Política de Seguridad de la Información

CONTROL DE LAS MODIFICACIONES DEL DOCUMENTO

Versión	Fecha	Aprobado	Control de cambios
1.0	21/04/2023		Creación del documento
1.0	29/05/2023	Sí	Aprobado en Comité de Seguridad
2.0	21/10/2024		Se añade rol de CISO

Contenido

1. OBJETO 3
   1.1 ALCANCE 3
2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 3
   2.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 3
   2.2 ANÁLISIS Y GESTIÓN DEL RIESGO 5
   2.3 OBLIGACIONES DE LOS USUARIOS 5
3. REVISIÓN DE LA POLÍTICA 6
4. INCUMPLIMIENTO DE LA POLÍTICA 6
5. CONSIDERACIONES ADICIONALES 6

1. OBJETO

Este documento establece la Política de Seguridad de la Información aprobada por la Dirección de DONTE GROUP de acuerdo con los diferentes Estándares, Normas y Leyes relativas a la seguridad de la información.

Esta política estará disponible y será distribuida entre todas las partes interesadas.

El objetivo de la Seguridad de la Información es diseñar, implementar y monitorizar un conjunto efectivo de medidas para minimizar los riesgos de comprometer la confidencialidad, integridad y disponibilidad de los datos e información de la empresa, así como asegurar el cumplimiento de esta por terceras partes y, a su vez, garantizar que cumplen con la responsabilidad que aceptan al tratar información confidencial de la empresa.

1.1 ALCANCE

Esta política se refiere a la información de la empresa de cualquier tipo, incluyendo todos los contenidos, informaciones, ficheros almacenados, información temporal, incluyendo la información que se almacene en herramientas facilitadas al usuario por parte de la empresa, como ejemplo y de manera no excluyente el correo electrónico empresarial, ordenadores, equipos portátiles, smartphones, tabletas, sistemas de información, dispositivos y sistemas almacenamiento, equipos de impresión, y cualquier información comunicada mediante los sistemas de información de la empresa.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es necesario que DONTE GROUP tenga una Política de Seguridad de la Información que establezca los requisitos mínimos de control de seguridad administrativo, técnico y físico. Es por ello por lo que:

1. Cada área de la empresa ha adoptado y se ha adherido a la Política de Seguridad de la Información.
2. La política se ha comunicado por la empresa de forma relevante, accesible y comprensible.

Cuando un requisito no pueda cumplirse, se realizará una Excepción de Seguridad de la Información, que deberá disponer de una solución alternativa con los controles mitigantes de seguridad de la información y obtener la aprobación del Departamento de Sistemas para aceptar el riesgo y la validación del Comité de Seguridad ordinario o extraordinario.

2.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La estructura organizativa apoya las políticas de seguridad de la información. Por ello:

- Se han establecido dos foros para la gestión de la seguridad y la privacidad de la información sensible y/o confidencial de la empresa. Por un lado, el Comité

Ejecutivo autorizado a proporcionar un apoyo claro y visible a las iniciativas de seguridad de la información y, por otro lado, el Comité de Seguridad.

- El responsable de Seguridad de la Información (CISO), o en su defecto, el Chief Information Officer (CIO), han sido designados como responsables del cumplimiento de la Política de Seguridad de la Información.
- Las responsabilidades de la seguridad de la información se han definido, asignado y comunicado y se encuentra estructurada en los diferentes roles **y/o áreas del Departamento de Sistemas:**
    - **CISO (Chief Information Security Officer)** es la persona responsable de la seguridad de la información en una organización. Su rol se centra en proteger los activos digitales, datos sensibles y sistemas informáticos contra amenazas cibernéticas, fraudes y accesos no autorizados. Entre sus principales funciones destacan:
        - Desarrollo de políticas de seguridad: El CISO crea y mantiene las políticas y procedimientos de seguridad que guían la protección de los activos tecnológicos.
        - Evaluación de riesgos: Identifica, analiza y prioriza los riesgos de seguridad, estableciendo controles para mitigar posibles ataques o vulnerabilidades.
        - Cumplimiento normativo: Asegura que la empresa cumpla con leyes y regulaciones de seguridad, como GDPR o normas sectoriales como ISO/IEC 27001.
        - Gestión de incidentes: Lidera la respuesta ante incidentes de ciberseguridad, coordinando las acciones de contención, remediación y recuperación.
        - Concienciación y formación: Promueve la educación interna sobre buenas prácticas de seguridad entre empleados.

      CISO actúa como enlace entre la alta dirección y el equipo técnico, asegurando que la ciberseguridad esté alineada con los objetivos estratégicos de la organización.
    - **Seguridad de la explotación tecnológica:** Liderar la seguridad operacional de los sistemas de información, atendiendo a los estándares de seguridad nacionales e internacionales, así como la gestión de las identidades privilegiadas. También se tendrá en cuenta la seguridad en entornos cloud, minimizando en la medida de lo posible cualquier riesgo que pueda impedir o limitar el continuo y correcto funcionamiento de la operativa diaria y, en caso de producirse dicha situación, restablecer la normalidad funcional con la mayor rapidez posible.
    - **Gobierno y cumplimiento normativo IT:** Diseñar y aprobar la certificación de controles de ciberseguridad, orientados a brindar la correcta cobertura ante los riesgos asociados al cumplimiento normativo y supervisar el cumplimiento de lo dispuesto en el reglamento de protección de datos y todas las disposiciones de protección de datos que resulten exigibles.
    - **Gestión del riesgo y Continuidad de Negocio:** Definir a nivel tecnológico un modelo de gobierno capaz de establecer los principios

DONTE GROUP
Cuidamos tu salud bucodental
Parque Empresarial La Finca, 28223 Pozuelo de Alarcón, Madrid, España
+(34) 91 375 65 60 dontegroup.com

básicos y pautas de actuación que se deben seguir en la gestión del riesgo tecnológico, información y comunicación. Asimismo, deberá garantizar la gestión de crisis, la continuidad de negocio y la resiliencia de la organización, así como el cumplimento de la regulación correspondiente y del buen gobierno corporativo. Incluyendo además la gestión de identidades corporativa.

- **Gestión de vulnerabilidades:** Detección, gestión y corrección de las vulnerabilidades encontradas en los sistemas de información y comunicaciones de la empresa. Los sistemas de información de la empresa están monitorizados de manera automática y permanente, reservándose al departamento de Ciberseguridad la facultad de acceder, intervenir, investigar, interceptar o revisar el contenido de las comunicaciones en caso de alerta - una vez recibidas y abiertas por sus destinatarios -, así como cualquier fichero o información almacenados en cualquier dispositivo de la empresa, de conformidad con la normativa interna vigente. Esta revisión será realizada siempre con las debidas garantías para no afectar a los derechos y libertades de los usuarios.

2.2 ANÁLISIS Y GESTIÓN DEL RIESGO

Todos los sistemas de información de la empresa serán objeto de análisis de riesgos, que deberá repetirse de forma periódica y cíclica. Los análisis de riesgos, además, se actualizarán en caso de:

- Identificación de nuevos activos de información y/o cambio total de los existentes o sus requisitos de seguridad.
- Identificación de cambios en relación con los servicios prestados.
- Cuando ocurra un incidente grave de seguridad, o se identifiquen o reporten vulnerabilidades de seguridad graves en los sistemas existentes.

Las decisiones sobre las medidas, proyectos e iniciativas de seguridad a realizar en la empresa contemplarán los resultados de la evaluación de riesgos existentes en relación con la seguridad de la información sobre los sistemas utilizados. Dichos resultados serán elevados por el responsable de Riesgo y Continuidad de Negocio al Comité de seguridad.

2.3 OBLIGACIONES DE LOS USUARIOS

Todos los usuarios de los sistemas de información de la empresa (usuarios internos o externos, proveedores y usuarios de terceras partes), sin excepción, tienen la obligación de conocer y cumplir la Política de Seguridad de la Información y su Marco Normativo, siendo responsabilidad del Departamento de Sistemas el disponer los medios necesarios para que la información llegue a los afectados.

La empresa garantiza la definición y ejecución de las acciones necesarias para la concienciación del personal en relación con los riesgos y amenazas relativos a la seguridad de la información.

3. REVISIÓN DE LA POLÍTICA

Cuando se produzca un cambio significativo en la estructura o en la operativa de DONTE GROUP que afecte a esta política, deberá producirse una modificación y actualización de esta.

4. INCUMPLIMIENTO DE LA POLÍTICA

Cualquier usuario advertido de no respetar las normas establecidas en el Marco Normativo de DONTE GROUP puede estar sujeto a las medidas disciplinarias definidas por las políticas de la empresa y la legislación laboral.

En caso de incumplimiento grave y probado por parte de un usuario, este puede estar sujeto a los procedimientos civiles y/o penales a petición de la empresa y de acuerdo con las leyes vigentes.

5. CONSIDERACIONES ADICIONALES

La Dirección de DONTE GROUP se compromete a impulsar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información mediante el proceso de mejora continua, orientado a garantizar la confidencialidad, integridad y disponibilidad de la información de tal forma que las actividades de la empresa se desarrollen de acuerdo con los requisitos de las partes interesadas, los reglamentariamente establecidos y/o la normativa legal vigente.

Esta política de seguridad de la información se ha desarrollado teniendo en cuenta las siguientes normativas:

- UNE-ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información.
- UNE-ISO/IEC 27002:2022 Código de buenas prácticas para los controles de seguridad de la información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La presente política se aplica a todos los usuarios que traten con información de la empresa, por lo que debe estar a disponible y comunicada a todas las partes interesadas y para ello se aprueba y publica en Madrid, a 22 de diciembre de 2023.

Director General

Chief Information Officer (CIO)