**Política de Segurança Cibernética e da Informação**

Versão atualizada em abril de 2024.

**INTRODUÇÃO**

A Política de Segurança Cibernética e da Informação abrange todo o ambiente da Inova e contém objetivos, diretrizes e regras de Segurança Cibernética, visando a garantir a segurança do seu ambiente e, consequentemente, dos usuários da sua plataforma ou dos seus serviços, ou de partes interessadas.

O cumprimento das diretrizes estabelecidas é de responsabilidade de todos os colaboradores e prestadores de serviço, e essencial para atingir níveis adequados de proteção à informação.

**PAPEIS E RESPONSABILIDADES**

Os papeis e responsabilidades referentes a esta política estão distribuídos entre os seguintes níveis da organização:

* Vice-presidência de Tecnologia;
* Diretoria responsável pela Segurança Cibernética - Diretoria de Tecnologia;
* Gerência de Segurança Cibernética e da Informação;
* Gerência de Privacidade e Regulações;
* Gerência de Controles Internos;
* Todos os Colaboradores;
* Todos os Fornecedores e Prestadores de Serviços.

**DIRETRIZES**

A Companhia adota um conjunto de ações, diretrizes e procedimentos para reduzir riscos e vulnerabilidades de segurança da informação, os quais convergem para o fortalecimento dos pilares que amparam todo tratamento de dados pela Inova:

* Confidencialidade: a informação tratada não deve ser divulgada para pessoas sem autorização de acessá-la;
* Integridade: a informação tratada não deve ser alterada sem autorização apropriada;
* Disponibilidade: a informação tratada pode ser armazenada, acessada ou protegida a qualquer tempo;

As diretrizes e regras adotadas pela Companhia coordenam a consecução dos seguintes objetivos:

* monitoramento eficaz da efetividade dos processos e controles implementados para mitigação dos riscos de segurança cibernética e direcionados nesta Política;
* identificação tempestiva de riscos emergentes de segurança da informação a serem tratados;
* otimização contínua da capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;
* disseminação perene de uma cultura de atenção à segurança da informação e de assimilação da proteção dos dados tratados pela Inova como premissa de qualquer desenho de processos ou soluções e como padrão essencial de qualquer procedimento operacional.

**PROGRAMA DE SEGURANÇA DA INFORMAÇÃO**

O programa permanente de Segurança Cibernética da Inova consiste em um amplo processo que, no horizonte dos princípios e objetivos traçados, guia a implementação de controles ou instrumentos de gestão da informação, dentre os quais se destacam:

* + **Classificação dos dados e das informações:** Para que seja possível proteger e tratar informações de maneira adequada é necessário classificar os tipos de informações existentes na Companhia. A classificação é determinada com base no valor da informação, sensibilidade, criticidade, obrigações legais e contratuais, e a Companhia define rótulos para a classificação das informações, os quais devem ser observados e aplicados internamente durante o tratamento de informação;
	+ **Desenvolvimento voltado para privacidade e segurança dos dados:** A Inova possui equipes dedicadas à criação e otimização de instrumentos de melhoria de segurança das suas aplicações com foco em dados pessoais, observando-se exigências legais e melhores técnicas conhecidas no mercado;
	+ **Direito de propriedade:** A Companhia zela pelo respeito a todos os aspectos da propriedade intelectual presente em seu ambiente e em suas operações. É dever de todos a abstenção do uso de informações ou propriedade intelectual da Inova para fins particulares;
	+ **Gestão e definições de uso de ativos de informação:** Ativos de informação são qualquer recurso envolvido no ciclo de vida dos dados na organização. Na Inova, esses recursos são protegidos contra acessos indevidos, e os colaboradores devem observar os cuidados inerentes a cada atividade, atuando com integridade e discernimento durante a utilização dos equipamentos da Companhia, incluindo regras específicas para dispositivos móveis e conectados à sua rede;
	+ **Gestão de acessos:** A Companhia adota procedimentos formais para a gestão de acesso de todo o seu ambiente de TI, contemplando processos de Concessão, Revogação, Transferência, Revisão e Autenticação de Acessos;
	+ **Gestão de mudanças:** A Inova adota diversos controles sobre alterações em sistemas internos e bases de dados da Companhia, incluindo procedimentos de revisão de código, de integridade e continuidade dos sistemas desenvolvidos, rastreamento, versionamento, testes e gerenciamento do ciclo de integração contínua;
	+ **Gestão de redes e de criptografia:** Por meio da gestão das suas redes, a Inova preserva o fluxo seguro de dados entre os componentes dos seus sistemas, observando-se a segmentação das redes e o uso de padrões de configuração seguros e criptografia forte;
	+ **Gestão de vulnerabilidades:** A Inova realiza varreduras e testes recorrentes em seu ambiente de TI, por equipe especializada em testes de segurança, para aferição de falhas e vulnerabilidades em seus sistemas, cujo tratamento é realizado por suas equipes de segurança cibernética e desenvolvimento seguro;
	+ **Proteção contra malware:** Mecanismos de proteção são implementados contra códigos maliciosos em pontos de entrada e saída dos sistemas da Inova. Esses pontos incluem firewalls, servidores de acesso remoto, estações de trabalho, servidores de e-mail, servidores web, servidores proxy e dispositivos móveis;
	+ **Gestão de fornecedores:** A partir de informações recebidas e verificações internas, a Inova avalia os riscos envolvidos na contratação de cada fornecedor, para garantir a conformidade com as regras de segurança cibernética e da informação da Companhia, de acordo com os serviços prestados;
	+ **Manutenção e análise de logs de auditoria:** Trilhas de auditoria automatizadas são implantadas para os componentes de sistemas da Inova, permitindo o rastreamento de eventos de segurança, de autenticação e de ações executadas por usuários;
	+ **Prevenção do vazamento de informações:** A Inova aplica controle de transmissão de informação em seu ambiente de TI, por meio de soluções automatizadas, que detectam, restringem e alertam a circulação indevida de dados. Os controles estão associados à classificação destas informações;
	+ **Plano de contingência:** A Inova possui plano para recuperação segura dos dados tratados pela companhia e funcionalidades dos seus sistemas, em caso de indisponibilidade de serviços críticos de tecnologia que sustentam sua operação, e conta com backup de dados em mais de um datacenter;
	+ **Treinamentos e conscientização em segurança da informação:** Com o objetivo de disseminar o conhecimento e aprimoramento contínuo, a Companhia realiza treinamentos e promove meios de conscientização periódicos relativos à Segurança Cibernética e da Informação, abrangendo todos os colaboradores;
	+ **Gestão de incidentes:** O processo de gestão de incidentes da Inova destina-se a prevenir, detectar, responder e recuperar-se diante de evento inesperado que gere algum tipo de instabilidade, violação de política ou norma interna, ou que possa causar danos à Companhia. Todos os incidentes reportados no ambiente de tecnologia da Inova passam por procedimentos de identificação, análise, classificação e comunicação, de acordo com seus efeitos e com o interesse das partes envolvidas e eventualmente afetadas.

Em caso de identificação, pelo público externo, de alguma inconsistência ou falha no ambiente da Inova, a Companhia disponibiliza canal para recebimento do comunicado respectivo, pelo e-mail dpo@fatecie.edu.br.

**VIOLAÇÃO DA POLÍTICA**

O descumprimento das diretrizes do Programa de Segurança da Informação, definidas nesta Política, constitui ofensa grave e acarreta a aplicação de sanções em conformidade com as normas vigentes.

O colaborador ou prestador de serviço que deliberadamente deixar de notificar violações a esta política também estará sujeito às medidas mencionadas acima.