POLÍTICA

PÚBLICAS DE SEGURIDAD DE LA INFORMACIÓN,
CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

SEG-PL02

GESTIÓN DE SEGURIDAD Y CONTINUIDAD

2025

TABLA DE CONTENIDO

OBJETIVO

Dar a conocer a las partes interesadas de **IFX** el acápite del documento SEG-PL01 Políticas Generales de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad en el cual se define el objetivo:

"Establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, ciberseguridad y protección de la privacidad (SGSI) robusto y eficaz, alineado con la ISO 27001:2022, que garantice la confidencialidad, integridad y disponibilidad de la información, protección de datos personales, protegiendo los activos de información de la organización y cumpliendo con los requisitos legales y regulatorios aplicables, asegurando el entrenamiento en seguridad de la información para los empleados, para así minimizar los riesgos y asegurar la continuidad de las operaciones, contribuyendo directamente al logro de los objetivos estratégicos de la organización.

Este documento también está alineado al cumplimiento de los objetivos específicos planteados en el documento interno SGI-FR06 planificación de objetivos del SGI (Sistema de Gestión Integral) los cuales se revisan y establecen anualmente, tomando como base esta política, los resultados del análisis de riesgos y los requisitos de las partes interesadas y posterior aprobación del Comité de Ciberseguridad.

ALCANCE

El documento SEG-PL01 Políticas Generales de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad establece las políticas, estándares y requisitos de seguridad de la información, ciberseguridad y protección de la privacidad que deben ser cumplidos por todos los miembros de **IFX**, incluyendo terceros que tengan acceso a información confidencial de la compañía o de sus clientes.

Este marco normativo se aplica a todos los sistemas de información, equipos informáticos y de telecomunicaciones (incluyendo, pero no limitado a, computadoras, servidores, dispositivos móviles y redes) y a todos los procesos que involucren el manejo de información confidencial, tanto interna como de nuestros clientes.

En caso de conflicto entre las políticas de **IFX** y las políticas de nuestros clientes, prevalecerán siempre las normas más restrictivas para garantizar la máxima protección de la información.

DEFINICIONES

Todas las contenidas en la norma ISO/IEC 27000:2018 e ISO/IEC 20000-1:2018.

- **Comité de Ciberseguridad**: Está conformado por el Chief Technology Officer, Regional Director of Engineering, Chief Information Officer, Network and Voice Engineering Manager, Cloud Security Manager, Systems Manager y Security Manager, sesiona con periodicidad mensual.
- **Comité del SGI:** Está conformado por las Gerencias de los procesos de **IFX**, pertenecientes al alcance del SGI.
- **SGI**: Sistema de Gestión Integral.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

POLÍTICAS Y LINEAMIENTOS

A continuación, se listan los lineamientos generales definidos en el documento SEG-PL01 Políticas Generales de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad:

1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

IFX se compromete a establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, ciberseguridad y protección de la privacidad (SGSI) alineado con los requisitos de la norma ISO 27001:2022. Este compromiso se fundamenta en los siguientes principios:

- **Confidencialidad**: Proteger la información de accesos no autorizados.
- **Integridad**: Garantizar la exactitud y completitud de la información.
- **Disponibilidad**: Asegurar el acceso oportuno y continuo a la información autorizada.

Para cumplir con este compromiso, **IFX**:

- **Asignará los roles y responsabilidades** necesarias para la gestión del SGSI.
- **Establecerá un proceso de comunicación efectiva** para difundir las políticas y procedimientos de seguridad.
- **Realizará evaluaciones de riesgos periódicas** para identificar y tratar las amenazas a la seguridad de la información.
- **Implementará controles de seguridad** adecuados para mitigar los riesgos identificados.
- **Fomentará una cultura de seguridad** a través de capacitación y sensibilización a su personal.
- **Realizará auditorías internas** para verificar el cumplimiento del SGSI.

- **Promoverá la mejora continua** del SGSI a través de la revisión y actualización periódica de las políticas y procedimientos.
- **Satisfacer las necesidades** de seguridad de la información, ciberseguridad y protección de la privacidad de las partes interesadas identificadas en el SGI-M01 Manual del Sistema de Gestión Integral (SGI)

La Alta Dirección de IFX revisará periódicamente la efectividad del SGSI y proporcionará los recursos necesarios para implementar, mantener y mejorar continuamente el SGSI.

2. VIGENCIA Y ACTUALIZACIÓN DE LAS POLÍTICAS

La definición, actualización y mantenimiento la SEG-PL01 Políticas Generales de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, es responsabilidad del Gerente de Seguridad y los dueños de proceso de **IFX** a quienes aplique, con la debida aprobación del Comité de Ciberseguridad.

3. POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD PUBLICAS

3.1.1. Relaciones con los proveedores

3.1.1.1. Seguridad de la Información en las relaciones con los proveedores

La Gerencia de Seguridad revisa los requisitos de seguridad de la información relacionados con el acceso de proveedores a los activos de **IFX**, los cuales hacen parte integral del contrato de acuerdo con el alcance del servicio prestado por el proveedor; de acuerdo con la aceptación de la política del SGI para proveedores y contratistas.

La Gerencia de Seguridad de **IFX** incluirá dentro de los acuerdos con los proveedores los requisitos necesarios para mitigar los riesgos de seguridad de la información asociados con la cadena de suministro que impacten la continuidad de la operación o los servicios de tecnología y comunicación.

El acceso a la información y a la infraestructura de procesamiento de información de **IFX** por parte de proveedores, deberá ser solicitado por el área respectiva y autorizado por el Gerente de Seguridad.

Para los proveedores críticos que su ausencia o indisponibilidad total o parcial afecten los servicios CORE de negocio de IFX, es necesario que **IFX** solicite los planes de continuidad estructurados en su organización o certificación de estos donde contemplen el plan de pruebas de cada uno. Lo anterior, para poder asegurar que si algún proveedor se encuentra en contingencia la operación de **IFX** continúa sin impactar el Cliente.

3.1.1.2. Abordar la seguridad de la información en los acuerdos con proveedores

La Gerencia de Seguridad apoyara al área de Compras para efectuar el seguimiento y revisión a la prestación de los servicios de los proveedores dentro del marco de cumplimiento con los requisitos de seguridad de la información establecidos en los contratos.

3.1.1.3. Gestión de la seguridad de la información en la cadena de suministro de las TIC

Con el apoyo de la Gerencia de Seguridad se realizará una reevaluación de los riesgos relacionados con Seguridad de la información que puedan afectar la cadena de suministro de tecnología de información y comunicación (TIC) mediante la metodología de riesgos organizacional definida, la cadena de suministro de las TIC incluye, pero no se limita a los proveedores de:

- Software y hardware.
- Servicios en la nube (IaaS, PaaS, SaaS).
- Servicios gestionados de TI.
- Servicios de telecomunicaciones.
- Servicios de desarrollo y mantenimiento de software.
- Cualquier otro tercero que proporcione productos o servicios de TIC críticos para las operaciones de la organización.

3.1.1.4. Seguimiento, revisión y gestión de cambios de servicios de proveedores

El área o usuario que hace uso del servicio contratado revisará los cambios en el suministro de servicios por parte de los proveedores, basado en la criticidad de la información, los sistemas y procesos del negocio, garantizando que se cumplan los términos y condiciones de seguridad de la información, que los incidentes y problemas de seguridad de la información se gestionen adecuadamente sin afectar la prestación del servicio.

3.1.1.5. Seguridad de la información para el uso de servicios en la nube

El solicitante de servicio, en conjunto con la Gerencia de Seguridad de **IFX**, establecerá los requisitos de seguridad de la información necesarios para el uso de servicios en la nube, basados en la preservación de la confidencialidad, integridad y disponibilidad de la información, y considerando el principio de responsabilidad compartida con el proveedor, también definirán los criterios para la selección del servicio. Con el apoyo la Gerencia de Seguridad de **IFX**, se llevará a cabo una identificación y evaluación de los riesgos que puedan afectar la seguridad de estos servicios en la nube.

3.1.1.6. Seguridad de la información como proveedor de servicios en la nube

IFX como proveedor de servicios en la nube adopta el Modelo de Responsabilidad Compartida para la seguridad de la información, ciberseguridad y protección de los datos. **IFX** gestiona la seguridad "de la nube" (infraestructura), mientras que el cliente gestiona la "seguridad en la nube" (datos, configuración, accesos). Definiendo las siguientes responsabilidades entre IFX y el cliente:

- **IFX** como proveedor de Servicios en la Nube:

- Seguridad de la infraestructura física y de red de gestión.
- Seguridad de los servicios de nube ofertados por IFX.
- Cumplimiento con las normativas y estándares de seguridad aplicables.

- Cliente:

  - Seguridad y controles en la red del cliente.
  - Gestión y protección de los datos y aplicaciones alojados en la nube.
  - Configuración segura de los servicios en la nube.
  - Gestión de identidades y accesos.

3.1.2. Cumplimiento de las Obligaciones Legales y contractuales

IFX cumple con la legislación aplicable propia de las leyes de cada país, las regulaciones generadas por otros entes gubernamentales o nacionales que apliquen y las obligaciones contractuales con colaboradores, proveedores, contratistas y terceros.

En **IFX** está prohibido el uso de software ilegal o no licenciado. Los usuarios que son administradores de sus máquinas son responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo, por lo tanto, deben velar por el buen uso de los recursos asignados.

3.1.2.1. Derechos de propiedad intelectual

IFX cumple con la reglamentación de propiedad intelectual y ejecuta revisiones periódicas para asegurar que se están respetando los derechos de propiedad intelectual.

3.1.3. Privacidad y protección de información de datos personales

En cumplimiento de las regulaciones vigentes de cada país, **IFX** ha adoptado las medidas técnicas y organizativas necesarias para mantener el nivel de seguridad requerido en atención a los datos personales tratados. Así mismo, está dotado de los mecanismos para evitar los accesos no autorizados, sustracciones, modificaciones ilícitas y la pérdida de los datos. **IFX** ha definido, aprobado y publicado las “Políticas de Tratamiento de Datos” desde del 4 de septiembre de 2013 disponible al público en - https://ifxnetworks.com/legal.

3.1.4. Revisiones de seguridad de la información

La Gerencia de Seguridad de **IFX** verifica el cumplimiento de las Políticas de Seguridad apoyado en los líderes de proceso mediante revisiones anualmente al cumplimiento de los procesos y procedimientos, dentro del marco de las políticas, normas y cualquier otro requisito de seguridad aplicable.

3.1.5. Identificación de la legislación aplicable y de los requisitos contractuales

La Gerencia Regional Jurídica identifica y mantiene actualizada la matriz de requisitos legales pertinentes que aplican para la operación de la Compañía.

3.1.6. Acuerdos de confidencialidad o de no divulgación

Todos los colaboradores, contratistas y usuarios deben firmar la cláusula y/o acuerdo de confidencialidad definido por **IFX** y este debe ser parte integral de cada uno de los contratos.

Todos los usuarios de bienes y servicios informáticos de **IFX** deben conducirse de acuerdo con lo establecido en la cláusula y/o acuerdo de confidencialidad, así como aplicar el uso adecuado de los mismos.

El acuerdo de confidencialidad indicado también aplica para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de **IFX** a personas o entidades externas.

3.1.7. Informes de eventos de seguridad de la información

Los colaboradores, contratistas y terceros de **IFX** deben informar inmediatamente al Gerente de Seguridad o al Comité de Ciberseguridad cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, privacidad, integridad y/o disponibilidad de la información mediante correo electrónico a seguridadinformacion@ifxcorp.com.