridad de la información (ENS), Real Decreto 311/2022, de 3 de mayo

Este registro se revisa anualmente por el Comité de Seguridad para asegurar que está actualizado y refleja las normativas vigentes y aplicables. La revisión incluye la incorporación de nuevas leyes y regulaciones, así como la actualización de las existentes para garantizar un cumplimiento continuo y efectivo.

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1. Comité de seguridad de la información

El Comité de seguridad de la información será el encargado de coordinar la seguridad de la información en HISPAVISTA y reportará a la organización. Estará formado por los siguientes responsables:

- Responsable de la información y servicio
- Responsable de la seguridad
- Responsable del sistema
- Delegado de protección de datos
- Administrados del sistema

Las funciones del Comité de seguridad de la información son:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas 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 la organización. En particular velará por la coordinación de distintos 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 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 y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir
- Promover la vigilancia continua del sistema con el objetivo de detectar actividades o comportamientos anómalos, así como garantizar una respuesta acorde.
- Promover la evaluación permanente del estado de la seguridad de los activos con el objetivo de medir su evolución, detectar vulnerabilidades e identificar deficiencias de configuración.

4.2. Funciones y responsabilidades

HISPAVISTA define las siguientes responsabilidades para cada rol designado:

4.2.1. Responsable de la información (Rol de especificación):

- Determina los requisitos de seguridad de la información tratada
- Valora las consecuencias de un impacto negativo sobre la seguridad de la información. Se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Propietario de los riesgos de la información. Encargado de aceptar riesgos residuales de la información. Encargado de monitorizar estos riesgos (puede delegar el día a día).

4.2.2. Responsable del servicio (Rol de especificación):

- Determina los requisitos (de seguridad) de los servicios prestados
- Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios. Se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- Propietario de los riesgos de los servicios. Encargado de aceptar riesgos residuales de los servicios. Encargado de monitorizar estos riesgos (puede delegar el día a día).

4.2.3. Responsable de la seguridad (Rol de supervisión):

- Es el Secretario/a del Comité de Seguridad de la Información
    - Convoca las reuniones del Comité de Seguridad de la Información.
    - Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.

    - Elabora el acta de las reuniones.
    - Es responsable de la ejecución directa o delegada de las decisiones del Comité
- Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios
- Supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- Es jerárquicamente independiente del Responsable del Sistema
- En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.
- Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.
- Firma la relación de medidas seleccionadas del Anexo II formalizada en un documento denominado Declaración de Aplicabilidad.
- Aprueba formalmente el reemplazo de las medidas de seguridad referenciadas en el Anexo II por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan.
- Analiza los informes de autoevaluación y/o los informes de auditoría que eleva las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas
- Proponer indicadores para el seguimiento de riesgos y definirlos junto a sus propietarios.

4.2.4. Responsable del sistema (Rol de operación):

- Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros), cuando los sistemas de información se encuentran externalizados.
- Analiza los informes de autoevaluación y/o los informes de auditoría que eleva las conclusiones al Responsable del Sistema para que adopte las medidas correctoras

adecuadas.

- En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

4.2.5. Delegado de protección de datos (Rol de supervisión):

- Informa y asesora al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisa el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrece el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisa su aplicación de conformidad con el artículo 35.
- Coopera con la autoridad de control.
- Actúa como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realiza consultas, en su caso, sobre cualquier otro asunto.

4.3. Procedimiento de designación

Es función de la Dirección de la entidad designar:

- Al Responsable de la Información
- Al Responsable del Servicio, que puede ser el mismo que el Responsable de la Información
- Al Responsable de la Seguridad, que debe reportar directamente a la Dirección
- Al Responsable del Sistema, escuchando la opinión de los responsables de las informaciones y los servicios afectados. En materia de seguridad reportará al Responsable de la Seguridad. Puede estar compartimentado entre una responsabilidad mediata (dentro de la organización) y una responsabilidad inmediata (tercero, para sistemas externalizados).

El nombramiento se revisará cada año o cuando el puesto quede vacante.

4.4. Resolución de conflictos

HISPAVISTA establece un mecanismo claro y definido para la resolución de conflictos relacionados con la seguridad de la información. Este mecanismo incluye los siguientes pasos:

- **Identificación del conflicto:** cualquier conflicto relacionado con la seguridad de la información debe ser reportado inmediatamente al Responsable de Seguridad de la Información.
- **Evaluación inicial:** el Responsable de Seguridad de la Información evaluará el conflicto para determinar su naturaleza, impacto y urgencia. Esto incluye la recopilación de información relevante y la consulta con las partes implicadas.
- **Mediación interna:** se convocará una reunión con todas las partes involucradas, incluyendo el Comité de seguridad de la información, para intentar resolver el conflicto mediante mediación. En esta fase se buscan soluciones que satisfagan a todas las partes implicadas.
- **Decisión del Comité de seguridad de la información:** si la mediación interna no resuelve el conflicto, el Comité de Seguridad de la información tomará una decisión final basándose en los principios y políticas de HISPAVISTA, así como en las leyes y normativas aplicables.
- **Documentación y comunicación:** Todas las decisiones y acciones tomadas durante el proceso de resolución de conflictos serán documentadas y comunicadas a las partes implicadas. Esta documentación se mantendrá como registro para futuras referencias.
- **Seguimiento y Revisión:** Tras la resolución del conflicto, se llevará a cabo un seguimiento para asegurar que las soluciones implementadas son efectivas y sostenibles. El Comité de seguridad de la información revisará el caso para identificar posibles mejoras en los procesos y políticas de seguridad.

4.5. Documentación

La documentación sobre la que se soporta esta política estará compuesta por un conjunto de normas, guías y procedimientos que ayudarán a las personas usuarias en el desarrollo de sus tareas.

Esta documentación está disponible en TEAM en el equipo de Teams Hispavista SGSI

Toda esta documentación debe contar con una cabecera que incluya:

- Logo
- Código y título de la política
- Número de revisión
- Fecha de la revisión (y, por lo tanto, fecha en la que comienza su aplicación)
- Categoría de la información: pública, interna, restringida, confidencial
- Número de hoja de total de hojas

Además, debe contar con un espacio al inicio con el detalle y fecha de las revisiones y debe estar aprobada y firmada por el Comité de Seguridad de la Información.

4.6. Datos de carácter personal

HISPAVISTA trata datos de carácter personal de trabajadores y clientela. Para garantizar la adecuada protección de estos datos, existe el Documento de Seguridad que refleja la postura

de HISPAVISTA respecto de estos. Este documento detalla las medidas y procedimientos específicos adoptados para asegurar la protección y el tratamiento adecuado de los datos personales de salud, cumpliendo con las normativas vigentes en materia de protección de datos.

Todos los sistemas de información que traten datos de carácter personal en HISPAVISTA se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal y la finalidad especificada en el Documento de Seguridad.

5. CONCIENCIACIÓN Y FORMACIÓN

HISPAVISTA, siguiendo el principio de Seguridad Integral del ENS tiene como objetivo que el personal tenga una plena conciencia de la seguridad de la información en todas las actividades que realizan.

Por ello, HISPAVISTA se compromete a disponer los medios necesarios para asegurar que todas las personas que intervienen en los procesos y sus responsables, desarrollen una sensibilidad y comprensión adecuadas hacia los riesgos asociados a la seguridad de la información y la disponibilidad de los servicios.

Para alcanzar este objetivo, HISPAVISTA implementará las siguientes acciones:

- Programas de concienciación:
    - Realización de sesiones de concienciación obligatorias para todo el personal al menos una vez al año.
    - Programas continuos de concienciación para mantener a todos los miembros de la organización actualizados sobre los riesgos y mejores prácticas en seguridad de la información.
- Formación continua:
    - Formación específica para el personal con responsabilidades en el uso, operación o administración de los sistemas TIC, asegurando que reciban la capacitación necesaria antes de asumir sus responsabilidades.
    - Actualización periódica de la formación para reflejar los cambios en las amenazas y las mejores prácticas en seguridad.

6. GESTIÓN DE RIESGOS

El Comité de Seguridad de la Información realizará un análisis de riesgos de los sistemas de información, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis 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, o cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de seguridad de la información establecerá una valoración de referencia para los diferentes tipos de información manejados y

los diferentes servicios prestados. También se encargará de poner a los recursos necesarios para atender a las necesidades de seguridad de los diferentes sistemas.

7. APROBACIÓN Y ENTRADA EN VIGOR

Esta política de seguridad es aprobada el 30/07/2025 por el Comité de Seguridad de la información de Hispavista. Es efectiva desde dicha fecha y permanecerá vigente hasta su reemplazo por una nueva política. Se revisará anualmente y se actualizará si es necesario, indicándolo en el cuadro de revisiones (Punto 1 de esta política).

GERENCIA