CESUMIN S.L. (en adelante, "la empresa") considera que la información, y los elementos electrónicos para el procesamiento de la misma, son activos críticos que deben ser protegidos para asegurar su correcto funcionamiento.

Por ello, la Empresa ha decidido elaborar una Política de Ciberseguridad (en adelante, "la Política" y/o "la Política de Ciberseguridad"), orientada a gestionar eficazmente la seguridad tanto de la información tratada por los sistemas informáticos de la misma, como de las personas y los activos, tangibles e intangibles, que participan en sus procesos.

1. Definición

La Ciberseguridad consiste en la protección de los activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

2. Objetivos Generales

El objetivo general de la Política de Ciberseguridad es definir y formalizar los marcos generales que ayudarán a la empresa a mitigar los riesgos de la ciberseguridad.

Así, la función de seguridad de la información se entiende como el conjunto de medidas de prevención, detección y reacción ante los riesgos de origen deliberado, y no deliberado, que afecten a la empresa y a todas las personas que la conforman.

3. Ámbito de Aplicación

Esta Política de Ciberseguridad es de aplicación a todos los empleados, directivos y administradores que integran la Empresa, incluyendo aquellas sociedades participadas sobre las que tenga un control efectivo, dentro de los límites previstos en la normativa aplicable.

En aquellas sociedades participadas en las que CESUMIN S.L. no tenga el control efectivo, la empresa fomentará el cumplimiento de los principios y directrices coherentes con los establecidos en esta Política.

De la misma forma, la empresa informará sobre la presente Política, y las medidas adoptadas a su amparo, a todos aquellos terceros facultados a utilizar y/o interactuar con los sistemas de información de la misma, a fin de que, por su parte, en la medida que les resulte posible y exigible, den el mayor cumplimiento a la misma.

4. Principios y Garantías

La presente Política de Ciberseguridad se basa en los siguientes principios básicos:

- Principio de cumplimiento normativo: todos los sistemas de información de la Empresa se ajustarán a la normativa de aplicación legal regulatoria y sectorial que afecte a la seguridad de la información, en especial, aquellas relacionadas con la protección de datos de carácter personal, seguridad de los sistemas, datos, comunicaciones y servicios de transferencia electrónica de información.

- Principio de seguridad y resiliencia: la Empresa garantiza que los sistemas de información y telecomunicaciones de los que dispone, poseen el adecuado nivel de seguridad y resiliencia, e

intentará impulsar dicha implementación en los sistemas y operaciones de terceros que le presten servicios.

- Principio de proporcionalidad: se implantarán controles que mitiguen los riesgos de ciberseguridad, buscando el equilibrio entre las medidas de seguridad, la naturaleza del riesgo y el riesgo identificado.

- Principio de confidencialidad e integridad: se debe garantizar la confidencialidad de la información de tal manera que solo tengan acceso a la misma las personas autorizadas a tal efecto. Así mismo, la información con la que se trabaja debe ser concisa y precisa, garantizándose así su integridad.

- Principio de formación y concienciación: todos los empleados, contratistas y colaboradores recibirán formación acerca de los riesgos de ciberseguridad y se garantizará que dispongan de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad de la Empresa.

- Principio de diligencia: todos los miembros de la empresa deben llevar a cabo conductas diligentes, cumpliendo con las normas y controles establecidos.

- Principio de mejora continua: se garantiza que, de manera recurrente, se revisará la eficacia de los controles de seguridad ya implantados para aumentar la capacidad de adaptación a la constante evolución y riesgo del entorno tecnológico y las nuevas amenazas.

- Principio de colaboración: se colaborará con los organismos, agencias gubernamentales y asociaciones relevantes para la mejora de la ciberseguridad tanto global, como de la Empresa.

5. Gestión y Seguimiento

La empresa dispondrá de un modelo de gestión aplicable a la ciberseguridad basado en la normativa internacional y nacional aplicable, de modo que facilitará, de forma proporcional, todos los medios y recursos necesarios para que la organización disponga de un entorno alineado con los objetivos de negocio y los objetivos de ciberseguridad establecidos.

De esta forma, el modelo definido por la empresa se basa en:

- Establecer mecanismos para alinear los objetivos y metas de la ciberseguridad con la conformidad de los requisitos legislativos, reguladores y contractuales.

- Elaborar un marco para la gestión de las medidas de ciberseguridad aplicables, mediante el establecimiento de una metodología de riesgos aprobada por la Dirección de la empresa, en la que se fijen los objetivos y las metas, alineadas con la estrategia y los objetivos del negocio y que sea coherente con el contexto donde se desarrollan las actividades de la misma.

- Establecer mecanismos para reaccionar frente a los incidentes que se produzcan tanto en la gestión del sistema, como en los procedimientos operativos que dependen del mismo, incluyendo mecanismos para el tratamiento global de las amenazas de ciberseguridad.

- Establecer un organigrama corporativo en el que el conjunto de las funciones y responsabilidades en materia de ciberseguridad queden claramente definidas y asignadas.

- Elaborar un proceso de revisión y actualización continua del modelo de gestión de la ciberseguridad para adecuarlo en todo momento a las nuevas ciberamenazas que van surgiendo y puedan afectar a la empresa.

6. Implementación y Comité de Seguridad de la Empresa

A efectos de proceder con la implementación de la Política, y según correspondan en cada momento de acuerdo con la legislación vigente, llevar a cabo el control, desarrollo, ejecución y revisión del modelo de gestión de la ciberseguridad, la empresa nombrará a un Comité de Seguridad que, al efecto, será designado por el Consejo de Administración de la Sociedad.

7. Revisión, Evaluación y Actualización de la Política

El Comité de Seguridad evaluará, al menos una (1) vez al año, el cumplimiento y la eficacia de esta Política de Ciberseguridad, e informará del resultado al Consejo de Administración de la Sociedad, proponiéndole, en su caso, cualquier actualización, modificaciones y/o revisión que proceda o estimen.

La presente Política Corporativa de Ciberseguridad fue aprobada el 2 de enero de 2021