POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

OBJETIVO

Garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral, observando as regulamentações aplicáveis e melhores práticas de mercado.

INTRODUÇÃO

A informação é um dos principais bens de qualquer organização. Para a devida proteção desse bem, a FOXZIPCODE estabelece a presente política de Segurança da Informação e Cyber Security, a fim de garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral.

Nossa estratégia de Segurança da Informação e Cyber Security foi desenvolvida para evitar violações da segurança dos dados, minimizar os riscos de indisponibilidade dos nossos serviços, proteger a integridade e evitar qualquer vazamento de informação.

Para alcançarmos esse objetivo nossa estratégia está baseada na proteção de perímetro expandido, apoiado em processos de controle para detecção, prevenção, monitoramento e resposta a incidentes garantindo a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital da FOXZIPCODE. O conceito de perímetro expandido considera que a informação deve ser protegida independentemente de onde ela esteja, em todo o seu ciclo de vida, desde o momento que ela é coletada, passando pelo processamento, transmissão, armazenamento, análise e seu descarte.

PÚBLICO ALVO

Colaboradores da FOXZIPCODE. Para os fins do disposto nesta política o termo "Colaboradores" abrange todos os empregados, menores aprendizes, estagiários e administradores da FOXZIPCODE ou prestadores de serviços que tenham acesso às informações.

REGRAS

Regras Gerais

Todas as políticas de segurança da informação precisam estar disponíveis em local acessível aos colaboradores e devem ser protegidas contra alterações. As políticas de segurança da informação são revisadas anualmente pela FOXZIPCODE com aplicação no Brasil.

Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da FOXZIPCODE, clientes e público em geral está fundamentado nos seguintes princípios:

- Confidencialidade: garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;
- Disponibilidade: garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- Integridade: garantimos a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.
- Autenticidade: garantir a identificação da informação e registro dos acessos e modificações.

Diretrizes de Segurança da Informação

A Segurança da Informação na FOXZIPCODE estabelece as seguintes diretrizes:

a) As informações da FOXZIPCODE, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

c) Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

d) O acesso às informações e recursos só deve ser feito se devidamente autorizado.

e) A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

f) A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

h) Todo colaborador deve reportar os riscos às informações à área de Segurança da Informação.

i) A área de Segurança de Informação deve divulgar amplamente as responsabilidades sobre Segurança da Informação aos Colaboradores, que devem entender e assegurar estas diretrizes.

Processo de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a FOXZIPCODE adota os seguintes processos:

a) Gestão de Ativos da Informação

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos ("*software*" e "*hardware"*) e não tecnológicos (pessoas, processos e dependências físicas). Os ativos da informação, de acordo com sua criticidade, devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "*hardening*", *patch management*, autenticação e autorização) e ter documentação e planos de manutenção atualizados anualmente.

Os ativos da FOXZIPCODE, dos participantes e assistidos e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da FOXZIPCODE. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, prestador de serviço, para que seja responsabilizado por suas ações.

As credenciais de login e senha relativas a um colaborador atribuem responsabilidade pelo acesso às informações e ações sobre essas, vale, como assinatura eletrônica e são de uso pessoal, intransferível, vedada a sua exposição, compartilhamento ou acesso por terceiros, ainda que colaboradores da FOXZIPCODE. Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

Para tanto, credenciais, suportes tecnológicos ou físicos deverão ser usados para fins profissionais apenas, não devendo o colaborador ter expectativa de sigilo sobre a sua utilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

d) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da FOXZIPCODE, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, segundo condições de mercado, independentemente de estarem dentro da infraestrutura da FOXZIPCODE, parceiros ou prestadores de serviços.

As tecnologias em uso pela FOXZIPCODE devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas, de modo a garantir interoperabilidade e integridade das informações.

Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios definidos pela gestão.

e) Gestão de Riscos em Prestadores de Serviços

Os prestadores de serviços contratados pela empresa são classificados considerando alguns critérios, tais como: Criticidade do segmento; Auditoria remota; Informações mais críticas manipuladas pelo fornecedor; Forma de acesso às informações; Frequência de acesso às informações; Histórico de fraude e/ou de vazamento de informação; Certificações; Data da última avaliação; Top fornecedor do segmento; classificação do risco identificado na última avaliação. Dependendo da classificação do prestador de serviço referente aos critérios acima, deverá passar por avaliação de risco, que vai desde a validação *in loco* dos controles de segurança da informação, avaliação remota das evidências ou outros processos de avaliação, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

Para avaliação de risco, é utilizado um Baseline de Fornecedores, que consiste em um documento com diversos controles de segurança baseado em padrões internacionais e melhores práticas do segmento. Existe um canal de comunicação para que os prestadores de serviços, que prestam serviços ao FOXZIPCODE, informem as ocorrências de incidentes relevantes relacionados as informações da FOXZIPCODE armazenadas ou processadas na empresa contratada, em cumprimento às determinações legais e regulamentares.

Os prestadores de serviços devem informar os incidentes relevantes, relacionados às informações da FOXZIPCODE armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares, conforme previsão contratual.

f) Tratamento de Incidentes de Segurança da Informação e Cyber Security

A área de Cyber Security realiza a monitoração de segurança do ambiente tecnológico da FOXZIPCODE, analisando os eventos e alertas com o objetivo de identificar possíveis incidentes. Os incidentes que são identificados pelos alertas são classificados com relação ao impacto de acordo com os critérios adotados pela FOXZIPCODE.

Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro. Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, etc, de acordo com o procedimento operacional. Visando aprimorar a capacidade da FOXZIPCODE na resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes. Para os incidentes que possam impactar outra empresa, há um processo de troca de informações entre as instituições, visando a colaboração na mitigação do risco do incidente em cumprimento às determinações legais e regulamentares.

A gerência de Controle Interno e Compliance da FOXZIPCODE elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Risco e ao Conselho de Administração, conforme determinações legais e regulamentares.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a gerência de Controle Interno e Compliance da FOXZIPCODE e na mitigação dos riscos relacionados à segurança da informação.

g) Conscientização em Segurança da Informação e Cyber Security

A FOXZIPCODE promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, mídia indoor, redes sociais aos colaboradores e clientes.

h) Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

i) Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas à Administração Predial.

Os colaboradores deverão manter documentos físicos (papel, pen drive, CD ou outro suporte físico), inclusive pastas, formulários e dados pessoais seus e de terceiros, participantes e assistidos, em local de acesso restrito, preservado de fácil visualização, acesso ou cópia.

j) Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da FOXZIPCODE e às boas práticas de segurança.

Os sistemas utilizados devem ser estruturados de forma a proteger os dados, principalmente dados pessoais e sensíveis, de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, atendendo aos padrões de boas práticas e de governança e aos princípios gerais em Lei.

Em caso de aquisição de novos sistemas, os mesmos deverão ser homologados seguindo o padrão de segurança estabelecido pela Patrocinadora, conforme legislações em vigor.

k) Gravação de LOGs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional de forma a permitir identificar: quem fez o acesso; quando o acesso foi feito; o que foi acessado e como foi acessado. As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

l) Programa de Cyber Security

O Programa de Cyber Security da FOXZIPCODE é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores práticas;
- Cenário mundiais.

Conforme sua criticidade, o programa divide-se em:

- Ações críticas: Consiste de correções emergenciais e imediatas para mitigar riscos iminentes;

- Ações de Sustentação: Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- Ações Estruturantes: Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam a empresa para o futuro.

m) Proteção de perímetro

Para proteção da infraestrutura da FOXZIPCODE contra um ataque externo, utilizamos ferramentas e controles contra: ataques que afetem a disponibilidade (DDoS), Spam, Phishing, ataques avançados persistentes (APT), Malware, invasão de dispositivos de rede e servidores, ataques de aplicação e scan externos.

No sentido de nos protegermos contra vazamento de informações, utilizamos diversas ferramentas preventivas contra vazamento de informação, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além de criptografia de disco em notebooks e solução de proteção de dispositivos móveis.

Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de Auditoria Interna.

Propriedade Intelectual

A propriedade intelectual é composta por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio). Quaisquer informações e propriedade intelectual que pertençam a FOXZIPCODE, ou por ele disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

Pertencem exclusivamente à FOXZIPCODE todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criadas ou realizadas pelo colaborador da FOXZIPCODE, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho, de estágio ou trabalhos desenvolvidos por fornecedores contratados pela FOXZIPCODE, cujas normas de direito de propriedade intelectual estejam disponíveis em contrato. Quaisquer informações e conteúdos cuja propriedade intelectual

pertença a FOXZIPCODE, ou tenham sido por ele disponibilizado, inclusive informações e conteúdo que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da FOXZIPCODE não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa da FOXZIPCODE.

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual da FOXZIPCODE.

Declaração de Responsabilidade

Pela confirmação e ciência da presente Política, os Colaboradores e Prestadores de Serviços diretamente contratados pela FOXZIPCODE consideram-se formalmente comprometidos a agir segundo os critérios e definições descritas e a adotas as medidas indicadas, quando aplicável.

Periodicamente os Colaboradores e Prestadores de Serviços diretamente contratados pela FOXZIPCODE devem também aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados entre terceiros e a FOXZIPCODE devem possuir cláusula que assegure a confidencialidade das informações.

Papéis e Responsabilidades

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas com o suporte da Patrocinadora, através da Diretoria de Segurança Corporativa e discutidos nos fóruns específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou Tecnologia.

Medidas Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas da empresa do FOXZIPCODE, e na legislação vigente no Brasil.

Documentos Relacionados

Esta Política Corporativa de Segurança da Informação é complementada por procedimentos específicos de Segurança da Informação da FOXZICODE, em conformidade com os aspectos legais e regulamentares e aprovadas nos fóruns competentes da empresa.

Glossário

Segregação de funções: Consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

Cyber Security: é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

APT: Adbvanced Persintent Threat, ou ataques avançados persistentes.

Canais de Comunicação de Segurança da Informação

- Suspeitas de incidentes de segurança da informação?

Encaminhe e-mail para: compliance@foxzipcode.com.br

- Recebeu um e-mail suspeito e deseja enviá-lo para análise?

Encaminhe e-mail para: compliance@foxzipcode.com.br

- Suspeitas de incidentes de segurança da informação?

Encaminhe e-mail para: compliance@foxzipcode.com.br

- Está com dúvida sobre como solicitar, excluir ou alterar um acesso?

Fale com a Unidade de Relacionamento de Segurança

Encaminhe e-mail para: compliance@foxzipcode.com.br

APROVAÇÃO

Esta Política foi aprovada pela Diretoria da FOXZIPCODE em 15.02.2024.

RESPONSÁVEL PELO DOCUMENTO

Etapa Nome da área	
Elaboração	Controles Internos e Compliance
Aprovação	Diretoria Executiva FOXZIPCODE
Órgão Responsável	Diretoria Executiva FOXZIPCODE