Política de Seguridad de la Información

Historial de Versiones

Fecha	Versión	Elaborado por	Descripción de cambios
01/09/2024	1.0	Beñat Uriarte	Primera Versión

Información del documento

Nombre	Política de Seguridad de la Información
Versión	1.0
Creado por	Beñat Uriarte
Aprobado por	Comité de Dirección de Danobatgroup

CONFIDENCIALIDAD

Este documento se establece para permitir conocer la información que describe. Está destinado al uso exclusivo de la persona a quien está dirigido, llamados en este documento "el lector".

Ninguna información contenida en este documento puede ser comunicada a terceros sin la conformidad del autor. Está prohibida la reproducción total o parcial del mismo.

Una vez recibido este documento, el lector se compromete a:

- Utilizar la información contenida en el mismo, ya sean técnicas, económicas, comerciales, financieras, sociales u otras, dentro de los límites establecidos por el autor y siempre bajo su autorización.
- Prohibir el uso abusivo o ilícito de esta información.
- Divulgar esta información únicamente a las personas directamente relacionadas con el conocimiento de la misma, nunca a terceros que no sean el autor o lector de la misma.

Si el lector no estuviera de acuerdo con estos puntos, este documento sería devuelto a su autor.

La/s persona/s autora/s de este documento puede/n decidir, en cualquier momento, divulgarlo total o parcialmente a terceros.

Contenido

1. Objeto del documento

La presente Política de Seguridad de la Información tiene como objetivo marcar los principios y directrices que den el soporte adecuado para una correcta gestión de la Seguridad de la Información, de modo que se asegure el adecuado control, rigor y cumplimiento en las actuaciones que se lleven a cabo.

La Dirección de Danobatgroup, reconoce la importancia que tiene la seguridad de la información para la correcta realización de sus actividades.

Por ello ha desarrollado la Política de Seguridad de la Información, que fija e integra los principios básicos de seguridad con los requisitos operativos en términos de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y conservación de la información.

El principal objetivo de esta Política es reforzar el compromiso de la Dirección de Danobatgroup con los empleados, empresas, clientes y proveedores, expresado en términos de mejora continua del servicio ofrecido, del cumplimiento de la legislación aplicable, de la mejora de los procesos internos y de la protección de la información manejada dentro del entorno de Danobatgroup.

Se hace por tanto necesario que todas las personas que interaccionen de manera directa o indirecta con Danobatgroup conozcan esta Política y las Normativas pertinentes para que apliquen sus directrices como tareas propias de las funciones desarrolladas en su vinculación con la misma.

Así pues, la Política de Seguridad de la Información desarrollada en este documento velará por garantizar la protección de los activos de información de Danobatgroup, siendo ésta de aplicación en todas las fases del ciclo de vida de dichos activos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción.

Para la aplicación efectiva de la presente Política y de la Normativa que la desarrolla, la Dirección de Danobatgroup se dotará de los recursos necesarios para su buen desarrollo, tanto en lo referente a las actividades de implantación como de mantenimiento, incluyendo los controles o medidas de seguridad que en cada ámbito se establezcan.

2. Ámbito de aplicación

El alcance de la presente Política (tanto en formato físico o electrónico) comprende a las siguientes figuras:

- A todo el personal que participe en Danobatgroup
- A contratistas y terceros con acceso a los activos propiedad de Danobatgroup o bajo su responsabilidad.
- A la información tratada, almacenada y custodiada dentro de Danobatgroup.
- A todas las instalaciones, recursos y procesos utilizados para la prestación de servicios de Danobatgroup, sean estos internos o vinculados con terceros a través de acuerdos o contratos.

La aprobación de esta Política, así como su modificación o sustitución, en su caso, son competencia de la Dirección de Danobatgroup.

3. Aprobación por la dirección

La presente Política ha sido aprobada por la Dirección de Danobatgroup en su reunión de 16 de Julio de 2025, encontrándose a partir de ese momento plenamente en vigor en todos sus términos.

4. Premisas principales de la seguridad de la información

Con el fin de garantizar la existencia de un marco global de seguridad de la información que proteja, en la medida de lo posible, frente a dichas amenazas, la Dirección de Danobatgroup procederá a adoptar una serie de medidas para prevenir, detectar, reaccionar y recuperarse ante posibles incidentes que afecten a la información.

La seguridad de la información es entendida como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

Se llevarán a cabo diferentes iniciativas que respalden los esfuerzos ya realizados, de cara a proporcionar una visión general sobre la seguridad de la información a todas las partes interesadas, definir los controles adecuados para proteger los activos y cumplir con los requisitos marcados por la legislación vigente.

En este sentido, se deberá poner en marcha los mecanismos adecuados para prevenir, detectar, reaccionar y recuperarse a los posibles incidentes que puedan afectar a la seguridad de la información. Entre dichos mecanismos se encuentran, entre otros, las medidas que se detallan a continuación.

4.1 Prevención

Se tratará de prevenir y evitar la existencia de incidentes que puedan afectar a la seguridad de la información y a los servicios prestados. Para ello, se implantarán las medidas y controles de seguridad necesarios, que se definirán mediante un proceso formal de análisis y gestión de riesgos.

Dichas medidas y controles, así como las responsabilidades en materia de seguridad de la información serán definidos y documentados de manera clara y formal tanto en la Política como en la Normativa de Seguridad de la Información.

Asimismo, y para garantizar el cumplimiento de la Política de Seguridad de la Información, a través de cada uno de sus departamentos, deberá:

- Participar activamente en el ciclo de vida de desarrollo de los sistemas, especialmente en la autorización de estos antes de entrar en operación.
- Realizar evaluaciones periódicas del estado de seguridad de la información, solicitando la revisión por parte de terceros para disponer de una evaluación independiente

4.2 Detección

Las medidas de prevención no son siempre suficientes ante incidentes de seguridad, por lo que se monitorizará de manera continua el funcionamiento de los sistemas de información de cara a identificar anomalías en su operación.

Ante la detección de un incidente de seguridad de la información, se pondrán en marcha los mecanismos de verificación, análisis y comunicación de este.

4.3 Respuesta

Tras la detección y verificación de un incidente que afecte a la seguridad de la información se deberá:

- Establecer mecanismos para responder de manera ágil y eficaz.
- Designar puntos de contacto para las comunicaciones relativas a incidentes de seguridad de la información detectados en otros organismos públicos o privados, que ayuden a disponer de información temprana sobre posibles incidentes, así como disponer de mecanismos de respuesta que hayan demostrado ser exitosos.
- Establecer protocolos para el intercambio de información relacionada con el incidente de seguridad de la información.

4.4 Recuperación

Para aquellos casos en que los incidentes causen un impacto importante, se dispondrá de planes de continuidad, asegurando que se encuentran integrados con los planes generales de continuidad de negocio y actividades de recuperación.

5. Marco Normativo

La Política de Seguridad de la Información se sitúa dentro del marco jurídico definido por la legislación y normativa vigente, relacionada directa o indirectamente con el tratamiento de la información mediante métodos automatizados y con la seguridad de la información.

Se ha diseñado con un espíritu duradero y práctico, de cara a contemplar nuevas normativas que puedan surgir de forma posterior a su entrada en vigor.

Es de aplicación toda la legislación y normativa vigente, tanto estatal como europea, en relación con la protección de datos personales, propiedad intelectual y uso de herramientas telemáticas.

La Política y la Normativa de Seguridad de la Información son el resultado de un análisis de requisitos e investigación en materia seguridad de la Información, utilizando como referencia algunos de los siguientes estándares:

- ISO/IEC 27001 (Information technology - Security techniques - Information security management systems- Requirements).
- ISO/IEC 27002 (Information technology – Security techniques – Code of practice for information security management).
- Reglamento General de Protección de Datos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

6. Organización de la Seguridad

La seguridad de los activos de la información es responsabilidad de todos los departamentos de la empresa, así como de todas y cada una de las personas que interaccionen con los mismos.

La Dirección designará los puestos y las personas concretas que deberán llevar a cabo las funciones relacionadas con la seguridad de la información, y en especial las figuras organizativas descritas en el presente apartado.

La Dirección de Danobatgroup definirá la siguiente organización para garantizar la seguridad de la información y de los activos relacionados con esta:

- El Comité de Seguridad será el encargado de realizar la revisión, al menos de forma anual, de la Política de Seguridad de la Información. Además, cuando sea necesario, se encargará de desarrollar normativas para su aprobación por parte del Comité de Dirección de Danobatgroup. Tendrá la responsabilidad de establecer los medios necesarios para que tanto la Política como la Normativa sean conocidas por todos los afectados.

  Este Comité estará compuesto por representantes del departamento de Informática (tanto del área de sistemas como del área de aplicaciones), figuras necesarias para coordinar las iniciativas de seguridad de la información. Asimismo, este Comité, contará con miembros permanentes y miembros invitados en función de la situación y los condicionantes de seguridad de la información.

- La persona Responsable de Seguridad de la Información establecerá los requisitos de la información en materia de seguridad, siendo responsable sobre el uso que se haga de la información relacionada con su ámbito de actuación, así como de su protección.

  Podrá designar a una o varias personas competentes para ejercer las funciones relacionadas con los requisitos de seguridad de la información.

  También adoptará las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios, verificando que las medidas de seguridad establecidas sean adecuadas para la protección de los mismos y manteniendo el nivel de seguridad de la información dentro de su ámbito de actuación.

  Asimismo, se encargará de promover la realización de revisiones periódicas que verifiquen el cumplimiento de las obligaciones en materia de seguridad de la información, así como de promover la

formación y concienciación en el departamento o departamentos bajo su responsabilidad.

7. Objetivo(s) de la seguridad de la información

El objetivo principal es la obtención de la certificación de la norma ISO/IEC 27001 por lo que se deberán tener diferentes indicadores que podrán dar una medición real de cómo está el proceso de implantación en Danobatgroup de dicha norma.

El desarrollo de objetivos se realizará dentro del informe de la revisión por la dirección donde se irá indicando la evolución de dicho(s) objetivo(s) e indicador(es).

8. Principios básicos de seguridad

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos y, en su defecto, prevalecerá la decisión adoptada por el Comité de Seguridad de la información de Danobatgroup.

Se establecerá medidas de seguridad para garantizar los niveles necesarios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de la información sobre los sistemas de información, constituyendo un conjunto de mecanismos de prevención, detección y recuperación. Estas medidas se basarán principalmente en el estándar ISO/IEC 27002.

8.1 Gestión de riesgos

Se proporcionará las herramientas y medios necesarios, para llevar a cabo un proceso de análisis y gestión de riesgos sobre los activos de información y los sistemas que los soportan.

Asimismo, facilitará la evaluación del riesgo asociado a las amenazas de todos los activos estratégicos sujetos a la presente Política de Seguridad de la Información, y la valoración del impacto que se materializaría en caso de que se produjera un incidente de seguridad.

Dicho proceso de gestión de riesgos se basará en las iniciativas de gestión de activos, usando el inventario de estos como base para el alcance de la evaluación y gestión de riesgos.

8.2 Organización interna de la seguridad de la información

Se establecerá un modelo organizativo que permita una adecuada gestión de la seguridad de la información. La gestión de la seguridad deberá tener como objetivo el establecimiento de un marco de control que determine las directrices de actuación oportunas (preventivas, de detección y reactivas) que protejan el valor de la información y garantice la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y conservación de esta.

8.3 Seguridad de los Recursos humanos

La Dirección establecerá medidas de seguridad de la información para todo el personal a su servicio. Dichas medidas se compartirán con todas las personas que colaboren directa o indirectamente con Danobatgroup.

Asimismo, se hará uso de planes de formación y concienciación en materia de seguridad de la información con el objetivo de promover una cultura de seguridad entre las personas que vean su actividad profesional vinculada con Danobatgroup.

8.4 Gestión de activos

Se deberá establecer las directrices generales que definan las reglas básicas a seguir durante el proceso de clasificación e inventariado de activos.

8.5 Control de acceso

Se dispondrá de los mecanismos suficientes de control de acceso a sus activos, tanto de forma local como remota, contemplando entre otras medidas la segregación de funciones y la responsabilidad de los usuarios. Estos controles de acceso deberán ser tanto físicos como lógicos.

8.6 Cifrado

Se establecerán las medidas necesarias para garantizar la protección de la información sensible mediante el uso de mecanismos criptográficos seguros.

8.7 Seguridad física

La Dirección establecerá medidas de seguridad física para la detección y prevención de amenazas en los centros de proceso de datos y las oficinas bajo su responsabilidad. Se deberán realizar revisiones periódicas, al menos con carácter anual, de la adecuación de dichas medidas de seguridad físicas.

Asimismo, se contará con medidas de reacción y respuesta ante amenazas de origen físico. El objetivo principal, en todo caso, deberá ir orientado a la

salvaguarda de la integridad de las personas que puedan encontrarse en cualquier instalación de Danobatgroup.

8.8 Gestión de las comunicaciones y las operaciones

Se establecerá medidas de seguridad para la correcta implantación de la seguridad en la red y las comunicaciones, comenzando por un correcto diseño de la red y un posterior establecimiento de controles de acceso a los servicios y las comunicaciones.

8.9 Seguridad operativa

Se deberá definir e implantar, las medidas de seguridad necesarias para permitir y garantizar un control adecuado de los sistemas y servicios.

8.10 Adquisición, desarrollo y mantenimiento

Previamente a la adquisición de sistemas y servicios se establecerán medidas de seguridad para definir los requisitos y/o controles que garanticen la idoneidad desde la perspectiva de seguridad de la información.

Se deberá mantener un adecuado entorno de control en aquellos elementos e infraestructura tecnológica que soporten el desarrollo de aplicaciones y sistemas. Deberá encontrarse estrictamente controlada la implantación de sistemas y servicios en los entornos de producción con el fin de garantizar su adecuado funcionamiento.

8.11 Gestión de incidentes

Se contará con un proceso de gestión de incidentes de seguridad ágil y operativo para aquellos casos en los que se pudiera materializar un incidente de seguridad de la información.

Dicho proceso se evaluará periódicamente para garantizar su eficacia e incluirá las medidas organizativas y técnicas necesarias de cara a salvaguardar la integridad de los activos de Danobatgroup, así como sus responsabilidades para con los interesados.

8.12 Gestión de continuidad, recuperación y respaldo.

Se diseñará e implementará planes de contingencia y continuidad de negocio que establezcan las acciones necesarias a llevar a cabo en caso de que se produzcan incidentes de seguridad de la información que afecten a la interrupción de los servicios prestados por la compañía.

8.13 Cumplimiento.

Se cumplirá en todo momento la legislación aplicable, así como sus obligaciones reglamentarias o contractuales. Para garantizar dicho cumplimiento se implantarán las medidas de seguridad que sean necesarias y se evaluarán y actualizarán de forma periódica.

9. Obligaciones del personal

El personal que participe en Danobatgroup, como aquellas personas que dispongan de alguna vinculación profesional directa o indirecta con la compañía, deberán cumplir con la presente Política de Seguridad de la Información y sus Normativas aplicables, en su ámbito de actuación.

Los órganos responsables en materia de seguridad de la información garantizarán el acceso a la información necesaria para el conocimiento y correcto cumplimiento por parte de los afectados. Para ello, la persona responsable de Seguridad llevará a cabo sesiones de formación y concienciación que faciliten la comprensión de las medidas establecidas en la Política y Normativa de Seguridad de la Información.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de la Política y de la Normativa de Seguridad aplicable a dichos servicios y/o información.

El incumplimiento manifiesto de la Política o Normativa de Seguridad ya sea por personal interno o vinculado a la compañía, podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

Cualquier excepción a la Política o Normativa de Seguridad de la Información deberá ser precedida de un informe de los riesgos asociados, que deberá ser aprobado por la Dirección.

10. Terceras partes

Cuando Danobatgroup preste servicios o maneje información de otras organizaciones, se les hará partícipe de esta política. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Danobatgroup utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta política y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe de la persona Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los/as responsables de los servicios y la información afectados antes de seguir adelante.

11. Desarrollo de la política de seguridad

Esta Política se complementa con el Sistema de Gestión de Seguridad de la Información (SGSI) por medio de la diversa normativa y recomendaciones de seguridad (políticas, normativas, procedimientos, etc.) que contiene, de acuerdo con las buenas prácticas de la norma ISO 27001.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

12. Actualización de las políticas de Seguridad

Esta Política habrá de mantenerse actualizada en el tiempo. Para ello debe revisarse de forma ordinaria con periodicidad anual, y de forma extraordinaria, cada vez que se produzcan variaciones en los objetivos estratégicos o legislación aplicable, procediéndose a presentar una propuesta de modificación por parte del Comité de Seguridad.

13. Comunicación y difusión

Los cambios realizados en esta Política se divulgarán a todas las personas y partes interesadas destinatarias según lo recogido en esta, utilizando los medios que se consideren pertinentes. Cada una será responsable de su lectura y conocimiento, así como de las restantes Políticas de Seguridad de Danobatgroup.