Política de Seguridad de TI

Nuestro Planteamiento sobre la Seguridad de las Tecnologías de la Información (TI)

F.I.L.A. Group es una de las principales empresas mundiales dedicadas a investigar, diseñar, fabricar y comercializar herramientas para la expresión creativa. La empresa diseña, fabrica y empaqueta herramientas y soportes para dibujar, colorear, pintar y moldear, dirigidas a niños, jóvenes y adultos. Nuestra gama de productos incluye más de 25 marcas conocidas y miles de productos que se venden en todos los continentes.

Estamos comprometidos con un comportamiento responsable hacia todas nuestras partes interesadas en la actividad empresarial, combinando el respeto a las personas, el medio ambiente y las comunidades, por lo que la sostenibilidad está integrada en nuestro Propósito, Visión, Misión, Valores establecidos en nuestro Código Ético, y en nuestras operaciones diarias.

Esta política, junto con nuestro Código Ético y el Modelo de Gobernanza Corporativa, debe ser adoptada por todas las empresas del Grupo y formar parte del Modelo de Organización, Gestión y Control del Grupo, de acuerdo con los principios y objetivos del Modelo de Organización, Gestión y Control según el Decreto Legislativo Italiano 231/2001.

El Grupo protege sus activos corporativos al más alto nivel de sus capacidades técnicas y recursos disponibles, desglosados en los siguientes elementos fundamentales: personas, bienes (activos) e información. La condición necesaria para el desempeño de todas las actividades del F.I.LA. Grupo es la protección de la información gestionada mediante criterios, medidas y controles de seguridad proporcionales a los riesgos y valor de la propia información.

La Seguridad de TI de F.I.L.A Group es un requisito fundamental para garantizar la fiabilidad de la información tratada, así como la eficacia y eficiencia de los servicios prestados por nuestra empresa. La seguridad informática tiene como objetivo primordial la protección de la información, datos personales y conservación digital y de los elementos a través de los cuales se gestionan los datos frente a todas las amenazas, ya sean organizativas o tecnológicas, internas o externas, accidentales o intencionadas, garantizando su confidencialidad, integridad y disponibilidad. y el cumplimiento de la legislación vigente aplicable.

Estamos comprometidos con la seguridad informática, lo que significa tanto proteger "activos" como un sitio, un ordenador o un automóvil, contra las ciberamenazas, como al mismo tiempo minimizar el impacto en el caso de vulnerabilidades que superen las defensas implementadas.

En F.I.L.A Group, los objetivos de seguridad informática pueden resumirse del siguiente modo:

- Confidencialidad; es decir, garantizar la prevención del acceso abusivo o no autorizado a la información, los servicios y los sistemas.
- Integridad; es decir, garantizar que la información no ha sido alterada por accidente o abuso
- **Seguridad**: la información debe conservarse y mantenerse a salvo de cualquier posible amenaza externa, ya sea física o lógica.
- Disponibilidad, o garantizar el acceso a la información y a los servicios de red por parte del personal encargado en relación con las necesidades de trabajo
- Coherencia; es decir, comprobar que existen herramientas que nos permiten comprender si lo que esperamos ocurre realmente
- Control; es decir, tener la capacidad de regular el acceso al sistema de datos y de limitar el acceso y dividir a los usuarios por grupos, funcionalidades, etc.
- Supervisión de las operaciones realizadas; es decir, controles o auditorías.

La falta de un nivel adecuado de seguridad de los datos, en términos de confidencialidad, disponibilidad e integridad, puede tener como consecuencias la pérdida de ventajas competitivas, de imagen, de clientes, de volumen de negocio y, en consecuencia, importantes pérdidas financieras. A todo ello, hay que añadir el riesgo de incurrir en sanciones ligadas a infracciones de la normativa vigente.

Por tanto, la seguridad del sistema de información se obtiene implantando una serie de medidas de seguridad adecuadas, o procedimientos, mecanismos técnicos o prácticas que reduzcan los riesgos a los que están expuestos los activos de información.

Dirigimos nuestras actividades para cumplir con la legislación vigente, con especial referencia a los códigos aplicables en materia de protección de datos personales en todos los países en los que operamos, no sólo para evitar el riesgo de implicación de la empresa, sino sobre todo para garantizar un nivel adecuado de seguridad de los datos personales del Grupo y de su sistema de información.

Nos comprometemos a mantener los estándares éticos más elevados posibles y a cumplir todas las leyes aplicables en todos los países en los que desarrollamos nuestra actividad. Creemos firmemente tener la responsabilidad de operar de acuerdo con las normas de los países en los que estamos presentes, distinguiéndonos como una empresa capaz de exportar los valores que impregnan nuestras acciones, promoviéndolos en las comunidades en las que operamos.

Ámbito de Aplicación de esta Política

Esta política se aplica a F.I.L.A. S.p.A., sus filiales, las entidades en las que posee una participación mayoritaria y las instalaciones que gestiona. Nos comprometemos a colaborar con nuestros socios comerciales y a animarles a respetar los principios de esta política y a adoptar políticas similares en sus empresas.

A nivel local, cada empresa deberá adoptar normas y procedimientos más estrictos, según sea necesario y de conformidad con las leyes y reglamentos locales. Al llevar a cabo sus actividades de gestión, coordinación y supervisión, F.I.L.A. S.p.A. respeta la autonomía de gestión de cada filial dentro de su grupo, gestionando y controlando el negocio en su conjunto, según los intereses legítimos de los accionistas mayoritarios y minoritarios, teniendo en cuenta los requisitos de confidencialidad y las leyes locales aplicables.

Creemos firmemente tener la responsabilidad de operar en conformidad con las normas de los países donde estamos presentes, distinguiéndonos como una empresa capaz de exportar los valores que impregnan nuestras acciones, promoviéndolos en las comunidades donde operamos. El objetivo de esta política es guiar a los directores, funcionarios, empleados, agentes, consultores, intermediarios, empresas conjuntas controladas y otros representantes de terceros de F.I.L.A. para garantizar el cumplimiento de la normativa aplicable y de nuestros valores y políticas.

F.I.L.A. Group se compromete a mejorar continuamente sus políticas y sus programas, facilitando la adopción a nivel local de todos los procedimientos, normas e instrucciones necesarios para que los principios establecidos en esta política sean aplicables y supervisados, con el fin de lograr un impacto. Al adoptar esta política, confiamos en contribuir a una mejor condición de las generaciones actuales y futuras, proporcionando herramientas para una mejor calidad de vida.

Principios Generales

En nuestras estrategias y operaciones, tenemos en cuenta los siguientes principios relativos a la seguridad informática

- **Sistemas de información empresarial:** a los empleados y colaboradores internos se les proporcionan todas las herramientas necesarias para llevar a cabo las tareas asignadas. Las herramientas y aplicaciones de software proporcionadas son herramientas de trabajo y deben utilizarse para estos fines: los datos presentes dentro de las herramientas de trabajo (incluidos los sistemas de correo electrónico y los sistemas de archivos locales/de red, así como las ubicaciones de almacenamiento de datos en la nube) se consideran datos corporativos y, como tales, propiedad de la empresa. En consecuencia, la empresa puede tener acceso completo a los mismos y los usuarios no podrán tener expectativas de privacidad con respecto a la información enviada, recibida o almacenada. Los usos indebidos de los sistemas de la empresa incluyen el procesamiento, la transmisión, la recuperación, el acceso, la visualización, el almacenamiento, la impresión y, en general, la difusión de materiales y datos fraudulentos, acosadores, amenazadores, ilegales, racistas, de orientación sexual, obscenos, intimidatorios, difamatorios o que no sean congruentes con el comportamiento profesional. Por lo tanto, ningún dato de este tipo debe estar presente en la red de F.I.L.A., en los ordenadores personales, dentro de las aplicaciones (como el correo electrónico, los portales Intranet, etc.). Además, los usuarios de los sistemas de la empresa no deben utilizar las infraestructuras para hacer negocios, vender productos o para cualquier otra actividad comercial distinta de las expresamente previstas por la dirección de la empresa.
- **Acceso a la información:** El acceso a la información por parte de cada usuario individual debe limitarse únicamente a la información que necesite para el desempeño de sus funciones (principio de "necesidad de saber"). La divulgación y transmisión de información, tanto interna como externamente, debe basarse en el mismo principio. F.I.L.A Group hará cumplir esta política estableciendo perfiles y derechos de usuario adecuados, para restringir la capacidad de acceso a la información de acuerdo con el principio arriba enunciado. Compartir la información de acceso de los usuarios, como cuentas y contraseñas, con otros empleados o individuos, no mantenerlos almacenados de forma adecuada y segura o no actualizar la información de acceso de forma regular y de acuerdo con las Directrices Operativas de Seguridad Informática, se considera un uso indebido de los sistemas e información de la empresa y, como tal, se sanciona.
-

- **Personal y seguridad:** F.I.L.A Group planifica y lleva a cabo actividades de formación e información dirigidas al personal, con especial atención a la seguridad de la información y al uso correcto de los equipos de la Empresa. Se debe exigir al personal que garantice un nivel mínimo de seguridad para los equipos asignados. El robo, daño o pérdida de herramientas de trabajo debe ser comunicado con prontitud. El personal (incluidos consultores y colaboradores externos) debe firmar cláusulas de confidencialidad.
- **Incidentes y anomalías cibernéticas:** Todos los empleados están obligados a detectar y notificar a quien corresponda cualquier problema relacionado con la seguridad del Grupo y de la empresa. Se requiere y se espera de todos los empleados que lleven a cabo sus actividades diarias y utilicen los sistemas de la empresa (con especial referencia, pero sin limitarse a ellos, a las herramientas de colaboración como el correo electrónico, Microsoft Teams, Microsoft Sharepoint) con el debido cuidado y atención a los mensajes sospechosos, archivos adjuntos, solicitudes de contacto.
- **Seguridad física:** El acceso a los edificios y locales relevantes para la protección de los activos sólo debe tener lugar tras la identificación de las partes autorizadas. La identificación y el diseño de las contramedidas de seguridad física deben tener en cuenta tanto la posibilidad de amenazas físicas como la legislación aplicable. El mantenimiento de los equipos debe realizarse de acuerdo con las instrucciones del fabricante o con procedimientos documentados para garantizar la disponibilidad y la integridad del servicio.
- **Seguridad de TI:** La identificación y el diseño de contramedidas de seguridad de TI deben considerar tanto la posibilidad de intentos de acceso no autorizados internos y externos, como la legislación aplicable y cualquier otra restricción relevante. Los usuarios no deben aprovechar las debilidades o deficiencias del sistema de seguridad de TI para dañar sistemas o datos, obtener recursos para los que no están autorizados, robar recursos de otros usuarios o tener acceso a sistemas para los que no disponen de las autorizaciones necesarias. Por el contrario, los usuarios deberán procurar comunicar al administrador del sistema, por escrito, cualquier disfunción del sistema que pueda sugerir la posible pérdida de estabilidad o fiabilidad del mismo.
- **Comprobaciones:** Los sistemas de información deben comprobarse periódicamente, así como la aplicación de los procedimientos operativos. El personal responsable que trabaja en la división de TI está autorizado a realizar intervenciones en el sistema de TI del Grupo destinadas a garantizar la seguridad y protección del propio sistema, así como por otros motivos técnicos y/o de mantenimiento (por ejemplo, actualización/sustitución/implantación de programas, mantenimiento de hardware, etc.).

Los controles de seguridad que deben realizarse para proteger los recursos informáticos que constituyen su patrimonio se consiguen mediante:

- aplicación y cumplimiento de las políticas en todos los ámbitos organizativos, procedimentales y tecnológicos de forma homogénea con respecto a los objetivos definidos
- la adecuada asignación de tareas y responsabilidades dentro del Grupo para la aplicación de las políticas
- verificación (en el marco del análisis de riesgos informáticos) del nivel de eficacia de las medidas aplicadas, recurriendo también a la evaluación periódica de la vulnerabilidad realizada por partes externas e independientes.

El incumplimiento de las disposiciones de la presente Política de Seguridad de TI será objeto de las sanciones disciplinarias que correspondan.

La alta gerencia de F.I.L.A. juega un papel estratégico en la plena aplicación de esta política, garantizando la implicación de todo el personal y de aquellos que colaboran con F.I.L.A. y la coherencia de su comportamiento con los valores plasmados en dicha política.

Esta política se comunica dentro de la organización y se pone a disposición de todas las partes interesadas en la página web www.filagroup.it.

F.I.L.A. anima a cualquier persona que tenga conocimiento de hechos o comportamientos contrarios al código ético de la empresa, a las políticas y a las normas internas, leyes o reglamentos, a realizar una denuncia con la máxima confidencialidad. F.I.L.A., garantizando la confidencialidad de la identidad del denunciante, ofrece los siguientes canales para presentar una denuncia:

- E-mail: whistleblowing.fila@gmail.com
- Enviar a: odv@fila.it Organismo di Vigilanza, F.I.L.A. Fabbrica Italiana Lapis ed Affini S.p.A. Via XXV Aprile, 5 20016 Pero (MI).

Octubre de 2021

CEO de F.I.L.A. Group – Massimo Candela