Eurovía Servicios Telemáticos, S.L.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Índice

1. Introducción

EUROVIA integra la seguridad de la información en el gobierno y en la prestación de los servicios incluidos en su sistema sometido al Esquema Nacional de Seguridad. La presente Política constituye el marco superior de gobierno para proteger la información, los servicios, las personas, los activos tecnológicos y las relaciones con terceros que forman parte del alcance ENS de la organización.

El sistema se encuentra categorizado como MEDIA. La gestión de la seguridad se articula mediante responsabilidades diferenciadas, gestión basada en riesgos, autorización y control de accesos, protección de la información, control documental, gestión de terceros, prevención y detección, respuesta a incidentes, continuidad y mejora continua. La Normativa de Seguridad de la Información, la arquitectura, los procedimientos y los soportes de registro desarrollan este marco sin sustituirlo.

2. Objeto, finalidad y alcance

2.1. Objeto y finalidad

EUROVIA establece mediante esta Política el marco de gobierno y seguridad aplicable a la información y a los servicios incluidos en el sistema ENS. Su objeto es fijar principios, responsabilidades y reglas generales para preservar, de forma proporcional, la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad que resulten exigibles dentro del alcance.

La finalidad es orientar las decisiones de seguridad, la asignación de responsabilidades, el análisis y tratamiento de riesgos, el control de la documentación y la mejora continua. Esta Política no sustituye los procedimientos operativos ni los registros que deben acreditar la ejecución de las actividades de seguridad.

2.2. Alcance de aplicación

El alcance comprende la prestación de servicios digitales y cloud, la administración de servidores externos -incluidos servicios soportados en AWS/Amazon y Templus-, el diseño, desarrollo y mantenimiento web/Web Apps y el soporte técnico asociado a los sistemas y servicios administrados por EUROVIA.

- Información en alcance: datos personales de relevancia limitada; información de comercios electrónicos sobre empresa, productos, precios, stocks y pedidos; información de clientes e históricos de pedidos y referencias de pago tratadas mediante pasarelas; información pública de la web corporativa; datos empresariales, ERP y permisos gestionados en servicios de administración; código fuente, configuraciones, registros y copias cuando formen parte del servicio.
- Usuarios en alcance: Dirección y responsables ENS; personal técnico de sistemas y administración; personal de desarrollo y soporte; personal administrativo; cuentas técnicas, privilegiadas y de servicio; y terceros autorizados cuando intervengan en los sistemas o servicios incluidos.
- Ubicaciones en alcance: centro de trabajo de EUROVIA en Barcelona, rack técnico e infraestructura local inventariada, infraestructuras y CPD de proveedores cloud/SaaS y sistemas de clientes administrados por EUROVIA en la medida necesaria para prestar el servicio contratado.
- Tecnologías y servicios relevantes: Microsoft 365, GitHub, AWS, Templus, Active Directory, servidores Linux y Windows, VMware ESXi, QNAP NAS, infraestructura de red inventariada, puestos Windows y macOS, dispositivos móviles y mecanismos de comunicación segura como HTTPS/TLS y SSH/SFTP cuando proceda.

El alcance sobre sistemas de clientes se limita a las funciones de administración, soporte o acceso necesarias para el servicio contratado. La inclusión de un recurso, plataforma o relación con un tercero en el entorno de trabajo no amplía por sí misma el alcance más allá de las actividades y servicios expresamente cubiertos por el sistema ENS.

3. Compromisos y principios de seguridad

3.1. Compromiso de la Dirección

La Dirección General asume el gobierno del marco de seguridad y establecerá las condiciones necesarias para que la protección de la información y de los servicios sea coherente con la categoría MEDIA, el alcance y los riesgos del sistema.

- Aprobar la Política y su marco de desarrollo, manteniéndolos alineados con los servicios y responsabilidades de EUROVIA.
- Designar los roles ENS, asegurar la aceptación de sus responsabilidades y proporcionar recursos humanos, técnicos, organizativos y económicos proporcionales a los riesgos.
- Velar por la identificación y observancia de los requisitos legales, regulatorios, contractuales y de seguridad aplicables al alcance.
- Promover una gestión sistemática basada en riesgos, con tratamiento, seguimiento y aceptación del riesgo residual conforme al proceso definido.
- Exigir que la prevención, detección, respuesta ante incidentes, continuidad, dependencias externas y desviaciones de seguridad se gestionen dentro del sistema.
- Revisar la información de seguimiento y promover acciones de mejora cuando los cambios, riesgos, incidentes, revisiones o resultados de los indicadores lo requieran.

3.2. Marco para los objetivos de seguridad

Los objetivos de seguridad se establecerán dentro del sistema de gestión y deberán ser coherentes con el alcance ENS, la protección de la información, el control de accesos, la configuración segura, la continuidad, la gestión de terceros, la prevención y tratamiento de incidentes y la mejora continua. Cada objetivo contará con responsable, método de seguimiento y evidencia asociada.

El seguimiento incluirá indicadores definidos para materias como la revisión de usuarios y permisos y la revisión de la configuración segura de equipos y servidores. Las mediciones y sus resultados se conservarán en los soportes de seguimiento correspondientes y no forman parte de esta Política.

3.3. Principios rectores

- Seguridad integral. La seguridad se incorpora al gobierno, planificación, operación, cambio, mantenimiento y finalización de los servicios y no se trata como una actividad aislada.
- Gestión basada en riesgos. Las decisiones de seguridad se adoptan considerando los activos y servicios reales, las amenazas y escenarios aplicables, las salvaguardas, el tratamiento y el riesgo residual.
- Prevención, detección, respuesta y recuperación. Las medidas se orientan a reducir la probabilidad e impacto de incidentes, detectar anomalías, contener sus efectos y recuperar el servicio de forma ordenada.
- Proporcionalidad y protección por capas. Los controles, recursos y mecanismos de seguridad se ajustan a la categoría MEDIA, al riesgo, a la criticidad, a la exposición y a las dependencias tecnológicas y contractuales.
- Responsabilidad diferenciada, necesidad de conocer y trazabilidad. Las funciones de gobierno, seguridad, servicio y operación se definen separadamente, y el acceso a información y recursos se limita a la necesidad funcional y a la autorización concedida.
- Mínimo privilegio y seguridad durante el ciclo de vida. Usuarios, procesos, servicios y cuentas técnicas dispondrán exclusivamente de las capacidades necesarias, desde la adquisición y puesta en servicio hasta el cambio, mantenimiento y retirada.
- Continuidad y mejora continua. La organización revisará su capacidad de protección y recuperación, las dependencias externas, las incidencias, los cambios y los resultados del seguimiento para mantener la adecuación del sistema.

3.4. Mínimo privilegio

El acceso a información, servicios, equipos, procesos y funciones administrativas estará prohibido por defecto y requerirá autorización expresa. Los permisos y privilegios se limitarán al mínimo necesario de acuerdo con la función asignada, la necesidad de conocer y el ámbito del servicio autorizado.

Los privilegios serán objeto de revisión periódica y se modificarán o retirarán cuando cambien las funciones, cese la necesidad, finalice la relación autorizada o se produzca una circunstancia que altere su justificación. Este principio se aplicará igualmente a usuarios, cuentas privilegiadas, procesos, servicios y cuentas técnicas.

3.5. Mejora continua del proceso de seguridad

EUROVIA mantendrá la mejora continua del proceso de seguridad mediante la revisión de riesgos, servicios, tecnologías, responsabilidades, requisitos aplicables, incidentes, cambios y resultados de seguimiento. La revisión se realizará también cuando se produzcan cambios relevantes que puedan alterar la eficacia o proporcionalidad del marco establecido.

Los indicadores, las revisiones de seguridad y las evidencias asociadas servirán como entrada para decidir acciones de mejora y actualizar, cuando proceda, la documentación y las medidas correspondientes. Los resultados concretos se conservarán en los registros y soportes de seguimiento aplicables.

4. Marco normativo y documental

4.1. Marco normativo

La seguridad de la información de EUROVIA se desarrolla, dentro del ámbito que corresponda a cada disposición, tomando como referencias normativas expresas las siguientes:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

EUROVIA identificará y revisará periódicamente los requisitos legales y regulatorios relevantes para los servicios y la información incluidos en el alcance, trasladando los cambios que resulten aplicables a los riesgos, responsabilidades, documentación, autorizaciones y controles correspondientes.

4.2. Marco documental

La Política de Seguridad de la Información constituye el nivel superior del marco documental. NOR-SEG-001 Normativa de Seguridad de la Información concreta las reglas internas obligatorias, y CAT-SEG-001 Categorización del sistema y ARQ-SEG-001 Arquitectura de Seguridad establecen la categorización y la descripción estructural del sistema dentro de sus respectivos ámbitos.

El desarrollo específico se realiza mediante POL-ACC-001 Política de control de acceso; PRO-ACC-001 Proceso gestión derechos accesos; PRO-AUT-001 Proceso de autorización; PRO-AUT-002 Procedimiento de autorización de nuevas herramientas y aplicaciones; PRO-ADQ-001 Proceso adquisición nuevos componentes y gestión de proveedores; PRO-CFG-001 Procedimiento de gestión de la configuración de seguridad; PRO-FIS-001 Procedimiento de gestión de equipos, dispositivos y soportes; PRO-DOC-001 Procedimiento de gestión de la información; PRO-DES-001 Procedimiento de desarrollo seguro; PRO-CAM-001 Procedimiento de gestión del cambio; PRO-MON-001 Procedimiento registro, monitorización y verificación de actividad y métricas; PRO-INC-001 Proceso tratamiento incidentes; PRO-BCK-001 Procedimiento de copias de seguridad y restauración; BIA-SEG-001 Análisis de impacto en el Negocio (BIA); POL-DPD-001 Política de proteccion de datos y/o seguridad de

la información; POL-FIR-001 Política de Firma electrónica y de Certificados; y PRO-CER-001 Procedimiento de gestión de criptografía, certificados, claves y secretos.

5. Organización e implantación del proceso de seguridad

El proceso de seguridad se organiza mediante la Dirección General, un Comité de Seguridad de la Información o mecanismo equivalente, las funciones de Responsable de la Información, Responsable del Servicio, Responsable de la Seguridad y Responsable del Sistema, y el Departamento de Sistemas para la ejecución técnica que corresponda. Las responsabilidades se mantienen funcionalmente diferenciadas aunque, por razón de la estructura organizativa, varias funciones puedan recaer en una misma unidad o persona.

5.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información o mecanismo equivalente actuará como órgano de coordinación, decisión, revisión y escalado de las cuestiones relevantes de seguridad. Su composición comprenderá al Gerente/Director General y al Director Técnico, sin perjuicio de la participación de los responsables o especialistas que deban intervenir por razón de la materia tratada.

El Comité coordinará riesgos, cambios relevantes, continuidad, incidentes, dependencias externas, necesidades de seguridad y conflictos entre responsabilidades. Las decisiones que requieran aprobación superior o excedan su autoridad se elevarán a la Dirección General y deberán conservar la trazabilidad correspondiente fuera de esta Política.

5.2. Roles y responsabilidades

Rol	Responsabilidad de alto nivel
Dirección General	Aprobar la Política, designar los roles ENS, proporcionar orientación y recursos proporcionales, supervisar el sistema y resolver los conflictos elevados.
Responsable de la Información	Determinar los requisitos de protección de la información, participar en su clasificación y en las decisiones de riesgo y tratamiento que afecten a la información.
Responsable del Servicio	Determinar los requisitos de seguridad y continuidad de los servicios incluidos en el alcance y participar en la priorización de necesidades de servicio.
Responsable del Sistema	Gestionar la operación del sistema y ejecutar las medidas, configuraciones, cambios y autorizaciones aprobadas dentro de su ámbito.
Responsable de Seguridad	Coordinar la seguridad, el análisis y seguimiento de riesgos, la supervisión de controles, los incidentes, la mejora y el asesoramiento a la Dirección.
Comité de Seguridad de la Información o mecanismo equivalente	Coordinar decisiones, revisar riesgos y resultados de seguimiento, tratar conflictos y elevar a la Dirección las cuestiones que excedan su autoridad.
Departamento de Sistemas	Ejecutar las tareas técnicas de administración, configuración, accesos, cambios y operación que le sean asignadas conforme a las autorizaciones y procedimientos vigentes.
Personal usuario y administradores	Cumplir la Política, la Normativa y los procedimientos; proteger información y credenciales; operar dentro de las autorizaciones y comunicar incidentes.
Proveedores y terceros	Cumplir los requisitos contractuales y de seguridad, limitar los accesos a lo autorizado y colaborar en trazabilidad, continuidad e incidentes cuando corresponda.

5.3. Designación y renovación de roles

La Dirección General designará formalmente los titulares de los roles de seguridad mediante nombramiento, acuerdo u otra evidencia equivalente. La designación identificará el rol, el ámbito de responsabilidad, las atribuciones y los límites aplicables, y deberá ser aceptada por el titular de forma trazable.

La designación será revisada y, cuando proceda, renovada, modificada o cesada ante sustituciones, cambios organizativos, modificaciones del alcance, alteraciones relevantes de funciones o cualquier circunstancia que afecte a la capacidad para ejercer la responsabilidad asignada. La evidencia de cada actuación se conservará en el expediente documental correspondiente.

5.4. Resolución de conflictos

Los conflictos entre requisitos de protección de la información, necesidades de servicio, seguridad y operación se resolverán preservando la separación funcional de responsabilidades. En particular, la supervisión de seguridad y la ejecución operativa deberán mantenerse diferenciadas entre el Responsable de Seguridad y el Responsable del Sistema.

Cuando una misma persona acumule excepcionalmente las funciones de Responsable de Seguridad y Responsable del Sistema, la situación deberá justificarse, analizar sus incompatibilidades y contar, antes de su aceptación, con la medida compensatoria aprobada que proceda. Los conflictos no resueltos o que excedan la autoridad de los responsables se elevarán al Comité o a la Dirección General.

6. Tratamiento de datos personales e información de clientes

Los datos personales y la información de clientes incluidos en el alcance se protegerán de acuerdo con su naturaleza, clasificación, riesgos, finalidad y requisitos aplicables. La responsabilidad sobre los requisitos de protección de la información se asigna al Responsable de la Información, sin perjuicio de las responsabilidades específicas previstas en POL-DPD-001 Política de proteccion de datos y/o seguridad de la información.

La organización aplicará controles de acceso, custodia, conservación, transferencia y tratamiento acordes con la sensibilidad y el uso autorizado de la información. El detalle sobre clasificación, almacenamiento, transmisión, custodia y demás reglas de gestión se desarrolla en PRO-DOC-001 Procedimiento de gestión de la información.

Los inventarios, clasificaciones y evidencias de tratamiento se conservarán en los soportes correspondientes, incluido REG-ACT cuando proceda. Esta Política no incorpora inventarios cumplimentados ni resultados particulares de clasificación o tratamiento.

7. Análisis y gestión de riesgos

7.1. Enfoque de gestión

La seguridad del sistema se gobernará mediante análisis y gestión de riesgos sobre los activos y servicios reales del alcance. El proceso comprenderá la identificación de activos y servicios, amenazas y escenarios, valoración, identificación de salvaguardas, tratamiento, determinación del riesgo residual, asignación de responsables, revisión y aceptación conforme a la metodología aprobada.

La trazabilidad del análisis y de las decisiones se conservará en REG-RIE Análisis / Registro de Riesgos ENS. Los resultados, valoraciones y niveles concretos de riesgo se gestionan en dicho soporte y no se reproducen en esta Política.

7.2. Medidas compensatorias

Las medidas compensatorias solo podrán utilizarse cuando exista una limitación objetiva, estén formalmente justificadas y aprobadas, se vinculen al control o refuerzo afectado, a la limitación identificada y al riesgo correspondiente, y permitan preservar la finalidad de seguridad mediante un criterio de eficacia definido.

La medida compensatoria no sustituirá una implantación ordinaria meramente pendiente ni podrá considerarse eficaz por su sola documentación. Cuando proceda su utilización, su alcance, responsable, evidencias y revisión se mantendrán en el soporte aprobado para dicha finalidad.

8. Desarrollo documental de la política

La presente Política se desarrolla mediante la Normativa de Seguridad de la Información y los documentos finales aprobados del sistema, manteniendo en cada pieza el nivel de detalle que corresponde a su función y evitando duplicar contenido operativo o técnico.

Gobierno y arquitectura: NOR-SEG-001, CAT-SEG-001 y ARQ-SEG-001.
Acceso y autorizaciones: POL-ACC-001, PRO-ACC-001, PRO-AUT-001 y PRO-AUT-002.
Proveedores, configuración y operación: PRO-ADQ-001, PRO-CFG-001, PRO-FIS-001, PRO-DOC-001, PRO-DES-001, PRO-CAM-001 y PRO-MON-001.
Incidentes y continuidad: PRO-INC-001, PRO-BCK-001 y BIA-SEG-001.
Protección de datos y criptografía: POL-DPD-001, POL-FIR-001 y PRO-CER-001.

Las referencias visibles utilizarán exclusivamente los códigos y nombres vigentes de los documentos finales. Los registros y soportes de ejecución conservarán las evidencias operativas correspondientes y no se sustituirán por la existencia de esta Política.

9. Gestión de personal

Los puestos y funciones con acceso a información o servicios del alcance deberán disponer de responsabilidades y requisitos de seguridad definidos, actualizados y coherentes con los riesgos, las tecnologías utilizadas, los privilegios concedidos y el nivel de responsabilidad asumido.

La gestión de personal abarcará la incorporación, modificación y cese de funciones, la asignación y revocación de accesos, la información y formación necesarias y la actualización de obligaciones cuando cambien las funciones, los riesgos o la tecnología. Las evidencias de formación y concienciación se mantendrán en REG-FOR conforme al soporte definido.

9.1. Obligaciones del personal

- Utilizar la información, equipos, cuentas, servicios y accesos únicamente para las finalidades y funciones autorizadas.
- Mantener la confidencialidad y proteger credenciales, información, equipos, soportes y materiales frente a uso, pérdida, divulgación o modificación no autorizados.
- Cumplir NOR-SEG-001 Normativa de Seguridad de la Información y los procedimientos que resulten aplicables a la actividad realizada.
- Respetar el mínimo privilegio, la necesidad de conocer, las condiciones de acceso y las restricciones de uso establecidas para cada recurso o servicio.
- Utilizar de forma segura el correo, la navegación, los puestos y los medios de almacenamiento o transmisión, y comunicar sin demora incidentes, anomalías, pérdidas o sospechas de compromiso.
- Participar en las actividades de formación y concienciación que correspondan a la función y cumplir las obligaciones comunicadas por la organización.

10. Terceras partes, prestadores y proveedores

Los terceros, prestadores y proveedores que soporten el alcance estarán sujetos a requisitos de seguridad proporcionales al servicio, la información tratada, los accesos concedidos y su criticidad. La evaluación, autorización, contratación y seguimiento se desarrollarán conforme a PRO-ADQ-001 Proceso adquisición nuevos componentes y gestión de proveedores y se apoyarán en REG-PRO y en las evidencias contractuales o de seguimiento disponibles.

Entre los proveedores tecnológicos identificados en el alcance se encuentran Microsoft, incluidos Microsoft 365 y GitHub, Amazon/AWS y Templus. Las responsabilidades de EUROVIA sobre gobierno, autorización, configuración y uso no se trasladan automáticamente al proveedor por el hecho de utilizar un servicio cloud, SaaS o de infraestructura externa.

11. Profesionalidad

Las personas que administren, desarrollen, operen o soporten el sistema deberán disponer de competencias, conocimientos y profesionalidad adecuados a las funciones y responsabilidades asignadas. La autorización para ejecutar tareas de impacto relevante dependerá de la función y del nivel de acceso requerido.

Las necesidades de competencia se revisarán cuando cambien las funciones, los riesgos o la tecnología. La formación y la concienciación se gestionarán conforme a las necesidades definidas para cada colectivo, sin que esta Política presuponga certificaciones, cursos o acreditaciones que no consten expresamente.

12. Protección de las instalaciones

Las instalaciones, el centro de trabajo de EUROVIA en Barcelona, el rack técnico, la infraestructura local y las ubicaciones relevantes para el sistema se protegerán frente al acceso o manipulación no autorizados y frente a circunstancias que puedan afectar a la disponibilidad, integridad o custodia de los activos.

El acceso físico se limitará a personal autorizado y las intervenciones, entradas, salidas, traslados o actuaciones sobre equipos y soportes se someterán a los controles y trazabilidad que correspondan. El detalle se desarrolla en ARQ-SEG-001 Arquitectura de Seguridad y PRO-FIS-001 Procedimiento de gestión de equipos, dispositivos y soportes, utilizando REG-EQS cuando resulte aplicable.

13. Adquisición de productos de seguridad y contratación de servicios de seguridad

La adquisición o incorporación de componentes, herramientas, aplicaciones y servicios que puedan afectar al sistema requerirá una evaluación previa y proporcional de seguridad, la definición de requisitos aplicables y la autorización correspondiente antes de su incorporación al entorno de servicio.

La evaluación considerará la finalidad, riesgos, requisitos de protección, condiciones del proveedor, capacidad de gestión y compatibilidad con el sistema. El desarrollo operativo se realizará mediante PRO-ADQ-001 Proceso adquisición nuevos componentes y gestión de proveedores, PRO-AUT-001 Proceso de autorización y PRO-AUT-002 Procedimiento de autorización de nuevas herramientas y aplicaciones.

14. Integridad y actualización del sistema

La configuración, modificación, actualización y desarrollo de los componentes del sistema deberán preservar la integridad y seguridad del entorno, aplicar el principio de mínimo privilegio y quedar bajo responsabilidad de personal autorizado. Las configuraciones y cambios se mantendrán controlados durante su ciclo de vida.

Los cambios y desarrollos se validarán antes de su puesta en producción cuando proceda y mantendrán la trazabilidad necesaria en los soportes definidos, incluido REG-CAM para la gestión de cambios. El detalle se desarrolla en PRO-CFG-001 Procedimiento de gestión de la configuración de seguridad, PRO-CAM-001 Procedimiento de gestión del cambio y PRO-DES-001 Procedimiento de desarrollo seguro.

15. Prevención ante otros sistemas de información interconectados

Las interconexiones con servicios cloud/SaaS y con sistemas de clientes que resulten necesarias para la prestación deberán estar identificadas, autorizadas y protegidas mediante mecanismos adecuados al servicio y a los riesgos asociados. La arquitectura y las responsabilidades de cada conexión se documentarán al nivel que corresponda.

El entorno utiliza, según el servicio, mecanismos como HTTPS/TLS y SSH/SFTP y otros medios equivalentes autorizados. El detalle y control se desarrollan en ARQ-SEG-001 Arquitectura de Seguridad y PRO-AUT-001 Proceso de autorización. La Política no presupone que el inventario de interconexiones sea exhaustivo más allá de los elementos formalmente consolidados.

16. Registro de la actividad y detección de código dañino

La actividad relevante del sistema deberá registrarse y revisarse de acuerdo con las medidas y soportes operativos definidos, de forma que los eventos necesarios puedan apoyar la supervisión, la investigación y el tratamiento de incidentes. La protección frente a código dañino se aplicará conforme a la función y exposición de equipos y servicios.

El detalle se desarrolla en PRO-MON-001 Procedimiento registro, monitorización y verificación de actividad y métricas y PRO-CFG-001 Procedimiento de gestión de la configuración de seguridad. Los registros y paneles se soportan de forma distribuida en firewall, servidores, antivirus/EDR, Microsoft 365 y plataformas cloud; esta Política no presupone la existencia de un SIEM centralizado ni incorpora resultados de monitorización.

17. Gestión de incidentes de seguridad

Los incidentes de seguridad deberán notificarse, registrarse, analizarse, contenerse, resolverse y cerrarse conforme al proceso definido, preservando las evidencias que resulten necesarias. El personal y los terceros autorizados comunicarán las anomalías o hechos que puedan afectar a la información o a los servicios.

PRO-INC-001 Proceso tratamiento incidentes desarrolla las responsabilidades, escalado y actuaciones del proceso. REG-INC constituye el soporte de trazabilidad para los incidentes y las evidencias asociadas; esta Política no incorpora incidentes concretos ni resultados de su tratamiento.

18. Continuidad de la actividad

La continuidad y recuperación de los servicios se gestionarán atendiendo a las necesidades del negocio, la criticidad de la información y de los servicios, las dependencias tecnológicas y humanas, la capacidad disponible y las relaciones con terceros. El análisis de impacto y las prioridades de recuperación se mantendrán coordinados con las copias y la gestión de riesgos.

BIA-SEG-001 Análisis de impacto en el Negocio (BIA) y PRO-BCK-001 Procedimiento de copias de seguridad y restauración desarrollan este marco. REG-BCK y REG-CON conservarán las evidencias de copias, restauraciones y pruebas de continuidad conforme a sus respectivos soportes, sin que la Política anticipe resultados no evidenciados.

19. Gestión documental, revisión y comunicación

La documentación de seguridad se mantendrá identificada, versionada, controlada, disponible para quienes la necesiten y protegida frente a modificaciones no autorizadas. La Política, la Normativa y los documentos de desarrollo estarán sujetos a reglas de aprobación, revisión, comunicación y mantenimiento conforme a PRO-DOC-001 Procedimiento de gestión de la información y NOR-SEG-001 Normativa de Seguridad de la Información.

19.1. Autorización y control de accesos

El acceso a información, servicios, equipos y funciones administrativas estará prohibido por defecto, requerirá autorización expresa y se limitará al mínimo privilegio y a la necesidad funcional. Las altas, modificaciones, privilegios, revisiones y bajas se mantendrán trazables mediante REG-ACC y los soportes autorizados.

El acceso remoto estará igualmente sujeto a autorización y a las reglas específicas definidas para el servicio. POL-ACC-001 Política de control de acceso, PRO-ACC-001 Proceso gestión derechos accesos y PRO-AUT-001

Proceso de autorización desarrollan esta materia. La Política no presupone cobertura universal de autenticación multifactor en todas las plataformas.

19.2. Control documental

Los documentos del sistema deberán mantener identificación, código o denominación, versión, fecha de emisión, autoridad de aprobación y estado de vigencia cuando corresponda. Las versiones obsoletas se controlarán y la capacidad de modificar documentación se limitará a las personas autorizadas.

Los diagramas, documentos de arquitectura y demás información documental se protegerán conforme a su sensibilidad y necesidad de acceso. PRO-DOC-001 Procedimiento de gestión de la información desarrolla las reglas de estructura, control, conservación, revisión y protección documental.

19.3. Protección de la información almacenada y en tránsito

La información almacenada y en tránsito se protegerá mediante controles acordes con su clasificación, riesgo, finalidad y canal. Se aplicarán controles de acceso, custodia, integridad y trazabilidad, incluidos medios cifrados cuando proceda conforme a las condiciones autorizadas del servicio.

El detalle se desarrolla en PRO-DOC-001 Procedimiento de gestión de la información, PRO-CER-001 Procedimiento de gestión de criptografía, certificados, claves y secretos y POL-FIR-001 Política de Firma electrónica y de Certificados. Esta Política no fija algoritmos, suites, claves, longitudes ni una cobertura criptográfica distinta de la que se encuentre documentada y autorizada.

19.4. Comunicación y aplicación

La Política y la Normativa de Seguridad de la Información se pondrán a disposición de las personas afectadas y los procedimientos se comunicarán a quienes deban aplicarlos. La organización conservará fuera de esta Política las evidencias de comunicación, formación y aceptación que correspondan.

Las obligaciones aplicables a terceros deberán comunicarse o incorporarse en los instrumentos contractuales, autorizaciones y procedimientos que regulen su intervención. NOR-SEG-001 Normativa de Seguridad de la Información desarrollará las reglas internas de aplicación general.

19.5. Revisión y mantenimiento

La Dirección General revisará esta Política cuando cambien de forma relevante los riesgos, servicios, tecnologías, requisitos normativos, organización, responsabilidades o alcance del sistema, y utilizará los indicadores definidos y los resultados de revisión como entrada para decidir su mantenimiento o modificación.

Las modificaciones aprobadas se incorporarán bajo control de versión y se trasladarán a los documentos relacionados cuando afecten a sus obligaciones o referencias. PRO-DOC-001 y PRO-MON-001 desarrollan respectivamente el control documental y los mecanismos de seguimiento y métricas.

19.6. Aprobación y entrada en vigor

La aprobación de esta Política corresponde a la Dirección General de EUROVIA. La versión aprobada entrará en vigor desde la formalización de dicha aprobación y mantendrá su vigencia hasta que sea sustituida por una revisión posterior o se acuerde expresamente su retirada.

EUROVIA conservará la evidencia formal de aprobación, el control de versión y la trazabilidad de su publicación o puesta a disposición. La firma, la fecha de aprobación y la evidencia de comunicación se conservarán en los soportes formales correspondientes y no se presuponen por la emisión de esta versión documental.