FORTBRASIL
O crédito que chega junto.

AVISO “POLÍTICA” CIBERSEGURANÇA

1 - OBJETIVOS

Em linhas gerais, essa aviso tem com objetivo:

- Estabelecer diretrizes de Cibersegurança, com objetivo de proteger os ativos tecnológicos e os dados dos clientes da FORTBRASIL;
- Informar as áreas e atribuir as responsabilidades para cumprimento desta Política e garantia da segurança da informação;
- Dar ciência ao público em geral.

2 - DISPOSIÇÕES GERAIS

2.1 ABRANGÊNCIA

Esta documento destina-se a todos os colaboradores, parceiros, fornecedores, prestadores de serviços e clientes da FORTBRASIL. Para os fins do disposto nesta Política o termo "Colaboradores" abrange todos os empregados, menores aprendizes, estagiários e administradores do FORTBRASIL. Toda a atividade do FORTBRASIL deve respeitar os princípios estabelecidos nesta política; e tais princípios devem ser aplicados a todos os que estão acima mencionados.

2.2 DIRETRIZES

A FORTBRASIL visa atingir um alto padrão de Cibersegurança. Por isso, é comprometido com a confidencialidade, integridade e disponibilidade de todos os ativos físicos e lógicos de informação da empresa, garantindo que os requisitos legais, operacionais e contratuais sejam cumpridos. A preocupação com os riscos cibernéticos é comum aos diversos níveis de gestão e um compromisso individual de todos.

2.3 ASPECTOS GERAIS

Documento visa estabelecer princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, garantindo a proteção adequada dos ativos e dos dados, garantindo assim a identificação, proteção, detecção, resposta e recuperação de eventos em casos de eventual incidente de segurança.

2.3.1 IDENTIFICAÇÃO

Desenvolver uma cultura organizacional para gerenciar o risco de Cibersegurança, sistemas, pessoas, ativos, dados e capacidades. Além disto, visa realizar o registro, análise de causa e impacto, e controle dos efeitos de incidentes, incluindo informações recebidas de terceiros, utilizando como base os seguintes processos e recursos, a fim de mitigar riscos:

- Regulamentações Vigentes
- Diretrizes e Normas do Banco Central
- Estratégia de Gerenciamento de Riscos
- Avaliação de Risco
- Ambiente de Negócios
- Gerenciamento de Ativos
- Governança

2.3.2 PROTEÇÃO

Desenvolver e implementar salvaguardas apropriadas para garantir o controle e a mitigação de riscos, incluindo, mas não se limitando a realização de:

- Controle de acesso;
- Conscientização e Treinamentos
- Processos e procedimentos para proteção das informações

2.3.3 DETECÇÃO

Desenvolver e implementar ações estruturadas para identificar a ocorrência de eventuais eventos que causem riscos e comprometam a Cibersegurança, incluindo, mas não se limitando a:

- Monitoramento de eventos e anomalias
- Monitoramento contínuo de seguranças, incluindo parceiros, fornecedores de serviços e clientes
- Processos de detecção, analise e mitigação de riscos
- Plano de resposta a incidentes
- Comunicação
- Monitoramento e melhoria contínua

2.3.4 RECUPERAÇÃO

Desenvolver e programar ações sustentáveis para manter os planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados devido a um eventual incidente de Cibersegurança, incluindo, mas não se limitando a:

- Comunicação junto aos envolvidos
- Mapeamento e implementação de melhorias
- Plano de Recuperação

3 - RESPONSABILIDADES

3.1 COLABORADORES, PARCEIROS, FORNECEDORES, PRESTADORES DE SERVIÇOS E CLIENTES

Salvaguardar todo recurso e informação das empresas componentes do FORTBRASIL criada ou utilizada nas suas atividades, inclusive, mas não se limitando a distribuição não autorizada, acesso indevido, modificação ou destruição.

Conhecer suas responsabilidades a respeito da Cibersegurança, atuando de forma segura, ética e legal na utilização dos recursos e dados, primando pela preservação da integridade, confidencialidade e disponibilidade das informações da empresa.

Relatar através do e-mail governancati@fortbrasil.com.br qualquer situação que represente desvio ou violação desta Política bem como das normas vigentes.

4 - RECOMENDAÇÕES DE SEGURANÇA PARA O CLIENTE

Crie senhas complexas e não utilize seus dados ou informações pessoais na composição (ex.: data de nascimento ou nomes de familiares).

Altere sua senha sempre que existir algum indício ou suspeita de vazamento, ou comprometimento das suas credenciais

Evite utilizar a mesma senha em mais de um serviço, se possível use um gerenciador de senhas para o armazenamento e gerenciamento de credenciais

Sua senha é pessoal e intransferível, portanto não a compartilhe e nem a anote em lugares que outras pessoas tenham fácil acesso (ex.: cadernos e bloco de notas)

FORTBRASIL
O crédito que chega junto.

Evite acessar sites e aplicativos bancários ou realizar transações em dispositivos (computadores, celulares e tablets) de terceiros, públicos (ex.: Lan House) ou não confiáveis. O mesmo vale para redes wireless (Wi-Fi) públicas

Mantenha seus dispositivos com os sistemas operacionais e aplicativos atualizados

Procure instalar uma solução de antivírus no seu computador e a mantenha atualizada

Evite abrir e-mails cujo remetente ou conteúdo sejam desconhecidos

Não clique em links disponibilizados em e-mails ou em mensagens SMS suspeitas e/ou desconhecidas;

Nunca informe dados pessoais, corporativos ou financeiros em ligações, ou mensagens recebidas de pessoas desconhecidas

5 - MEDIDAS DISCIPLINARES

As violações a esta Política estão sujeitas às ações disciplinares previstas nas normas internas da FORTBRASL e na legislação brasileira vigente.

6 - REFERÊNCIAS

Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)

Resolução BCB 85

DATA DA ÚLTIMA ATUALIZAÇÃO:

27/08/2021

FORTBRASIL
O crédito que chega junto.