Política de Ciberseguridad

Fibra Danhos

Administradora Fibra Danhos

INTRODUCCIÓN

Fibra Danhos (FD) es un Fideicomiso mexicano constituido principalmente para desarrollar, ser propietarios de, arrendar, operar y adquirir activos inmobiliarios comerciales icónicos y de calidad premier en México.

Administradora Fibra Danhos (AFD) es una sociedad subsidiaria de Fibra Danhos (FD), que, a través del Contrato de Administración celebrado con el Fiduciario conforme a las instrucciones del Comité Técnico del Fideicomiso, está facultada para realizar todos los actos necesarios o convenientes para el cumplimiento de los fines del Fideicomiso, incluyendo la contratación de personal y la relación contractual con proveedores y prestadores de servicios.

AFD, considera que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la empresa.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de FD y AFD, así como los activos que participan en sus procesos.

Esta Política tiene como objetivo garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre la los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Esta política de ciberseguridad es de aplicación a todos los empleados, directivos y administradores de todas las sociedades que integran AFD, dentro de los límites previstos en la normativa aplicable.

PRINCIPIOS BÁSICOS

Para ello se establecen los siguientes principios básicos:

- Garantizar que los Sistemas de Información y Telecomunicaciones que dispone FD y AFD poseen el adecuado nivel de ciberseguridad y resiliencia.

- Sensibilizar a todos los empleados, contratistas y colaboradores acerca de los riesgos de ciberseguridad y garantizar que disponen de los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para sustentar los objetivos de ciberseguridad de AFD.

- Potencializar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a nuevas amenazas.

- Impulsar la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que presten servicios a FD y AFD.

- Establecer procedimientos y herramientas que permiten adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y nuevas amenazas.

- Colaborar con los organismos y agencias gubernamentales relevantes para la mejora de la ciberseguridad, el cumplimiento de la legislación vigente y la contribución a la mejora de la ciberseguridad en el ámbito internacional.

MODELO DE GESTIÓN

AFD dispone de un modelo de gestión aplicable a la ciberseguridad basado en la normativa internacional y nacional, para detectar amenazas y obtener los recursos necesarios para cumplir con los objetivos de ciberseguridad establecidos.

El modelo definido por AFD se basa en:

- Un marco para la gestión de las medidas aplicables mediante una metodología de riesgos aprobada por la dirección en la que se fijen los objetivos y metas de ciberseguridad, así como los principios alineados con la estrategia de negocio y coherente con el contexto dónde se desarrollan las actividades de FD y AFD.

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

- 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.

- La existencia de un conjunto de funciones y responsabilidades en materia de ciberseguridad claramente definida y asignada en el organigrama corporativo.

- Mecanismos para el tratamiento global de las amenazas de ciberseguridad incluyendo todas las actividades oportunas para el tratamiento de la seguridad.

- Un proceso de revisión y actualización continua del modelo de gestión de ciberseguridad para adecuarlo en todo momento a las ciberamenazas que van surgiendo y puedan afectar a FD y AFD.