



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Drive TechSolutions S.L. · DRIVE TECH

Sistema de Gestión de Seguridad de la Información (SGSI)

Código / versión	PSI.01
Estado	Propuesta pendiente de aprobación
Clasificación	Uso interno de esta versión de trabajo
Responsable	Responsable de Seguridad de la Información (CISO)
Revisión	Comité de Seguridad de la Información · pendiente
Aprobación	Dirección General · pendiente
Fecha de edición	14 de septiembre de 2026
Aprobación / vigencia	Fechas pendientes de la decisión de Dirección General
Próxima revisión	Anual desde su entrada en vigor y ante cambios relevantes

ÍNDICE

1. INTRODUCCIÓN	3
2. OBJETIVO DE LA POLÍTICA DE LA INFORMACIÓN	3
3. ALCANCE Y APLICABILIDAD	4
4. MARCO JURÍDICO Y NORMATIVO	5
5. ROLES Y RESPONSABILIDADES	5
6. GESTIÓN DE RIESGOS Y ACTIVOS DE INFORMACIÓN	9
7. PROTECCIÓN DE LOS SISTEMAS Y DE LA OPERACIÓN	10
8. SEGURIDAD DEL DESARROLLO Y DE LOS PRODUCTOS CONECTADOS ..	11
9. PROTECCIÓN DE DATOS PERSONALES	12
10. GESTIÓN DE INCIDENTES DE SEGURIDAD	13
11. CONTINUIDAD Y RECUPERACIÓN	13
12. SEGURIDAD EN LAS RELACIONES CON TERCEROS	14
13. DESARROLLO Y APLICACIÓN DE LA POLÍTICA	15
14. MEJORA CONTINUA	16

1. INTRODUCCIÓN

Este documento expone la Política de Seguridad de la Información de Drive TechSolutions S.L., que opera bajo la denominación comercial DRIVE TECH, y tiene como objetivo establecer el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, con el fin de garantizar la protección de la información en todos los procesos de la compañía, conforme a los requisitos legales y contractuales aplicables y a los criterios de referencia definidos en el apartado 4.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de DRIVE TECH. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información constituye un pilar estratégico para DRIVE TECH, ya que la empresa desarrolla y ofrece soluciones tecnológicas innovadoras que requieren garantizar la confianza de clientes, empleados y socios.

Esta Política se establece con la finalidad de asegurar la calidad de la información y la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de DRIVE TECH.

La dirección de DRIVE TECH, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento. La entrada en vigor de la presente Política de Seguridad de la Información de DRIVE TECH sustituye cualquier otra que existiera a nivel de los diferentes departamentos o áreas de la organización.

2. OBJETIVO DE LA POLÍTICA DE LA INFORMACIÓN

El objetivo empresarial de DRIVE TECH es consolidarse como un referente en el desarrollo de soluciones tecnológicas innovadoras, competitivas y seguras, capaces de aportar valor añadido a sus clientes y de diferenciarse en un mercado altamente dinámico. Para alcanzar dicho objetivo estratégico, la confianza en la seguridad y fiabilidad de sus productos y servicios constituye un factor crítico de éxito.

La Política de Seguridad de la Información (PSI) de DRIVE TECH tiene como finalidad establecer un marco común que garantice la protección adecuada de la información y de los sistemas tecnológicos que la gestionan, asegurando que los activos más críticos de la compañía se encuentran protegidos frente a amenazas internas y externas.

DRIVE TECH tiene presente que la ciberseguridad 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. Los requisitos de seguridad, calidad y de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para todos los proyectos.

La aprobación de esta política manifiesta el interés y compromiso de DRIVE TECH en cumplir con los requisitos aplicables y de mejora continua en la gestión de la seguridad de la información y la calidad en la prestación de sus servicios. Con ella se establecen los objetivos y las responsabilidades necesarias para proteger los activos de información frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada, o a los servicios prestados.

En este contexto, la PSI contribuye directamente al objetivo corporativo al:

- Proporcionar un marco normativo y organizativo que asegure la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de la información.
- Reforzar la confianza de clientes, socios y empleados, garantizando que los servicios se prestan con los más altos estándares de seguridad.
- Integrar la gestión de riesgos tecnológicos en la estrategia de la empresa, facilitando una toma de decisiones alineada con la innovación y la resiliencia digital.
- Favorecer el cumplimiento normativo en materia de protección de datos y ciberseguridad, evitando sanciones, pérdidas económicas y daños reputacionales.

El objetivo último de la seguridad de la información es garantizar que una organización pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

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

3. ALCANCE Y APLICABILIDAD

Esta política comprende la información y los procesos de Drive TechSolutions S.L. vinculados al diseño, desarrollo, comercialización, mantenimiento y soporte de dispositivos conectados, software, plataformas digitales y soluciones de inteligencia artificial, así como a la gestión interna de la empresa. Abarca el ciclo de vida de los productos y servicios, desde su concepción hasta su retirada y la eliminación o devolución de la información.

Se aplica a toda la información gestionada por DRIVE TECH, propia o confiada por clientes y terceros, en formato digital, físico o verbal. Incluye los sistemas corporativos y de desarrollo, código fuente y firmware, repositorios, datos utilizados en soluciones de IA, servicios en la nube, interfaces de comunicación, dispositivos y accesos remotos, cuando formen parte de su actividad o se utilicen para prestarla.

Es obligatoria para la Dirección, el personal y quienes accedan a la información o a los recursos de la empresa. Los requisitos exigibles a proveedores y colaboradores se incorporarán a los contratos o acuerdos correspondientes. La externalización de una actividad no la excluye del alcance ni elimina la responsabilidad de supervisarla.

Respecto de los dispositivos comercializados, se extiende a las actividades y componentes bajo responsabilidad de DRIVE TECH y a la seguridad de su integración con los servicios asociados. Las condiciones de uso y obligaciones de los clientes se establecerán en la documentación y los contratos de producto. Los inventarios y registros de servicios concretarán este alcance y sus dependencias.

4. MARCO JURÍDICO Y NORMATIVO

DRIVE TECH cumplirá los requisitos legales y contractuales de seguridad que correspondan a sus actividades, productos, servicios y tratamientos de información. Su aplicabilidad se determinará por la actividad efectiva, el papel de la empresa y el ámbito territorial, atendiendo a las disposiciones transitorias y a las fechas de aplicación.

En el tratamiento de datos personales se aplicarán el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD). La prestación de servicios en línea, el comercio electrónico y las comunicaciones comerciales deberán cumplir la Ley 34/2002 (LSSI-CE) cuando se encuentren dentro de su ámbito.

Para los productos conectados, servicios relacionados y soluciones de IA se determinarán las obligaciones que correspondan conforme al Reglamento (UE) 2023/2854, de Datos; al Reglamento (UE) 2024/2847, de Ciberresiliencia; y al Reglamento (UE) 2024/1689, de Inteligencia Artificial. La evaluación tendrá en cuenta las funciones de cada producto, el rol de DRIVE TECH, las exclusiones y el calendario de exigibilidad de cada obligación.

El Esquema Nacional de Seguridad, regulado por el Real Decreto 311/2022, será exigible cuando concurren los supuestos de su ámbito de aplicación, incluidos los servicios al sector público que queden comprendidos en él. También se comprobará si la actividad y dimensión de DRIVE TECH determinan obligaciones específicas bajo la normativa nacional de seguridad de redes y sistemas y el régimen derivado de la Directiva (UE) 2022/2555 (NIS2). No se presumirá la sujeción a estos regímenes por el mero carácter tecnológico de la empresa.

Las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 se utilizarán como referencias voluntarias para organizar la gestión y seleccionar controles proporcionales al riesgo. Las guías de INCIBE y CCN-CERT podrán servir de apoyo técnico. Su utilización no acredita certificación ni conformidad integral; los compromisos contractuales que incorporen requisitos concretos deberán identificarse y cumplirse.

Legal mantendrá, con la colaboración del CISO y de los responsables de producto y servicio, un registro de requisitos aplicables y compromisos contractuales. Identificará su fundamento, alcance, responsables, obligaciones y fechas relevantes, y lo revisará ante cambios normativos o de actividad. El CISO coordinará su incorporación a los procedimientos y controles; las decisiones de no aplicabilidad deberán quedar justificadas.

5. ROLES Y RESPONSABILIDADES

La seguridad de la información se organizará de acuerdo con las funciones de dirección, negocio, desarrollo de producto, operación tecnológica y asesoramiento jurídico de DRIVE TECH. Las responsabilidades definidas en esta política deberán formalizarse mediante

designaciones y delegaciones documentadas, con indicación de su ámbito, autoridad, dependencia y suplencia.

Se diferenciarán la determinación de las necesidades del negocio, la supervisión de la seguridad y la operación de los sistemas. Cuando el tamaño de la organización requiera acumular funciones compatibles, la Dirección documentará esa decisión y establecerá una revisión independiente de las actuaciones que puedan generar conflicto de interés. Nadie podrá autorizar por sí mismo sus propios privilegios ni aceptar unilateralmente los riesgos derivados de su actuación técnica.

5.1. Alta Dirección

La Dirección General asumirá la responsabilidad última sobre la seguridad de la información y su integración en la estrategia, los productos y los servicios de DRIVE TECH. Aprobará esta política y sus modificaciones, dejando constancia de la versión, la decisión y la fecha de entrada en vigor. Le corresponderá establecer las prioridades de protección, dotar los recursos necesarios, formalizar las responsabilidades y resolver los riesgos o conflictos que excedan la autoridad de los responsables de área.

La Alta Dirección ejercerá estas funciones a través de la Dirección General (CEO), la Dirección Financiera (CFO), la Dirección de Operaciones (COO) y la Dirección Tecnológica (CTO), dentro de sus respectivos ámbitos. La Dirección Financiera incorporará las necesidades de seguridad a la planificación económica; Operaciones coordinará la continuidad de los procesos de negocio; y Tecnología asegurará que el desarrollo de producto y la operación tecnológica dispongan de medios para cumplir los requisitos de seguridad.

La Dirección General establecerá los criterios de aceptación de riesgos y las delegaciones para su aprobación. Los riesgos que superen esos criterios, afecten transversalmente a la organización o comprometan de forma relevante los productos o la continuidad deberán elevarse a su decisión expresa. La aceptación de un riesgo no podrá utilizarse para dispensar el cumplimiento de una obligación legal.

5.2. Comité de Seguridad de la Información

El Comité de Seguridad de la Información será el órgano de coordinación y seguimiento de esta política. Estará presidido por la Dirección General o su representante con delegación expresa e integrará a las direcciones Financiera, de Operaciones y Tecnológica, al Responsable de Seguridad de la Información y a la representación de Legal y Recursos Humanos. Se convocará a los responsables de producto, sistemas, servicios u otras áreas cuando los asuntos les afecten. El DPO, cuando esté designado, participará como asesor independiente en las cuestiones de protección de datos.

El Comité revisará la política y sus modificaciones y elevará su propuesta a la Dirección General para aprobación. Coordinará el plan de tratamiento de riesgos, propondrá prioridades y recursos, revisará incidentes y resultados de comprobaciones y realizará el seguimiento de las acciones pendientes. No sustituirá la responsabilidad ejecutiva de cada dirección ni aceptará riesgos reservados a la Dirección General.

La Dirección formalizará su composición, suplencias y reglas de funcionamiento. Se reunirá con la periodicidad que establezca ese acuerdo y, de forma extraordinaria, ante

incidentes graves o decisiones que requieran coordinación urgente. Sus acuerdos identificarán las decisiones, responsables de ejecución y plazos de seguimiento.

5.3. **Responsable de Seguridad de la Información (CISO)**

La función de Responsable de Seguridad de la Información, denominada también CISO, será única a efectos de esta política. Tendrá acceso directo a la Dirección General para informar sobre riesgos y discrepancias, con independencia de su adscripción administrativa. La Dirección asegurará que disponga de autoridad, recursos y acceso a la información necesarios para supervisar la seguridad.

Le corresponderá proponer los criterios de seguridad, coordinar el análisis de riesgos, revisar los requisitos de nuevos sistemas y productos y supervisar el tratamiento de vulnerabilidades y las medidas acordadas. Será responsable del mantenimiento y control de versiones de la política y coordinará su desarrollo documental, la concienciación, las verificaciones y los informes de seguimiento al Comité.

Coordinará la respuesta a incidentes y la colaboración entre las áreas afectadas. Podrá requerir medidas urgentes de contención dentro de la autoridad previamente delegada y elevará inmediatamente las decisiones que la excedan. Supervisará la eficacia de los controles sin asumir como función ordinaria su administración técnica ni la aceptación del riesgo de negocio. Su intervención no sustituirá las obligaciones de la Dirección ni las funciones independientes del DPO.

5.4. **Responsables de la información y de los servicios**

Cada conjunto de información y cada servicio relevante deberá tener un responsable de negocio identificado. Estas funciones se asignarán a los responsables de los departamentos o procesos que determinan su uso y sus necesidades; no recaerán automáticamente en IT por alojar o administrar los sistemas.

El responsable de la información determinará su clasificación, los usos autorizados, las necesidades de protección y conservación y las personas o perfiles que necesitan acceder a ella. El responsable del servicio definirá sus necesidades de disponibilidad y recuperación, sus dependencias y el impacto de una interrupción. Ambos participarán en el análisis de riesgos y validarán las medidas y prioridades que afecten a su ámbito.

Los responsables de Desarrollo de Producto, Ventas, Diseño y Marketing, Atención al Cliente y Legal y Recursos Humanos ejercerán estas funciones respecto de la información y los procesos de sus áreas, según la asignación documentada. Autorizarán los accesos de negocio, revisarán su necesidad y elevarán los riesgos que no puedan resolver dentro de sus competencias.

5.5. **IT y Responsable de Sistemas**

La Gerencia de IT organizará los recursos necesarios para operar y mantener los sistemas corporativos. El Responsable de Sistemas implantará y administrará las medidas técnicas aprobadas: configuración segura, accesos, actualizaciones, protección de comunicaciones, registros, copias de seguridad y recuperación.

IT ejecutará las altas, modificaciones y bajas de permisos previa autorización del responsable de negocio correspondiente y conservará la trazabilidad de las operaciones.

Administrará las cuentas técnicas y privilegiadas, documentará los cambios e informará al CISO de vulnerabilidades, desviaciones e incidentes. No podrá concederse a sí mismo permisos ajenos a los necesarios para su función ni sustituir al propietario del servicio en la aceptación de riesgos.

En los servicios externalizados, IT coordinará la operación técnica con el proveedor y comprobará el reparto de responsabilidades. La contratación de infraestructura o soporte externo no eliminará las obligaciones de supervisión de DRIVE TECH.

5.6. Desarrollo de Producto e ingeniería

La Dirección de Desarrollo de Producto, bajo la coordinación de la Dirección Tecnológica, incorporará requisitos de seguridad y privacidad a los dispositivos conectados, al software, al firmware y a los servicios asociados durante todo su ciclo de vida. Asignará responsables para las revisiones técnicas, las pruebas y la autorización de versiones.

Los equipos de desarrollo, calidad y especialistas en inteligencia artificial aplicarán las prácticas aprobadas para proteger código, componentes, datos y modelos, verificar cambios y corregir vulnerabilidades. Deberán conservar evidencia de las revisiones y pruebas pertinentes antes de una puesta en producción. Desarrollo de Producto coordinará con IT la operación y con Atención al Cliente la comunicación de actualizaciones e incidencias que afecten a los usuarios.

5.7. Legal y Recursos Humanos

La función jurídica identificará y mantendrá los requisitos legales y contractuales aplicables a la actividad, asesorará sobre contratos con terceros y coordinará la gestión corporativa de privacidad. Apoyará la evaluación de nuevos tratamientos, las obligaciones de notificación y las decisiones sobre conservación y uso de la información. No atribuirá al DPO la ejecución ni la aprobación de los tratamientos que deba supervisar.

Recursos Humanos coordinará las obligaciones de confidencialidad, la formación y la comunicación de esta política. Comunicará a IT y a los responsables de negocio las incorporaciones, cambios de puesto y salidas para adecuar los accesos y recuperar los activos. Las eventuales medidas disciplinarias se tramitarán con asesoramiento jurídico y conforme al marco laboral o contractual aplicable.

5.8. Delegado de Protección de Datos (DPO)

La Dirección evaluará y documentará la obligación de designar un DPO atendiendo a los tratamientos realizados y a la normativa aplicable. Cuando resulte obligatorio o se acuerde una designación voluntaria, formalizará el nombramiento, facilitará sus datos de contacto y garantizará los recursos y condiciones de independencia exigibles.

El DPO informará y asesorará a la organización, supervisará el cumplimiento en materia de protección de datos, asesorará sobre las evaluaciones de impacto y supervisará su realización. Cooperará con la autoridad de control y actuará como punto de contacto. Participará de forma adecuada y oportuna en los asuntos que afecten a datos personales y rendirá cuentas al nivel jerárquico más alto, sin recibir instrucciones sobre el desempeño de sus funciones.

El DPO no determinará los fines y medios de los tratamientos, no aprobará por la empresa las evaluaciones de impacto ni asumirá la responsabilidad de implantar los controles

que supervisa. No se le asignarán funciones que generen conflicto de interés. La responsabilidad de DRIVE TECH como responsable o encargado del tratamiento permanecerá en la entidad, según la posición que ocupe en cada actividad.

5.9. Personal, colaboradores y usuarios autorizados

Toda persona con acceso autorizado a información o recursos de DRIVE TECH deberá conocer las reglas que le afecten, utilizar los medios para los fines permitidos, proteger sus credenciales y comunicar sin demora sospechas de incidentes, pérdidas o accesos indebidos. No compartirá cuentas personales, desactivará controles ni trasladará información a herramientas no autorizadas.

El personal de Ventas, Diseño y Marketing y Atención al Cliente protegerá la información comercial, los materiales de producto y los datos de clientes que utilice. Atención al Cliente trasladará los avisos de seguridad al CISO y a los equipos competentes, evitando incluir datos o credenciales innecesarios en las solicitudes de soporte. El deber de confidencialidad subsistirá tras finalizar la relación en los términos legal y contractualmente exigibles.

5.10. Proveedores y terceros

Los proveedores y colaboradores externos deberán cumplir los requisitos de seguridad que les sean comunicados e incorporados a su relación contractual. Designarán un interlocutor, limitarán los accesos a lo autorizado, comunicarán los incidentes que afecten al servicio y colaborarán en su investigación y resolución en los términos acordados.

El responsable interno del servicio conservará la responsabilidad de supervisar la prestación y coordinará con IT, CISO y Legal las comprobaciones necesarias. Las obligaciones concretas sobre subcontratación, continuidad, acceso a evidencias y devolución o eliminación de información se establecerán conforme al riesgo y al servicio contratado.

6. GESTIÓN DE RIESGOS Y ACTIVOS DE INFORMACIÓN

6.1. Identificación y clasificación de activos

DRIVE TECH deberá mantener un inventario actualizado de los activos que soportan sus procesos y productos. Incluirá, según existan en cada servicio, información de clientes y empleados, documentación comercial y contractual, diseños y prototipos, código fuente, firmware, componentes y modelos de IA, credenciales, equipos, dispositivos de prueba, aplicaciones, infraestructura y servicios de terceros. El inventario identificará a su responsable, finalidad, ubicación o proveedor, dependencias y criticidad.

La clasificación distinguirá información pública, interna, confidencial y restringida, según el perjuicio de su divulgación o uso indebido. Los responsables de la información asignarán el nivel y las condiciones de acceso, compartición, almacenamiento y eliminación. Las claves, secretos técnicos y datos cuya exposición pueda causar un daño especialmente elevado recibirán protección reforzada. La publicación externa requerirá autorización del responsable de la información y revisión de las restricciones legales y contractuales.

6.2. Evaluación y tratamiento de riesgos

El CISO coordinará una evaluación documentada de amenazas, vulnerabilidades, probabilidad e impacto, con participación de negocio, IT y Desarrollo de Producto. El análisis considerará tanto la información corporativa como la seguridad de los productos y servicios utilizados por los clientes, incluidos los efectos de un compromiso de dispositivos conectados y sus dependencias externas.

La evaluación se revisará al menos anualmente y ante nuevos productos, cambios relevantes de arquitectura o proveedores, incidentes graves o vulnerabilidades significativas. Cada tratamiento del riesgo identificará las medidas, su responsable, la prioridad, el plazo aprobado y el riesgo residual. El responsable de negocio propondrá su aceptación dentro de las delegaciones establecidas; cuando las exceda, resolverá la Dirección General. La aceptación quedará motivada y sujeta a revisión.

7. PROTECCIÓN DE LOS SISTEMAS Y DE LA OPERACIÓN

7.1. Identidades y control de acceso

El acceso a información y sistemas se limitará a identidades identificables y a los permisos necesarios para cada función. Se utilizarán cuentas individuales para las personas y se asignará un propietario a cada cuenta técnica. Los permisos deberán contar con autorización, revisarse periódicamente según su criticidad y retirarse cuando desaparezca la necesidad que los justificaba.

Se exigirá autenticación multifactor para accesos remotos, administración y servicios que alberguen información confidencial o restringida. Las cuentas privilegiadas se separarán de las de uso ordinario y se restringirán y registrarán sus actuaciones. Las credenciales, claves y secretos se custodiarán mediante mecanismos autorizados y no se incorporarán al código fuente, a documentación compartida ni a solicitudes de soporte.

7.2. Equipos, trabajo remoto y seguridad física

Los equipos y dispositivos que accedan a recursos corporativos deberán estar inventariados, configurados y actualizados conforme a los requisitos definidos por IT y el CISO. Se aplicarán bloqueo de sesión, protección frente a software malicioso y cifrado cuando corresponda al riesgo y a la movilidad de la información. Se protegerán los puestos de trabajo, las áreas técnicas, los prototipos y los soportes frente a accesos físicos no autorizados, pérdida y daños ambientales.

El trabajo remoto utilizará medios y conexiones autorizados y deberá mantener la confidencialidad de la información en el entorno de trabajo. El acceso desde dispositivos personales solo se permitirá si existe autorización previa y una norma que regule los requisitos técnicos, la separación de información y los límites de actuación de la empresa, respetando los derechos de las personas. En ausencia de esa autorización, se utilizarán los medios corporativos habilitados.

7.3. Comunicaciones, cambios y vigilancia

Las comunicaciones y el almacenamiento se protegerán según la clasificación y el riesgo, con cifrado y gestión adecuada de claves cuando proceda. Se separarán los entornos corporativos, de desarrollo, de pruebas y de producción de acuerdo con sus necesidades. Las conexiones y los servicios expuestos se limitarán a los expresamente necesarios y autorizados.

IT y Desarrollo de Producto mantendrán una gestión de configuraciones, cambios, vulnerabilidades y actualizaciones. Cada cambio relevante deberá evaluarse, autorizarse y permitir la recuperación de una situación estable. Las correcciones se priorizarán según su exposición, posibilidad de explotación e impacto; las demoras deberán justificarse y acompañarse de medidas compensatorias.

Se generarán y protegerán registros de los eventos relevantes para detectar e investigar incidentes. Su alcance, acceso y conservación se establecerán de forma proporcionada, considerando las obligaciones legales y la privacidad. El CISO coordinará la revisión de alertas y la comprobación de la eficacia de las medidas, sin considerar que la mera disponibilidad de registros acredita una vigilancia efectiva.

8. SEGURIDAD DEL DESARROLLO Y DE LOS PRODUCTOS CONECTADOS

8.1. Seguridad desde el diseño y puesta en producción

Los requisitos de seguridad deberán definirse desde la concepción de Burno Clogg, Burno Vision, Burno AI, la plataforma Burnolder y los servicios de ingeniería, y mantenerse en las nuevas versiones y productos. La revisión abarcará el dispositivo, sus comunicaciones, las aplicaciones y los servicios asociados, según la arquitectura concreta. Se considerarán los riesgos de acceso no autorizado, alteración de funciones, exposición de datos e interrupción del servicio.

El código y los componentes deberán proceder de fuentes autorizadas y quedar sujetos a control de versiones, revisión y pruebas de seguridad proporcionadas al riesgo. Se protegerán los repositorios y los procesos de construcción y distribución. Las configuraciones iniciales limitarán las funciones y comunicaciones a las necesarias y evitarán credenciales predeterminadas compartidas entre dispositivos. Los datos de producción no se utilizarán en pruebas salvo necesidad justificada y medidas específicas; se priorizarán datos sintéticos o adecuadamente anonimizados.

La liberación de una versión requerirá la validación de calidad, la revisión de los requisitos de seguridad y la autorización del responsable de producto. Los riesgos pendientes deberán estar documentados y aceptados por quien tenga competencia. No se autorizará una puesta en producción que incumpla requisitos legales aplicables. Los cambios posteriores estarán sujetos al mismo control, con un tratamiento documentado para las intervenciones urgentes.

8.2. Mantenimiento, vulnerabilidades y fin de soporte

Cada producto deberá contar con condiciones de mantenimiento y soporte definidas, coherentes con sus obligaciones legales y contractuales. Desarrollo de Producto mantendrá la identificación de sus componentes y dependencias para evaluar vulnerabilidades y preparar correcciones. Los mecanismos de actualización deberán permitir verificar el origen y la integridad del software o firmware y proteger frente a modificaciones no autorizadas.

Se establecerá un medio accesible para recibir avisos de vulnerabilidades de clientes, investigadores y proveedores, y un procedimiento para evaluarlos, remediarlos y coordinar su divulgación. El CISO y Legal determinarán las obligaciones de notificación que resulten aplicables según el producto, el incidente y el calendario normativo. La finalización del soporte se planificará y comunicará con las medidas necesarias para reducir riesgos y facilitar la retirada o sustitución segura.

8.3. Componentes de inteligencia artificial

Los proyectos que incorporen IA deberán identificar los datos, modelos, dependencias y permisos utilizados. Se evaluarán los riesgos de manipulación de entradas, alteración de datos o modelos, extracción de información y uso abusivo de las funciones disponibles. Los accesos y cambios se controlarán de acuerdo con su impacto en el producto y en las personas.

Las funciones capaces de ejecutar acciones o acceder a otros servicios deberán operar con permisos limitados y controles acordes a su riesgo. El uso interno de asistentes o servicios de IA requerirá autorización y evaluación de las condiciones del proveedor; no se introducirán datos personales, código reservado ni información confidencial en herramientas no autorizadas. La determinación de obligaciones específicas de IA se realizará con Legal atendiendo al uso y a la posición de DRIVE TECH en cada sistema.

9. PROTECCIÓN DE DATOS PERSONALES

La seguridad de los tratamientos se integrará en el diseño y en la configuración por defecto de los productos y procesos. Los responsables de negocio, con apoyo de Legal, identificarán las finalidades, categorías de datos, destinatarios y periodos de conservación y limitarán el tratamiento a lo necesario. Se documentará en cada actividad si DRIVE TECH actúa como responsable, encargado u ocupa otra posición jurídicamente relevante.

Los datos vinculados a la salud que puedan derivarse de las funciones de Burno Clogg y cualesquiera otras categorías especiales requerirán una evaluación específica antes de su tratamiento. Se verificarán la base jurídica y las condiciones adicionales exigibles, la necesidad de una evaluación de impacto y las medidas de protección. Las funciones de monitorización o personalización no habilitarán por sí mismas la reutilización de datos para publicidad, entrenamiento de modelos u otros fines.

Los controles deberán permitir la confidencialidad, integridad, disponibilidad y recuperación de los datos y facilitar el ejercicio de derechos y la supresión o conservación justificada. Cuando se contraten encargados o se prevean transferencias internacionales, Legal comprobará las condiciones exigibles antes de habilitar el acceso. El DPO, cuando esté

designado, asesorará y supervisará sin sustituir las decisiones ni la responsabilidad de la organización.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD

DRIVE TECH deberá disponer de un procedimiento para identificar, comunicar, registrar, evaluar, contener, resolver y revisar los incidentes que afecten a su información, sistemas, productos o servicios. El CISO coordinará su aplicación con IT, Desarrollo de Producto, las áreas de negocio y Legal. El procedimiento establecerá contactos y suplencias, criterios de severidad, capacidad de actuación y vías alternativas de comunicación si los medios habituales quedan comprometidos.

El personal y los terceros obligados contractualmente comunicarán sin demora las sospechas de incidente a través de los medios que se les hayan facilitado. Si no están disponibles, escalarán al responsable de su área y al CISO por una vía alternativa. No se exigirá confirmar el ataque para comunicar una sospecha. Las actuaciones deberán evitar la destrucción innecesaria de evidencias y preservar su integridad, procedencia y acceso restringido.

Los incidentes con posible impacto grave en clientes, productos, datos personales o continuidad se elevarán de inmediato a la Dirección General. Esta coordinará las decisiones de negocio, incluida la suspensión o recuperación de servicios, con el asesoramiento del CISO y las áreas afectadas. Las medidas urgentes de contención podrán ejecutarse conforme a las delegaciones previstas, con registro y comunicación posterior inmediata.

Legal y el CISO evaluarán las comunicaciones exigibles a autoridades, clientes, usuarios y otros afectados, con asesoramiento del DPO cuando corresponda. Cada obligación se determinará conforme al régimen aplicable y sus plazos; un incidente no se notificará automáticamente bajo todas las normas citadas en la política. El procedimiento permitirá cumplir los plazos externos sin esperar a la siguiente reunión del Comité ni al cierre de la investigación.

Toda brecha de datos personales deberá documentarse. Cuando DRIVE TECH actúe como responsable, notificará la brecha a la autoridad de control sin dilación indebida y, de ser posible, dentro de las 72 horas desde que tenga constancia, salvo que sea improbable que constituya un riesgo para los derechos y libertades. Si es probable un alto riesgo, la comunicará a los interesados sin dilación indebida, salvo que concurra una excepción legal. Las decisiones y, en su caso, los motivos de demora deberán documentarse. Cuando actúe como encargado, informará al responsable sin dilación indebida. El cierre del incidente incluirá causas, actuaciones, efectos y mejoras necesarias.

11. CONTINUIDAD Y RECUPERACIÓN

La Dirección de Operaciones coordinará la identificación de los procesos críticos y el impacto de su interrupción, con participación de los responsables de servicio, IT y Desarrollo de Producto. Se analizarán las dependencias necesarias para la atención al cliente, la plataforma Burnolder, la distribución de actualizaciones y los demás servicios que soporten los productos, así como la información necesaria para reanudar la actividad.

Los responsables de servicio propondrán los tiempos de recuperación y la pérdida de datos admisible atendiendo al impacto de negocio, las necesidades de los usuarios y los compromisos asumidos. La Dirección General aprobará las prioridades y los recursos de continuidad. Los objetivos aprobados se documentarán en los planes de cada servicio y se utilizarán para definir y comprobar las capacidades de recuperación.

IT implantará copias de seguridad y mecanismos de recuperación proporcionados, protegidos frente a accesos indebidos y frente al compromiso del entorno principal. La selección de información, frecuencia, conservación, separación y custodia responderá a los requisitos aprobados. Se realizarán pruebas periódicas de restauración y ejercicios de continuidad, registrando los resultados y corrigiendo las deficiencias. La disponibilidad de una copia no se considerará prueba suficiente de recuperabilidad.

Los planes incluirán responsables y suplencias, alternativas operativas, comunicaciones, dependencias de proveedores y criterios para declarar la recuperación. Se revisarán ante cambios relevantes, incidentes o resultados insuficientes de las pruebas.

12. SEGURIDAD EN LAS RELACIONES CON TERCEROS

La contratación de servicios de nube, software, soporte, desarrollo u otras prestaciones que impliquen acceso a información o dependencia tecnológica requerirá una evaluación previa de seguridad proporcional a su criticidad. El responsable del servicio identificará qué se externaliza y qué obligaciones conserva DRIVE TECH, con revisión técnica del CISO e IT y asesoramiento de Legal.

Los contratos deberán concretar los requisitos aplicables: confidencialidad y usos permitidos, control de accesos, ubicación y tratamiento de datos, subcontratación, comunicación y colaboración ante incidentes, continuidad, acceso a evidencias y condiciones de terminación. Los plazos de aviso y la información exigida al proveedor deberán permitir a DRIVE TECH cumplir sus propias obligaciones. Las certificaciones o declaraciones del proveedor se valorarán por su alcance, vigencia y relación con el servicio efectivamente contratado.

El responsable interno revisará el desempeño y los cambios relevantes del proveedor. Al finalizar la relación, coordinará la retirada de permisos, la devolución o eliminación de información y la continuidad o migración del servicio, conservando evidencia de lo acordado. No se mantendrán accesos de terceros sin una necesidad y una autorización vigentes.

Cuando DRIVE TECH preste servicios a clientes, deberá identificar y comunicar las responsabilidades compartidas, los requisitos contractuales y los interlocutores para seguridad e incidentes. Los compromisos de servicio y cualquier exigencia sectorial, incluida la relativa a servicios para el sector público cuando corresponda, se evaluarán antes de su aceptación. No se declarará una certificación ni un nivel de cumplimiento sin evidencia suficiente y alcance definido.

13. DESARROLLO Y APLICACIÓN DE LA POLÍTICA

13.1. Desarrollo documental y entrada en vigor

Esta política se desarrollará mediante normas y procedimientos específicos por materia e instrucciones técnicas para los sistemas y tareas concretos. El CISO coordinará su coherencia. Los responsables de área aprobarán los documentos de su competencia tras la revisión de seguridad y, cuando corresponda, jurídica. Las modificaciones de esta política se someterán a revisión del Comité y aprobación de la Dirección General; las decisiones que excedan las facultades de un responsable se elevarán a la autoridad competente.

Cada documento deberá identificar responsable, versión, aprobación, fecha de entrada en vigor, destinatarios y revisión prevista. Los procedimientos recogerán los medios, frecuencias, contactos y evidencias necesarios para ejecutar las obligaciones, sin incluir esos detalles cambiantes en la política general. Los registros demostrarán las actuaciones realizadas y se conservarán separados de la mera descripción de los controles.

La entrada en vigor de esta política y sus modificaciones requerirá la aprobación documentada de la Dirección General conforme al apartado 5.1. El CISO mantendrá la ficha de control y el historial de versiones, con sus cambios, fechas y decisiones de aprobación. Se comunicará la versión aprobada a las personas y terceros afectados, se facilitará su consulta y se retirarán del uso ordinario las versiones sustituidas. La distribución de instrucciones técnicas y registros se limitará a quienes los necesiten por sus funciones.

13.2. Concienciación y cumplimiento

Recursos Humanos y el CISO coordinarán la formación inicial y periódica conforme a las funciones y riesgos de cada colectivo. Los equipos de desarrollo, administración, soporte y gestión de datos recibirán orientación específica sobre sus responsabilidades. Se conservará evidencia de las comunicaciones y actividades realizadas y se evaluará su utilidad.

Los incumplimientos se analizarán con criterios de proporcionalidad y conforme al marco legal y contractual. Las necesidades de formación, las deficiencias organizativas y las conductas individuales deberán valorarse antes de adoptar medidas. La comunicación de buena fe de una sospecha de incidente se atenderá como parte de la protección de la organización.

13.3. Excepciones y resolución de conflictos

Cualquier excepción a un requisito interno de seguridad deberá solicitarse y justificarse por escrito. El CISO evaluará su riesgo y las medidas compensatorias; el responsable de negocio tramitará su aceptación por quien tenga competencia. La autorización identificará alcance, responsable, duración, condiciones y fecha de revisión. Las excepciones no se renovarán automáticamente ni podrán dispensar obligaciones legales o compromisos con terceros sin la modificación válida que corresponda.

Las discrepancias entre responsables se tratarán en el Comité y, si no se resuelven o exceden sus competencias, se elevarán a la Dirección General. La decisión, su motivación y las medidas acordadas quedarán registradas. Cuando exista un incidente urgente se aplicará el procedimiento de respuesta sin esperar a la resolución ordinaria del conflicto. La independencia del DPO permanecerá preservada.

14. MEJORA CONTINUA

La gestión de la seguridad de la información estará sujeta a mejora continua. El Comité revisará esta política al menos anualmente y cuando se produzcan cambios relevantes en productos, servicios, organización, amenazas, tecnologías, obligaciones o incidentes. El CISO preparará la revisión con las aportaciones de las áreas y el análisis jurídico actualizado. Las modificaciones se someterán a aprobación de la Dirección General y seguirán el régimen de comunicación del apartado 13.1.

La revisión comprenderá los servicios y la información y su clasificación; la actualización anual del análisis de riesgos y cuando se produzcan cambios relevantes; las auditorías internas y, cuando proceda, externas; y la revisión de las medidas de seguridad, normas y procedimientos. El seguimiento considerará también los riesgos pendientes, las vulnerabilidades relevantes, las revisiones de acceso, las pruebas de recuperación, los incidentes, la formación y las dependencias de terceros.

Las desviaciones y oportunidades de mejora darán lugar a acciones con responsable, plazo y criterios para comprobar su cierre y eficacia. El CISO informará de su evolución al Comité, que elevará a la Dirección General las decisiones que requieran recursos o excedan sus competencias. Se conservarán los resultados de las revisiones y las evidencias de las actuaciones realizadas.

Para DRIVE TECH, la gestión adecuada de la ciberseguridad constituye un reto continuo y colectivo. La existencia de esta política o de un procedimiento aprobado no sustituirá la evidencia de que las medidas se han aplicado y funcionan.