

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión: 1.0

Fecha de aprobación: 14/04/2026

ÍNDICE

1. Aprobación y Entrada en Vigor	3
2. Misión de la Organización.....	3
3. Alcance.....	3
4. Objetivos	4
5. Desarrollo	4
6. APROBACIÓN POR DIRECCIÓN.....	4

1. Aprobación y Entrada en Vigor

Esta Política de Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política.

2. Misión de la Organización

B2DL GROUP SL para alcanzar sus objetivos asume su compromiso con la seguridad de la información, comprometiéndose a la adecuada gestión de esta, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

B2DL GROUP SL es una consultora de ciberseguridad, que se dedica a proteger la información y los activos digitales de las organizaciones, mitigando los riesgos de ciberataques y asegurando la continuidad del negocio en un entorno cada vez más digital y amenazante.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC 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 y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación).

3. Alcance

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

4. Objetivos

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

5. Desarrollo

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender.

6. APROBACIÓN POR DIRECCIÓN

La presente Política de Seguridad de la Información ha sido revisada por el Responsable de Seguridad y aprobada formalmente por la Dirección de **B2DL GROUP S.L.**, quien asume el compromiso de proporcionar los recursos necesarios para su cumplimiento y garantizar su implementación efectiva en todos los sistemas y procesos incluidos en su alcance.

La política entra en vigor en la fecha de su aprobación y es de obligado cumplimiento para todo el personal de la organización, así como para terceros que accedan a los sistemas o a la información bajo responsabilidad de **B2DL GROUP S.L.**