1. Objeto.

Establecer las directrices y principios que regirán el modo en que DESARROLLOS BINARIOS Y COMUNICACIONES, S.L., en adelante DBC, gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de medidas de seguridad aplicando los requisitos del marco regulatorio legal y vigente del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, siendo su aplicación en el ámbito de la administración electrónica del sector público, que exige el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

2. Alcance.

Teniendo en cuenta las interfaces y dependencias entre las actividades realizadas por la entidad y las que se llevan a cabo por otras organizaciones en el cumplimiento de su misión y del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, DBCha establecido el alcance siguiente:

- Los sistemas de la información que dan soporte a las actividades de mantenimiento y venta de material informático.

3. Misión, marco legal y regulatorio.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, obliga a DBC a proteger los servicios que presta a sus partes interesadas en los que emplea medios electrónicos.

Con la implantación del ENS, se fortalece la seguridad de los servicios, así como de la información que incluyen dichos servicios y que son necesarios para su correcta y adecuada prestación, por la estrecha relación entre ambos y los elementos adicionales que mejoran la gestión de la seguridad de la información.

DBC trata datos personales que se mantienen inventariados por tratamiento, con el objeto de facilitar el control, la gestión y la protección de estos, aplicando medidas para cumplir con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (RGPD), así como con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDgdd).

El ENS de DBC se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de éstas para el empleo adecuado de las mismas en el desarrollo de las actividades.

El marco legal antes indicado estará en consonancia con el ENS de DBC, ya que uno de los grupos de controles de seguridad de éste es el Cumplimiento de la Legislación Aplicable.

4. Liderazgo y Comité.

La Dirección de DBC se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del ENS, así como a demostrar liderazgo y compromiso respecto a éste, a través del Comité de Seguridad de la Información que tiene las siguientes responsabilidades:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que éstos sean compatibles con la estrategia de DBC.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del ENS en los servicios y procesos de DBC.
- Asegurar que los recursos necesarios para el ENS estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del ENS.
- Asegurar que el ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del ENS.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.
- Aprobación y adaptación de los diferentes procedimientos y Normativa de Seguridad.

5. Objetivos de seguridad de la información.

Los objetivos de seguridad de la información se establecen en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos se realiza tomando en cuenta los siguientes elementos:

- Lo que se va a hacer.
- Los recursos necesarios.
- El responsable.
- Plazo de consecución.
- Indicadores para evaluar el resultado/cumplimiento.

6. Directrices para la gestión de la documentación.

El despliegue del ENS de DBC se inicia a partir del análisis de riesgos de seguridad de los sistemas de información (incluyendo los derivados del tratamiento de datos personales), que permita determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles de seguridad necesarios y oportunidades de mejora para el tratamiento del riesgo y llevarlo a un nivel aceptable, tomando en cuenta el contexto de la organización.

Los controles de seguridad deben implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada que deberá

siempre ser revisada y aprobada por el Comité de Seguridad de la Información, según se establece en el procedimiento de gestión documental.

En cumplimiento del artículo 12 del Real Decreto del ENS, la presente política de seguridad se desarrolla aplicando los siguientes requisitos mínimos para incluirse en la documentación del sistema:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos de seguridad de los sistemas de información (incluyendo los derivados del tratamiento de datos personales).
- Gestión de personal.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de
- seguridad.
- Mínimo privilegio.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Además de aplicar los requisitos del propio Real Decreto 311/2022 como tal, se utilizan las Guías CCN-STIC de Seguridad que son las normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de seguridad de las organizaciones, especialmente la Serie CCN-STIC-800 que establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS.

Se comunicará la información documentada de los controles de seguridad al personal que trabaja en la entidad (personal interno y externo), que tendrá la obligación de aplicarla en la realización de sus actividades laborales,

comprometiéndose de este modo al cumplimiento de los requisitos del ENS de DBC.

La información documentada se clasifica en: pública, interna y confidencial, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio establecido en el Procedimiento de Clasificación, Etiquetado y Protección de la Información.

Con la periodicidad que la ley establezca se realizarán auditorías que revisen y verifiquen el cumplimiento del ENS de DBC según los requisitos vigentes en cada momento, por lo que el personal afectado por el alcance de dichas auditorías deberá ser colaborativo para la eficacia de estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

7. Funciones y responsabilidades de seguridad de la información.

a. El Comité de Seguridad de la Información es el órgano encargado de revisar y proponer la aprobación de la presente Política de Seguridad de la Información al Dirección, que será el máximo responsable de la información.

b. El Comité de Seguridad de la Información centraliza los mecanismos de coordinación y resolución de conflictos entre los responsables que se indican a continuación, que se tratarán mediante debate durante las reuniones de los miembros de dicho comité:

- El Dirección de DBC, será el encargado de aprobar la política y el responsable de la autorización de sus modificaciones.
- El Responsable de Seguridad de la Información, la Gerencia de DBC, será el encargado de notificar la presente política al personal y de los cambios que en ella se produzcan, así como de determinar la categoría de seguridad del sistema y coordinar las acciones de implantación, mantenimiento y mejora del ENS de la empresa (incluyendo la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables del Real Decreto que regula el ENS y de las derivadas del Análisis y Gestión de Riesgos), y de sus auditorías.
- El Responsable del Sistema correspondiente se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información derivados de la categoría de seguridad del sistema.

- El Responsable del Servicio correspondiente se encargará de gestionar los requisitos de seguridad de las actividades para la prestación de los servicios.

c. En cuanto al cumplimiento de la medida de seguridad del ENS de Calificación de la Información del ENS, con respecto a la categorización de los sistemas de información, se establece lo siguiente:

- El responsable de la información y del servicio afectado por el análisis y gestión de Riesgos se indicará en el Análisis de Riesgos del ENS.
- El Análisis de riesgos recogerá los criterios que determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS.
- El responsable de cada información y/o de cada servicio deberá seguir los criterios determinados, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS, para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- El responsable de la información y del servicio, en cada momento, tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido.

d. En cuanto al cumplimiento de la medida de seguridad del ENS marcado de soportes -de protección de los soportes de información-, los soportes de información que contengan información, que deba protegerse con medidas de seguridad específicas, llevarán las marcas correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación (que es la confidencial, que es la única que podrá incluir una etiqueta o marca de agua, en su caso). Esto se detallará en el Procedimiento de Gestión de Soportes de Información y Protección de la Información.

e. El Responsable de Protección de Datos, es el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, por lo que trabajará en coordinación con el Responsable de Seguridad de la Información y con el Responsable del Sistema.

f. Todo el personal, tanto interno como externo, es responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del ENS de DBC en sus actividades laborales que afecta a su desempeño en seguridad de la información.

8. Revisión de la política de seguridad de la información.

La presente Política de Seguridad de la Información será examinada por la dirección, a través del Comité de Seguridad de la Información, siempre que se produzcan cambios significativos, o en su defecto como mínimo, una vez al año.

9. Aprobación, difusión y aplicación de la política de seguridad de la información.

La presente Política de Seguridad de la Información es aprobada por el Dirección de DBC, mediante firma y difundida a las partes interesadas; y será efectiva desde el día siguiente al de su aprobación por este órgano.

Así mismo el Dirección dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el ENS de la entidad.

Firmado en Melilla a 1 de Septiembre de 2024

Fdo.: