PROCEDIMIENTO GENERAL PG 24

Política de Seguridad de la Información

Elaborado por: Responsable de Seguridad de la Información

Revisado por: Dirección

ÍNDICE

1. Objeto

Establecer los principios, responsabilidades y medidas clave para garantizar la confidencialidad, integridad y disponibilidad de la información utilizada en HMS INTELLIGENCE en el desempeño de sus actividades estratégicas y operativas.

2. Introducción

El equipo directivo y todo el personal de HMS INTELLIGENCE asumen el compromiso de garantizar la seguridad de la información y de las redes y los Sistemas de Información en los que se apoyan los diferentes procesos de negocio, con el fin de reforzar su Resiliencia Operativa Digital, alineando sus prácticas con la normativa vigente aplicable, así como con sus valores corporativos.

La información es uno de los activos más valiosos de HMS INTELLIGENCE. Su adecuada protección resulta esencial para garantizar la confianza de nuestros clientes, el cumplimiento normativo y la continuidad del negocio. Esta política establece el marco estratégico y operativo para la gestión segura de la información conforme a las mejores prácticas internacionales y los requisitos de las normas ISO 27001.

El análisis y gestión de riesgos permanentemente actualizados son una parte esencial del proceso de seguridad, que requerirá la implantación de un conjunto adecuado de controles, ya sean políticas, prácticas, procedimientos, o estructuras organizativas, que aseguren que los sistemas de información no incurren en riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos

e informaciones en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

• Los servicios deben estructurarse con diferentes líneas de defensa, constituidas por medidas de naturaleza organizativa, física y lógica, de modo que una amenaza que se materialice no pueda desarrollar todo su potencial y se mitigue, rápidamente, el daño producido.

• Las medidas de seguridad se evaluarán y actualizarán periódicamente

• Segregación de roles para asegurar la calidad y evitar posibles conflictos de intereses, asegurando la consistencia de la seguridad, mediante actuaciones coordinadas entre todos los actores implicados.

3. Definiciones

Para poder acometer con éxito los objetivos de seguridad se deben definir y asignar responsabilidades y competencias en seguridad de la información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

La seguridad: se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los servicios prestados. Por lo tanto, se excluye cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Gestión de Incidentes: conjunto de medidas y procedimientos destinados a prevenir, detectar, analizar y delimitar un Incidente, resolviéndose e incorporando medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Incidente de Ciberseguridad o Ciberincidente: suceso inesperado o no deseado que pueda comprometer la disponibilidad, autenticidad, trazabilidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por Sistemas de Redes y de Información o accesibles a través de ellos.

Información: activo principal de cualquier empresa que puede estar en formato físico, o digital y pueden estar determinados en ficheros de todo tipo (texto, imagen, multimedia, bases de datos…), pasando por los programas y aplicaciones que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.

Profesional: los miembros de los órganos de administración, directivos, trabajadores, colaboradores, estudiantes en prácticas y becarios, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios, su nivel jerárquico, su ubicación geográfica o funcional y de la sociedad del Grupo HMS para la que presten sus servicios.

Principio de autenticidad: persigue garantizar que el origen y las identidades asociadas a la información son realmente los que aparecen en los atributos de esta. Este principio va unido al de no repudio, que consiste en asegurar que un Usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos.

Principio de confidencialidad: procura que la información solo sea accesible para los Usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.

Principio de disponibilidad: consiste en que la información esté accesible y se pueda utilizar de forma constante, asegurando la continuidad de los procesos y de la actividad. Este principio va unido al de resiliencia, que consiste en asegurar la capacidad de recuperación de los sistemas y la información tras un incidente que impida el acceso temporal a los mismos.

Principio de integridad: pretende asegurar que los datos se mantendrán libres de modificaciones no autorizadas y que la información existente no ha sido alterada por personas o procesos no autorizados.

Principio de trazabilidad: busca la posibilidad de determinar en cada momento la identidad de las personas que acceden a la información y la actividad que desarrollan en relación con la misma, así como los distintos estados y rutas que ha seguido la información.

Resiliencia Operativa Digital: la capacidad de la entidad para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los Sistemas de Información que utiliza la entidad y que sustentan la prestación continuada de servicios y su calidad, incluso en caso de perturbaciones.

Riesgo: la posible pérdida o perturbación causada por un Incidente expresada como una combinación de la magnitud de tal pérdida o perturbación y la probabilidad de que se produzca tal Incidente

Sistema de Gestión de Seguridad de la Información ("SGSI"): conjunto de políticas y procedimientos de seguridad de la información que tratan de componer un sistema de organización y gestión, diseñado para implantar, mantener y mejorar dichas políticas. El SGSI trata de asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los Riesgos de

seguridad de la Información teniendo en cuenta los Riesgos analizados dentro de los procesos de negocio de HMS, y cuya base es la presente Política

Sistema de Información: un conjunto discreto de recursos de información que soportan aplicaciones o servicios de negocio, los cuales se organizan para obtener, procesar, mantener, utilizar, compartir, distribuir o disponer de la información.

Tratamiento de datos: cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, o conjuntos de éstos, ya sea por procesos automatizados o no, como la recogida, 5 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.

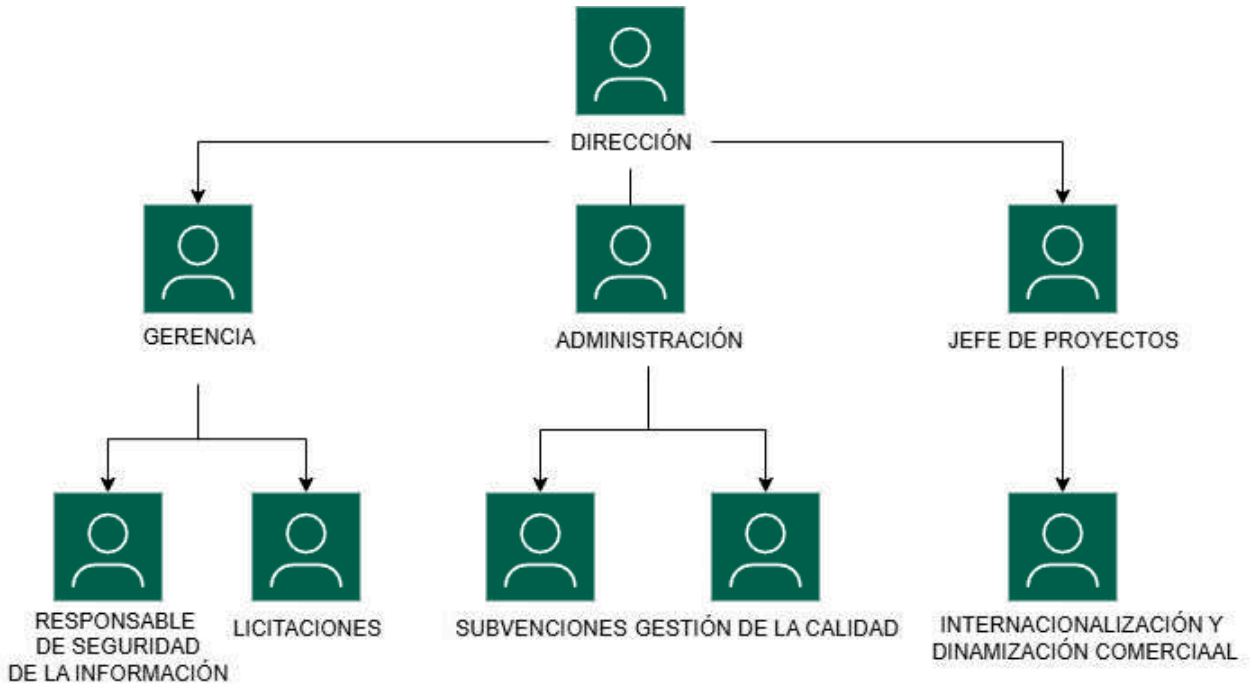
Usuario: Cualquier persona vinculada a HMS por una relación civil o mercantil, así como clientes, proveedores, subcontratistas, consultores o cualesquiera otras personas o entidades a los que se autorice a tener acceso a los datos.

Vulnerabilidad: cualquier debilidad, susceptibilidad o defecto de un activo, sistema, proceso o control que puede ser explotado.

4. Estructura empresarial

En HMS intelligence existe una estructura jerárquica operacional que separa en departamentos las diferentes actividades empresariales.

Para ello principalmente presentamos el organigrama estructural de la empresa:



5. Alcance

Esta política es de aplicación obligatoria a:

- Todo el personal de HMS INTELLIGENCE.

- Colaboradores externos, consultores, subcontratas y terceros con acceso autorizado a información, datos o sistemas de la organización.

- Todos los sistemas informáticos, aplicativos, entornos en la nube (p. ej., Zoho,) y soportes de almacenamiento utilizados.

6. Marco normativo

La presente política se alinea con los siguientes marcos y referencias:

- ISO/IEC 27001:2022

- Sistema de Gestión de Seguridad de la Información (SGSI)

- Ley Orgánica 3/2018 (LOPDGDD) y Reglamento (UE) 2016/679 (RGPD).

- ISO 9001:2015 e ISO 14001:2015.

- Contratos con cláusulas de confidencialidad

7. Responsabilidades

- Dirección y Gerencia: Aprobar, respaldar y promover la Política de Seguridad de la Información, asegurando los recursos necesarios.

- Responsable de la Seguridad de la información del SIG: Liderar la implementación, supervisión y mejora del SGSI, así como coordinar auditorías y revisiones.

- Usuarios y empleados: Cumplir con las directrices, salvaguardar la información en su día a día y reportar cualquier incidente o debilidad en la seguridad.

8. Directrices operativas

a) Control de acceso- Implementación de controles de acceso lógicos basados en roles.- Autenticación individual obligatoria, contraseñas robustas y uso de doble factor (2FA).- Bitwarden como gestor oficial de contraseñas.

b) Clasificación y tratamiento de la información

- Toda la información será clasificada como Pública, Interna o Confidencial.

- Información clasificada como Confidencial será cifrada y almacenada en entornos seguros.

- Queda prohibido compartir información sensible por canales no autorizados.

9. Gestión de proyectos

- **Objetivo**

Establecer las directrices y controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información durante todas las fases de gestión de proyectos, conforme a los requisitos del SGSI.

Este protocolo es aplicable a todos los proyectos gestionados por la organización, incluyendo proyectos internos, con clientes o con terceros, que impliquen el tratamiento o acceso a información sensible o crítica.

- **Responsables y Responsabilidades**

El jefe de proyecto deberá aplicar las medidas de seguridad durante todo el ciclo de vida del proyecto y asegurarse que los usuarios participantes del mismo también lo cumplan.

El Responsable de Seguridad de la Información deberá estar disponible para cualquier asesoramiento durante el proyecto y para recibir la comunicación de algún incidente.

- **Fases del protocolo y medidas asociadas**

- Evaluación del impacto sobre la seguridad
- Clasificación de la información que será tratada
- Determinar si el proyecto requiere tratamiento de datos personales o información clasificada.
- Designar un jefe de proyecto con formación en seguridad.
- Aplicación de control de acceso basado en roles

Planificación

- Análisis de riesgos específicos del proyecto
- Establecer requisitos de seguridad en contratos con terceros si aplica

Ejecución

- Aplicación de controles técnicos: cifrado, control de accesos, backups
- Verificación de cumplimiento de políticas de seguridad en cada entrega.
- Monitorización continua de incidentes y vulnerabilidades.
- Evitar uso de dispositivos no autorizados o redes no seguras.
-

Seguimiento y control

- Revisión periódica de controles y medidas de seguridad
- Auditorías internas del cumplimiento del SGSI en el proyecto.

Cierre del proyecto

- Asegurar la eliminación o retorno de la información a clientes/terceros
- Evaluación final de la conformidad con los requisitos de seguridad.

Gestión documental

- Toda la documentación generada será almacenada y protegida según los niveles de clasificación definidos.
- Aplicación de controles de acceso, trazabilidad y cifrado en la documentación sensible.
- El protocolo será revisado anualmente o tras cualquier incidente relevante, y actualizado para incorporar nuevas amenazas, requisitos regulatorios o mejoras identificadas.

Para más información referente a la Política de Seguridad de la información de HMS existen unos documentos internos donde se aclaran los diferentes puntos del alcance de la declaración de aplicabilidad de la normativa ISO 27001

Protocolo	Nombre del Archivo	Anexos de Control
Copias de Seguridad	250717.ProtocoloCopiadeSeguridad Doc	A.8.7
Concienciación y formación	250721.ProtocoloConcienciacionFormacionDoc	A.6.3
Contratación	250721.Protocolo Contratación	A.5.31-A.5.32-A.5.34-A.6.1-A6.2-A.6.5-A.6.6-A.6.7-a.7.4
Control de Acceso	250721ProtocoloControl Acceso.Formato Doc	A.5.15
Mantenimiento de equipos	250722.ProtocolodeMantenimiento	A.5.10-A.5.11
Soportes de almacenamiento	250722.ProtocolodeSoportesAlmacenamiento	A.7.10
Autenticación	250717.ProcesodeAutenticación Doc	A.5.17
Seguridad Física	250717.ProtocoloSeguridadFisica Doc	A.7.1-A.7.2-A.7.3
Gestión de evidencias	250721.GestionEvidenciasDoc	A-5-28
Brechas	250721.ProtocoloBrechas Seguridad	A.5.24-A.5.24-A.5.26-A.27
Etiquetado y Clasificación	250721.ProtocoloEtiquetadoClasificacionInformacion	A.5.12-A.5.13
Gestión de equipos	250721.ProtocoloGestion Equipos	A.5.10-A.5.11
Contacto Autoridades	250722.ProtocoloContactoAutoridades	A.5.5
Gestión del cambio	250722.ProtocoloGestion Cambio	A.8.32
Vulnerabilidades	250722.ProtocoloVulnerabilidades	A.8.8