POLÍTICA
DE CIBERSEGURIDAD

Texto aprobado por el Consejo de Administración
el 25 de enero de 2024.

INDICE

POLÍTICA
DE CIBERSEGURIDAD

1. FUNDAMENTO Y OBJETO

Viscofan S.A ("Viscofan" o "la Sociedad") cuenta con una *Política de control y gestión de riesgos* cuyo objeto es establecer los principios básicos y el marco general de actuación para la identificación, la gestión y el control de los riesgos de toda naturaleza a los que se enfrenta el Grupo Viscofan (indistintamente, el "Grupo Viscofan" o el "Grupo", que comprende el grupo de sociedades respecto de las que Viscofan S.A. es sociedad dominante en el sentido establecido en la ley). Dicha política general se desarrolla en las políticas específicas que puedan establecerse en relación con determinados riesgos del Grupo.

Viscofan considera la información, junto con los sistemas que la sustentan y procesan, uno de sus activos más importantes de su negocio, debido al impacto que puede generar en la propia actividad y organización, empleados, proveedores, clientes y grupos de interés por lo que establece como objetivo fundamental su protección y la gestión efectiva y eficiente de los riesgos a los que se ven sujetos.

En consecuencia, el Consejo de Administración de Viscofan aprueba esta Política de Ciberseguridad (la "Política") de la Sociedad y del Grupo Viscofan, que permita hacer frente a los nuevos retos de Ciberseguridad incorporando las recomendaciones aprobadas en la materia.

La Política establece los principios básicos y el marco general para el control y la gestión de los riesgos de Ciberseguridad a los que está expuesto el Grupo, con el fin de garantizar la protección de su información y de los sistemas que la soportan estableciendo un marco de control que facilite que su información esté disponible, sea íntegra y confidencial y que permita responder de forma adecuada a las amenazas propias de la evolución continua de las tecnologías de la información.

Los objetivos específicos de la Política son:

- Definir los principios que rigen la gestión de la Ciberseguridad del Grupo Viscofan, de forma que éstos protejan la información del Grupo, mitiguen los riesgos de Ciberseguridad a los que se ve expuesta y se encuentren alineados con los requerimientos normativos y regulatorios vigentes.
- Definir y asignar las responsabilidades asociadas a la implantación y mantenimiento de su modelo de gestión.
- Establecer un marco que facilite la toma de decisiones en lo referente a la implantación de medidas de Ciberseguridad, tanto técnicas como procedimentales y organizativas, con el fin de prevenir los siguientes impactos:
    - Daño en la imagen y reputación del Grupo Viscofan.
    - interrupción de los procesos críticos que soportan el negocio.
    - Pérdida o mal uso de los activos de información.

2. ALCANCE

La Política tiene por objeto la protección contra daños por ataques digitales contra la confidencialidad, integridad, disponibilidad, autenticidad, confiabilidad de la información y activos en el ciberespacio. Incluye y no se limita a la organización, la recopilación de recursos, procesos y estructuras para garantizar una seguridad de extremo a extremo en toda la cadena de suministro y se aplica tanto a las Tecnologías de la Información (IT) como a las Tecnologías de Operación OT), a las empresas y empleados del Grupo Viscofan, así como a terceros colaboradores y empresas externas que acceden a los sistemas de información del Grupo.

Se entiende por IT todo el espectro de tecnologías de procesamiento de información, incluyendo software, hardware, tecnologías de comunicación y servicios relacionados, así como los procesos implementados par su soporte y gestión.

Se entiende por OT el hardware, software y sistemas de comunicación utilizados para el control de equipos industriales, que interactúan con el mundo físico de las plantas productivas de Viscofan.

El Grupo tiene la obligación de garantizar, en los mismos términos, la seguridad de la información que concierne a sus clientes, entidades colaboradoras y a los organismos oficiales competentes.

3. DESARROLLO DE LA POLÍTICA

La Política se complementa con un segundo nivel normativo para la gestión de la Ciberseguridad, adecuado para dar respuesta a las amenazas actuales y emergentes, así como a los requerimientos regulatorios y estará integrado por las normas generales de Ciberseguridad procedimientos, manuales operativos y guías técnicas (el "Cuerpo Normativo de Ciberseguridad").

El Cuerpo Normativo de Ciberseguridad es revisado regularmente, al menos una vez al año, así como tras cambios significativos que afecten al entorno de la Ciberseguridad del Grupo y/o a las circunstancias de su negocio.

4. PRINCIPIOS DE ACTUACION Y COMPROMISOS

Los principios y compromisos que rigen la gestión de la Ciberseguridad en el Grupo Viscofan son los siguientes:

- Planificación. - Definir planes a corto, medio y largo plazo que aseguren la visión de futuro y mejora continua de la Ciberseguridad, permitiendo reducir su exposición al riesgo dentro de los niveles de tolerancia definidos.
- Evaluación del riesgo.-. Evaluar por anticipado los riesgos en materia de Ciberseguridad en las actividades y operaciones, adoptando las medidas de gestión que se consideren necesarias en función de su nivel de riesgos y se tomarán decisiones en materia de Ciberseguridad en función del riesgo real de la materialización de las amenazas sobre la organización.
- Gestión de incidentes y resiliencia. - Asegurar la continuidad de la capacidad operativa para los fines de la organización y la de los grupos de interés que puedan verse afectados por sus actividades.

- Monitorización. - Implantar un sistema de monitorización, detección y alerta temprana que permitan una identificación permanente y continuada de las vulnerabilidades, nuevas amenazas e incidentes a nivel global, así como definir los mecanismos oportunos para asegurar que las personas encargadas de la protección de los activos, infraestructuras y/o de sus sistemas de información estén informados de dichas incidencias en forma y plazo.
- Integridad. - Asegurar la completa integración de los compromisos de Ciberseguridad con los grupos de interés y requerir a proveedores y contratistas principales que puedan acceder a sistemas del Grupo responsabilidad y formación en la materia, previo al comienzo de la relación contractual efectiva.
- Formación. - Fomentar la formación, concienciación y cultura de Ciberseguridad en toda la organización con el objetivo de capacitar a su personal acerca de los hábitos y prácticas recomendables para prevenir y mitigar riesgos en el ámbito de la Ciberseguridad
- Continuidad. - Establecer procedimientos y responsabilidades de respuesta inmediata, eficaz y ordenada ante incidentes de Ciberseguridad, así como planes de contingencia y continuidad específicos.
- Cumplimiento normativo. - Garantizar el cumplimiento de las leyes y regulaciones aplicables en materia de Ciberseguridad en todos aquellos países en los que opera el Grupo. Viscofan colabora con las autoridades y organismos competentes para contribuir a la mejora de la Ciberseguridad.
- Mejora Continua. - Viscofan se apoyará en reconocidos estándares, nacionales, europeos e internacionales, adecuados a sus necesidades, para un mejor seguimiento de la evolución de su madurez en la materia.

5. ORGANIZACIÓN DE CIBERSEGURIDAD

5.1 Alta Dirección

La Ciberseguridad es una función cuya responsabilidad se ejerce a partir del máximo nivel jerárquico de la organización correspondiendo:

- Al Consejo de Administración la aprobación de la Política y su seguimiento, asegurando que los órganos con responsabilidad en la consecución de los objetivos establecidos disponen de suficientes capacidades materiales y humanas para poder llevar a cabo las funciones asignadas de forma efectiva y eficiente.

- A la Comisión de Auditoría, por delegación del Consejo de Administración, corresponderá la supervisión ejecutiva de la aplicación de la Política y especialmente la validación previa de los Planes y objetivos de Ciberseguridad del Grupo y el seguimiento periódico de los informes del CISO.

- La Alta Dirección asume el compromiso de promover e impulsar, bajo la responsabilidad del Director de Seguridad de la información (o Chief Information Security Officer, en adelante CISO) la implantación de los sistemas de gestión de la Ciberseguridad en sus respectivas áreas de responsabilidad y, en particular, el seguimiento de los riesgos de Ciberseguridad a través del Comité Global de Riesgos del Grupo.

5.2 Comité de Ciberseguridad y CISO

No obstante, de las responsabilidades de la alta dirección, existirá un Comité de Ciberseguridad que tiene como función esencial la definición, impulso y control de la Ciberseguridad y que participará en la toma de decisiones y estrategias en este ámbito.

El Comité de Ciberseguridad estará integrado por el CISO y un número adecuado de áreas de la organización para adoptar cualquier resolución, con relevancia en materia de seguridad de la información, que pueda afectar sustancialmente a la actividad de la organización.

La gestión ordinaria y ejecución de las medidas anteriores corresponde, por delegación del Comité de Ciberseguridad al CISO, que deberá reunir el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización. El CISO contará con suficientes capacidades y recursos, materiales y humanos, para la consecución de sus objetivos. Dependerá funcionalmente del Director Corporativo de Estrategia, Organización y Sistemas de la Sociedad garantizándose la debida independencia respecto de los responsables de sistemas de redes y de información.

5.3 Responsabilidades locales de Ciberseguridad

En cada una de las filiales del Grupo Viscofan se designará un responsable local en Ciberseguridad que, bajo de la Dirección del CISO, desarrolle las funciones de coordinación en la implantación y supervisión de la Política y del Cuerpo Normativa de Ciberseguridad.

5.4 Empleados y colaboradores

No obstante, las responsabilidades anteriores, todo empleado del Grupo Viscofan es responsable de cumplir con los requisitos de Ciberseguridad dentro del ejercicio de sus funciones, de tal forma que exista una corresponsabilidad compartida entre empleados, directivos, colaboradores y la organización de Ciberseguridad. Particularmente, deberá cumplir debidamente las actividades formativas que se promuevan en la organización.

6. GESTIÓN DE RIESGOS E INCIDENTES Y REPORTE

6.1 Gestión de riesgos e incidentes

El Cuerpo Normativo de Ciberseguridad impulsará el análisis de los riesgos, incluyendo la clasificación de activos y vulnerabilidades, clasificando los incidentes potenciales en función de su impacto, tanto en el ámbito de las Tecnologías de la Información (IT) como industrial o de las Tecnologías de Operación OT) con el fin de determinar los planes de mitigación así como la intervención y aplicación de los comités y protocolos de gestión de crisis existentes en el Grupo con el fin minimizar el impacto en el negocio y asegurar el cumplimiento regulatorio y la adecuada comunicación interna o externa.

Se dispondrá de las capacidades que permitan a la organización ser resiliente para asegurar la continuidad de las operaciones y la recuperación completa de los servicios en un plazo adecuado de tiempo que se determinará en el plan de continuidad de negocio.

6.2 Reporte e informes periódicos

El Consejo de Administración, directamente o a través de la Comisión de Auditoría, hará un seguimiento regular de la Ciberseguridad, incluyendo este tema en el orden del día de sus reuniones. Particularmente:

- Cuando en el orden del día de las reuniones del Consejo de Administración figure algún tema que pueda afectar a la Ciberseguridad, se tendrán que tratar las repercusiones que tenga la Ciberseguridad en el referido tema como, por ejemplo: grandes iniciativas de transformación digital, implementación de nuevas tecnologías y grandes inversiones en activos tecnológicos, fusiones y adquisiciones, expansión de instalaciones o grandes actualizaciones.

- El Comité de Ciberseguridad a través del CISO informará a la Comisión de Auditoría de las ciber amenazas que podrían afectar a los objetivos de la organización. Para ello, se tendrán en cuenta, al menos, los principales actores y las principales y más recientes ciber amenazas, considerando su potencial impacto sobre las operaciones de la organización. En todo caso deberá presentar su informe de actividad de forma semestral a la Comisión de Auditoría y debe contener al menos el estado de la Ciberseguridad, la evolución del grado de madurez y del ciber riesgo, la evolución de las amenazas, la asignación de los recursos destinados a la seguridad de las redes y los sistemas de información, los incidentes significativos gestionados si los hubiera, el estado de la seguridad de las operaciones de la cadena de suministro que dependan de terceros, así como cualquier resolución con relevancia en materia de Ciberseguridad adoptada por el equipo directivo que pueda afectar sustancialmente a la actividad de la organización. El CISO también deberá reportar, en su caso, cualquier obstáculo o impedimento que pudiera restringir el adecuado desempeño de su actividad.

7. CONTINUIDAD

Se practicarán pruebas periódicas completas que pongan a prueba los mecanismos de resiliencia de la organización como parte de los planes de Ciberseguridad. En este contexto se realizarán pruebas del plan de continuidad de negocio, así como simulaciones y ejercicios de preparación de los comités de gestión de crisis.

En general, las compañías deben ejecutar de forma sistemática simulacros y pruebas efectivas de las distintas medidas de protección, respuesta y recuperación. Estos ejercicios han de implicar a toda la organización, con especial atención a los procesos críticos de la compañía, incluida la cadena de suministro.

8. AUDITORÍA

Se realizan periódicamente auditorías independientes, por parte de Auditoría Interna o a través de empresas externas, ya sean de carácter total o parcial con el objetivo de verificar el grado de cumplimiento de la Política y así como de reglas previstas en manuales y procedimientos que integran el Cuerpo Normativo de Ciberseguridad del Grupo Viscofan.

9. VIGENCIA Y REVISONES

La Política entrará en vigor el siguiente día hábil a su aprobación del Consejo de Administración a propuesta de la Comisión de Auditoría de la Sociedad. Su vigencia se mantendrá mientras no sea modificada o derogada por otra posterior.

Desde su entrada en vigor, se dispone de 6 meses para adecuar las incompatibilidades con lo dispuesto en la Política que puedan existir en otras normas, tanto globales como locales.

La Política se revisará periódicamente y en función de los cambios organizativos, legales o de negocio que se produzcan en cada momento, con el fin de mantener su pertinencia, suficiencia y eficacia.

Esta Política está disponible en la Intranet para todos los empleados y en la web corporativa para todos los grupos de interés de la Sociedad.