

Política de Seguridad de la Información

Proyecto de portafolio

Jon Sanmillán Fuica

Este proyecto recoge la revisión y ampliación de una Política de Seguridad de la Información desarrollada en el contexto del TFM del Máster en Derecho Digital, IA y Blockchain de EBIS. La adaptación parte de DRIVE TECH, una empresa tecnológica ficticia, y de su documentación empresarial. Mi objetivo ha sido obtener una política verosímil para su actividad, con un alcance concreto, responsabilidades coherentes y reglas de seguridad que puedan orientar a las áreas que tendrían que aplicarlas.

14 capítulos en la PSI	10 bloques de responsabilidades	15 páginas de la política
----------------------------------	---	-------------------------------------

La Política de Seguridad de la Información, o PSI, establece los principios, las responsabilidades y las reglas generales para proteger la información de una organización. Comprende los datos personales y también otros activos, como el código fuente, los diseños de producto, las credenciales o la documentación comercial. Su utilidad está en fijar criterios comunes sobre quién decide, qué debe protegerse y cómo deben gestionarse los riesgos y las incidencias.

La política sirve de base para normas y procedimientos más concretos. Por ejemplo, puede exigir la autorización y revisión de los accesos; el procedimiento debe concretar cómo se solicitan, quién los concede y qué registro queda. En materia de datos personales, los artículos 24 y 32 del [RGPD](#) relacionan las medidas organizativas y técnicas con los riesgos del tratamiento. Disponer de una PSI no demuestra, por sí solo, que esas medidas se estén aplicando.

¿Qué ha sido necesario examinar?

La empresa y los activos que necesita proteger

La documentación del caso describe relojes y gafas inteligentes, un dispositivo con IA, una plataforma de gestión y servicios de ingeniería. Esa actividad obliga a considerar tanto la información corporativa como los productos y servicios utilizados por clientes. La revisión ha relacionado cada ámbito con riesgos concretos, como accesos indebidos, alteración del software, exposición de datos o interrupción del servicio.

La descripción comercial de un producto no permite conocer toda su arquitectura ni los datos que efectivamente trata. Por eso, el alcance y las medidas se han formulado sin dar por contratados proveedores, implantadas herramientas o acreditados flujos que no constan en las fuentes. Los inventarios y procedimientos previstos tendrían que concretar esas dependencias.

Las normas y las condiciones de aplicación

El análisis ha requerido distinguir obligaciones legales, compromisos contractuales y estándares voluntarios. El [ENS](#), por ejemplo, tiene un ámbito de aplicación que debe comprobarse antes de exigirlo a una empresa privada. Las normas [ISO/IEC 27001](#) y 27002 pueden orientar la gestión y los controles, sin que su mención acredite una certificación.

Para dispositivos conectados e IA se han considerado el Reglamento de Datos, el Reglamento de IA y el [Reglamento de Ciberresiliencia](#), atendiendo a los productos, el rol de la empresa y los calendarios de cada obligación. También se ha diferenciado la gestión de un incidente de seguridad de la valoración jurídica de una brecha de datos personales. No todos los incidentes activan las mismas comunicaciones ni los mismos plazos.

La coherencia entre la política y su aplicación

Cada obligación necesita una autoridad y una forma de desarrollarse. En los accesos, por ejemplo, se separan la autorización del responsable de negocio y la ejecución técnica de IT. En una actualización de producto, la revisión de seguridad y la autorización de la versión deben quedar relacionadas. Ante una excepción, la aceptación del riesgo debe corresponder a quien tenga competencia y quedar documentada.

La revisión documental ha comprobado la coherencia de esos repartos, la correspondencia del índice y la conservación del texto ajeno a los cambios autorizados. También se han inspeccionado las quince páginas de la PSI maquetada. Son comprobaciones del documento y de su diseño organizativo; la eficacia de las medidas requeriría pruebas sobre sistemas y actuaciones reales.

Qué pretendo demostrar con este proyecto

Con este proyecto pretendo mostrar cómo abordo la adaptación de una política corporativa a una actividad empresarial concreta. La PSI permite examinar el criterio empleado para delimitar el alcance, distribuir responsabilidades y relacionar las necesidades de seguridad con reglas comprensibles para Dirección, Legal, IT y los equipos de producto.

Mi interés está en la conexión entre el análisis jurídico y las decisiones de la organización. Exigir una revisión de accesos implica identificar quién la realiza y cómo se documentaría. Prever una respuesta a incidentes exige distinguir la contención técnica de las decisiones de negocio y de las obligaciones de comunicación. Esas relaciones permiten valorar el trabajo más allá de la enumeración de normas.

También busco mostrar criterio para tratar la información que falta. Una propuesta puede indicar qué debería existir y qué habría que comprobar sin presentar esas condiciones como ya cumplidas. Ese enfoque permite mantener visibles los límites del caso y orientar las siguientes actuaciones de un equipo.

Qué ha supuesto desarrollarlo

La adaptación ha exigido decidir qué conservar, qué reescribir y qué añadir. He orientado el trabajo hacia una PSI que pudiera resultar útil en una empresa como DRIVE TECH, tomando INCIBE como referencia y priorizando la corrección del alcance, del marco jurídico y del gobierno del documento. También he solicitado integrar la revisión en mejora continua y ajustar la política a quince páginas.

Una dificultad ha sido decidir cuánto detalle corresponde a la política general. Los contactos, configuraciones y frecuencias operativas necesitan procedimientos que puedan actualizarse sin rehacer toda la PSI. El resultado recoge esa relación y permite distinguir entre la obligación, su desarrollo y la evidencia que haría falta para comprobarla.

Alcance del resultado y uso de IA

La revisión, la redacción y las comprobaciones documentales se han realizado con apoyo de IA. Mi intervención se ha centrado en definir el objetivo, seleccionar las correcciones y orientar las decisiones de adaptación recogidas en esta memoria. Las conclusiones se apoyan en la documentación del caso y en las fuentes contrastadas durante el proyecto.

El resultado es una propuesta documental sobre una empresa ficticia. La aprobación empresarial y la entrada en vigor figuran pendientes; no acredita una implantación, una certificación de seguridad ni un ejercicio profesional de DPO o CISO. La autoría del texto original y de su adaptación corresponde a Jon Sanmillán Fuica. El enunciado y el presupuesto del caso proceden de EBIS y no se presentan como elaboración propia.