Política de Segurança de TI

Nossa abordagem à Segurança da Tecnologia da Informação (TI)

O Grupo F.I.L.A. é uma das empresas líderes mundiais dedicadas à pesquisa, projeto, fabricação e venda de ferramentas para expressão criativa. O Grupo projeta, fábrica e embala ferramentas e suportes para desenho, coloração e pintura, modelagem, para uso por crianças, jovens e adultos. Nossa gama de produtos inclui mais do que marcas conhecidas25 e milhares de produtos vendidos em todos os continentes.

Estamos comprometidos com um comportamento responsável em relação a todas as nossas partes interessadas relevantes na operação dos negócios, combinando o respeito às pessoas, ao ambiente natural e às comunidades, e a sustentabilidade está, portanto, incorporada ao nosso Propósito, Visão, Missão, Valores estabelecidos em nosso Código de Ética e operações do dia a dia.

Esta política, juntamente com nosso Código de Ética e o Modelo de Governança Corporativa, deve ser adotada por todas as empresas do Grupo e fazer parte do Modelo de Organização, Gestão e Controle do Grupo, de acordo com os princípios e objetivos do Modelo de Organização, Gestão e Controle, conforme o Decreto Legislativo italiano 231/2001.

O Grupo protege seus ativos corporativos no mais alto nível de suas capacidades técnicas e recursos disponíveis, divididos nos seguintes elementos fundamentais: pessoas, ativos (bens) e informações. A condição necessária para o desempenho de todas as atividades da F.I.LA. Grupo é a proteção das informações gerenciadas por meio de critérios, medidas e controles de segurança proporcionais aos riscos e ao valor das próprias informações.

A segurança informática do Grupo F.I.L.A. é um requisito fundamental para garantir a confiabilidade das informações processadas, bem como a eficácia e eficiência dos serviços prestados pelo Grupo. A Segurança de TI tem como objetivo principal a proteção de informações, dados pessoais e preservação digital e os elementos através dos quais os dados são gerenciados contra todas as ameaças, sejam elas organizacionais ou tecnológicas, internas ou externas, acidentais ou intencionais, garantindo sua confidencialidade, integridade e disponibilidade. e o cumprimento da legislação vigente aplicável.

Estamos comprometidos com a Segurança de TI, o que significa tanto proteger "ativos" como um site, um computador ou um carro, contra ameaças cibernéticas, e ao mesmo tempo minimizar o impacto no caso de vulnerabilidades que excedam as defesas implementadas.

No F.I.L.A. Group os objetivos de Segurança de TI podem ser resumidos como se segue:

- Confidencialidade, ou seja, assegurar a prevenção de acesso abusivo ou não autorizado a informações, serviços e sistemas
- Integridade, ou seja, garantir que as informações não tenham sido alteradas por acidente ou abuso
- **Segurança**: as informações devem ser mantidas e protegidas de qualquer possível ameaça externa, seja física ou logicamente perpetrada.
- Disponibilidade ou garantia de acesso às informações e serviços de rede pelo pessoal responsável em relação às necessidades de trabalho
- Consistência, ou seja, verificar se existem ferramentas que nos permitam entender se o que esperamos realmente acontece
- Controle, ou seja, ter a capacidade de regular o acesso ao sistema de dados e limitar o acesso e a partição dos usuários por grupos, funcionalidades, etc.
- Supervisão das operações que são realizadas, ou seja, verificações ou auditorias.

A falta de um nível adequado de segurança dos dados, em termos de Confidencialidade, Disponibilidade e Integridade, pode ter como conseqüências a perda de vantagem competitiva, imagem, clientes, volume de negócios e uma conseqüente perda financeira significativa. A tudo isso devemos acrescentar também o risco de incorrer em penalidades ligadas às violações das normas em vigor.

Portanto, a segurança do sistema de informação é obtida pela implementação de uma série de medidas ou procedimentos de segurança adequados, mecanismos técnicos ou práticas que reduzem os riscos aos quais os ativos de informação estão expostos.

Orientamos nossas atividades para o cumprimento da legislação vigente, com especial referência aos Códigos aplicáveis relativos à proteção de dados pessoais em todos os países onde operamos, não apenas para evitar o risco de envolvimento da empresa, mas sobretudo para garantir um nível adequado de segurança dos dados pessoais do Grupo e de seu sistema de informação.

Estamos comprometidos em manter os mais altos padrões éticos possíveis e em cumprir com todas as leis aplicáveis em todos os países nos quais fazemos negócios. Acreditamos firmemente que temos a responsabilidade de operar em conformidade com as regras dos países onde temos presença, distinguindo-se como uma empresa capaz de exportar os valores que permeiam nossas ações, promovendo-os nas comunidades onde atuamos.

Escopo desta política

Esta Política se aplica à F.I.L.A. S.p.A., suas subsidiárias, as entidades nas quais detém uma participação majoritária e as instalações que administra. Estamos comprometidos em trabalhar com e incentivar nossos parceiros comerciais a manter os princípios desta Política e adotar políticas similares dentro de seus negócios.

Localmente, cada empresa deve adotar regras e procedimentos mais rigorosos, conforme necessário e de acordo com as leis e regulamentos locais. Ao conduzir suas atividades de administração, coordenação e supervisão, a F.I.L.A. S.p.A. respeita a autonomia gerencial de cada afiliada dentro de seu Grupo, administrando e controlando o negócio como um todo, de acordo com os interesses legítimos dos acionistas majoritários e minoritários, considerando as exigências de confidencialidade e as leis locais aplicáveis.

Acreditamos firmemente que temos a responsabilidade de operar em conformidade com as regras dos países onde estamos presentes, distinguindo-nos como uma empresa capaz de exportar os Valores que permeiam nossas ações, promovendo-os nas comunidades onde operamos. O objetivo desta Política é orientar os diretores, administradores, funcionários, agentes, consultores, intermediários, joint ventures controladas e outros representantes de terceiros para garantir o cumprimento da regulamentação aplicável e de nossos Valores e Políticas.

O Grupo F.I.L.A. está comprometido com uma melhoria contínua de suas políticas e de seus programas, facilitando a adoção a nível local de todos os procedimentos, regras e instruções necessárias para que os princípios estabelecidos nesta Política sejam aplicáveis e monitorados, a fim de causar um impacto. Ao adotar esta Política, acreditamos contribuir para uma melhor condição das gerações existentes e das próximas gerações, fornecendo ferramentas para uma melhor qualidade de vida.

Princípios gerais

Em nossas estratégias e operações, consideramos os seguintes princípios relativos à Segurança de TI

- **Sistemas de informação empresarial**: os funcionários e colaboradores internos recebem todas as ferramentas necessárias para realizar as tarefas atribuídas. As ferramentas e aplicações de software fornecidas são ferramentas de trabalho e devem ser utilizadas para estes fins: os dados presentes dentro das ferramentas de trabalho (incluindo sistemas de e-mail e sistemas de arquivos locais/rede, bem como locais de armazenamento de dados na Nuvem) são considerados dados corporativos e, como tal, de propriedade da Empresa. Consequentemente, a empresa pode ter acesso completo a eles e os usuários não poderão ter expectativas de privacidade com relação às informações enviadas, recebidas ou armazenadas. Os usos impróprios dos sistemas da empresa incluem processamento, transmissão, recuperação, acesso, exibição, armazenamento, impressão e em geral a divulgação de materiais e dados fraudulentos, assediadores, ameaçadores e ilegais. Os sistemas da empresa incluem o processamento, transmissão, recuperação, acesso, acesso, exibição, armazenamento, impressão e em geral a divulgação de materiais e dados fraudulentos, assediadores, ameaçadores, ilegais. Portanto, nenhum dado deste tipo deve estar presente na rede F.I.L.A., nos computadores pessoais, dentro das aplicações (como e-mail, portais de Intranet, etc.). Além disso, os usuários dos sistemas da empresa não devem utilizar a infra-estrutura para fazer negócios, vender produtos ou para qualquer outra atividade comercial além daquelas expressamente previstas pela administração da empresa.

- **Acesso às informações: O** acesso à informação por cada usuário individual deve ser limitado apenas às informações necessárias para o desempenho de suas funções (princípio da "necessidade de conhecer"). A divulgação e transmissão de informações internamente, bem como externamente, deve ser baseada no mesmo princípio. O Grupo FILA aplicará esta política estabelecendo perfis e direitos adequados de usuários, para restringir a capacidade de acesso à informação de acordo com o princípio acima mencionado. O compartilhamento de informações de acesso do usuário, tais como contas e senha, com outros funcionários ou indivíduos, que não as guardam de forma adequada e segura ou não atualizam as informações de acesso regularmente e de acordo com as Diretrizes Operacionais de Segurança de TI, são considerados uso impróprio dos Sistemas e Informações da Empresa e, como tal, sancionados.
- **Pessoal e segurança**: O Grupo F.I.L.A. planeja e realiza atividades de treinamento e informação dirigidas ao pessoal, com foco na segurança da informação e no uso correto dos equipamentos da empresa. O pessoal deve ser obrigado a garantir um nível mínimo de segurança para o equipamento designado. O roubo, dano ou perda de ferramentas de trabalho devem ser imediatamente comunicados. O pessoal (incluindo consultores e colaboradores externos) deve assinar cláusulas de confidencialidade.
- **Incidentes e anomalias cibernéticas**: Todos os funcionários são obrigados a detectar e notificar quem for responsável por qualquer problema relacionado à segurança do Grupo e da Empresa. Todos os funcionários são obrigados e espera-se que continuem a realizar negócios diários e utilizem os Sistemas da Empresa (com referência especial, mas não limitada a Ferramentas de Colaboração como E-Mail, Equipes Microsoft, Microsoft Sharepoint) com o devido cuidado e atenção às mensagens suspeitas, anexos, solicitações de contato.
- **Segurança física**: O acesso aos edifícios e instalações relevantes para a proteção dos bens só deve ocorrer após a identificação das partes autorizadas. A identificação e concepção de contramedidas de segurança física devem considerar tanto a possibilidade de ameaças físicas quanto a legislação aplicável. A manutenção do equipamento deve ser realizada de acordo com as instruções do fabricante ou com procedimentos documentados para assegurar a disponibilidade e integridade do serviço.
- **Segurança informática**: A identificação e concepção de contramedidas de Segurança de TI devem considerar tanto a possibilidade de tentativas de acesso interno e externo não autorizado, como também a legislação aplicável e quaisquer outras restrições relevantes. Os usuários não devem explorar quaisquer pontos fracos ou deficiências do sistema de Segurança de TI para danificar sistemas ou dados, obter recursos para os quais não estão autorizados, roubar recursos de outros usuários ou ter acesso a sistemas para os quais não têm as autorizações necessárias. Pelo contrário, os usuários devem ter o cuidado de comunicar ao administrador do sistema, por escrito, qualquer mau funcionamento do sistema que possa sugerir a possível perda de estabilidade ou confiabilidade do mesmo.
- **Verificações**: Os sistemas de informação devem ser verificados periodicamente, assim como a aplicação de procedimentos operacionais. O pessoal encarregado que trabalha na divisão de TI está autorizado a realizar intervenções no sistema de TI do Grupo com o objetivo de garantir a segurança e proteção do próprio sistema, bem como por outras razões técnicas e/ou de manutenção (por exemplo, atualização / substituição / implementação de programas, manutenção de hardware, etc.).

As verificações de segurança a serem realizadas para proteger os recursos de TI que compõem seus ativos são conseguidas através de:

- implementação e cumprimento das políticas em todas as áreas organizacionais, processuais e tecnológicas de forma homogênea com respeito aos objetivos definidos
- a atribuição adequada de tarefas e responsabilidades dentro do Grupo para a implementação de políticas
- verificação (como parte da análise de risco de TI) do nível de eficácia das medidas implementadas, recorrendo também à avaliação periódica da vulnerabilidade realizada por partes externas e independentes.

O não cumprimento das disposições desta Política de Segurança de TI estará sujeito a sanções disciplinares, conforme apropriado. A Alta Direção da F.I.L.A. tem um papel estratégico na implementação plena desta Política, garantindo o envolvimento de todo pessoal e daqueles que colaboram com a F.I.L.A. e a consistência de seu comportamento com os valores incorporados nesta Política.

Esta Política é comunicada dentro da organização e disponibilizada on-line a todas as partes interessadas no site www.filagroup.it.

A F.I.L.A. incentiva qualquer pessoa que tome conhecimento de fatos ou comportamentos contrários ao Código de Ética da Empresa, políticas e regras internas, leis ou regulamentos, a fazer um relatório com a máxima confidencialidade. Assegurando a confidencialidade da identidade do denunciante, a F.I.L.A. oferece os seguintes canais para apresentar um relatório:

- E-mail: whistleblowing.fila@gmail.com
- Correio para: odv@fila.it Organismo di Vigilanza, F.I.L.A. Fabbrica Italiana Lapis ed Affini S.p.A. Via XXV Aprile, 5 Pero20016 (MI).

Diretor

Executivo do GRUPO2021 em

outubro - Massimo Candela