TLP:CLEAR

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Propósito

La información es uno de los activos más críticos para Global Exchange, por lo que es fundamental instaurar una serie de medidas en todos los lugares donde se almacene, transmita o procese la misma. El propósito de la Política de Seguridad de la Información de Global Exchange es asegurar la confidencialidad, integridad y disponibilidad de los datos para cumplir con las obligaciones y mejores prácticas en materia de seguridad de la información en el desarrollo de sus actividades.

Objetivo

La presente política tiene como objetivo principal definir las medidas que sean necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información gestionada por el Grupo Global Exchange.

La presente política se especificará y desarrollará a través de normas, guías, estándares, manuales, planes y procedimientos, que se irán actualizando cuando sea necesario en función de las nuevas exigencias impuestas por los avances de la tecnología y el negocio.

La política de seguridad de la información ha sido creada tomando como referencia los principales marcos de seguridad de la información, normativas y reglamentaciones tanto locales como internacionales, entre los que destacan:

- ISO/IEC 27001
- ISO/IEC 22301
- ISO/IEC 31000
- Esquema Nacional de Seguridad (ENS)
- Reglamento de Resiliencia Operativa Digital (DORA)
- Legislación nacional e internación sobre Ciberseguridad
- Legislación nacionales e internacional sobre Protección de Datos (RGPD, LOPDGDD)
- Legislación nacional e internacional sobre Propiedad Intelectual
- Legislación sobre Sociedad de la Información y Comercio Electrónico
- Legislación sobre Seguridad en las Redes y Sistemas de Información

Principios

La política de seguridad de la información de Global Exchange se desarrollará, con carácter general, de acuerdo con los siguientes principios:

- **Principio de confidencialidad:** los activos pertenecientes a las tecnologías de la información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respecto a las obligaciones de secreto y sigilo profesional.
- **Principio de integridad y calidad:** se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.
- **Principio de disponibilidad y continuidad:** se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.
- **Principio de trazabilidad:** se implementarán medidas para asegurar que en todo momento se pueda determinar quién hizo qué y en qué momento con el fin de tener capacidad de análisis sobre los incidentes de seguridad detectados.
- **Principio de gestión del riesgo:** se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.
- **Principio de concienciación y formación:** se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad de la información de todas aquellas personas que precisen ser objeto de ella.
- **Principio de prevención:** se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad de la información.
- **Principio de mejora continua:** se revisará el grado de eficacia de los controles de seguridad de la información implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de Global Exchange.
- **Principio de mínimo privilegio:** indica que, en una particular capa de abstracción de un entorno computacional, cada parte debe ser capaz de acceder solo a la información y recursos que son necesarios para su legítimo propósito.
- **Principio de necesidad de saber:** su objetivo es garantizar que sólo las personas autorizadas accedan a la información o a los sistemas necesarios para desempeñar sus funciones.
- **Principio de Zero Trust:** el principio de Zero Trust (confianza cero) establece un modelo de seguridad de confianza cero "nunca confíes, siempre verifica", lo que significa que no se debe confiar en los dispositivos por defecto.