PHISHX

Introdução a política de segurança

Objetivo

O objetivo da política de segurança é promover melhores práticas, padrões e diretrizes para o nosso ambiente no trato de ativos de informação, disseminando uma cultura de segurança das informações, mantendo a segurança dos sistemas, a integridade e disponibilidade de dados, a confidencialidade das informações, a continuidade dos negócios e a aderência às leis e normas que regulamentam os nossos negócios.

Esta política e os demais procedimentos que suportam sua implementação estão em conformidade com as nossas demais políticas.

Ativos

Todos os recursos tecnológicos disponibilizados, como servidores, computadores, e-mail, telefones, redes, acesso à Internet e sistemas se destinam única e exclusivamente aos interesses do negócio, no qual todos os colaboradores são responsáveis pelo correto manuseio devendo zelar e proteger com a finalidade de gerar benefícios à organização e, como consequência, auxiliar no cumprimento de sua missão.

Informações

As informações acessadas, geradas ou desenvolvidas nas dependências internas ou externas da instituição por colaboradores ou parceiros de negócios são consideradas ativos intangíveis devendo ser devidamente manuseadas, protegidas e utilizadas unicamente para a finalidade previamente autorizada, independente da forma como foi armazenada ou compartilhada.

Classificação da Informação

Classificar a informação é o procedimento de suma importância que permite diferenciar as informações de uma instituição através de um conjunto de critérios, sendo eles: grau de confidencialidade, disponibilidade e integridade.

Princípios de Segurança da Informação

Precisamos que todos respeitem os princípios de segurança para evitar riscos que podem comprometer a continuidade dos negócios e afetar nossa imagem perante nossos clientes, parceiros e controladores.

Os princípios são:

* **Confidencialidade**: garante que as informações tratadas são de conhecimento exclusivo de pessoas autorizadas a acessá-las.

* **Integridade**: garante que as informações são mantidas íntegras, sem modificações indevidas, sejam acidentais ou propositais.

* **Disponibilidade**: garante que as informações estão disponíveis a todas as pessoas autorizadas a consultá-las e/ou tratá-las.

Ciclo de Vida

Toda informação possui um ciclo de vida que é dividido em: Manuseio, Armazenamento, Transporte e Descarte.

* **Manuseio**: o proprietário é responsável por rotulá-la e classificá-la de acordo com a classificação da informação.

* **Armazenamento**: cada custodiante será responsável pela guarda das informações através de dispositivos de tecnologias e/ou de parceiros, garantindo a sua disponibilidade, confidencialidade e integridade.

* **Transporte**: qualquer meio, seja ele físico ou lógico, deverá refletir os controles proporcionais à classificação da Informação e aos riscos inerentes, e ocorrer sempre de forma segura.

* **Descarte**: processo final no ciclo de vida de uma informação. Devem ser utilizados mecanismos eficientes de deleção não passível de recuperação, como fragmentadora de papel ou processos digitais de limpeza de dados.

Utilização de Softwares

Os colaboradores devem utilizar apenas os softwares instalados pela equipe de tecnologia da informação, que se encontram devidamente registrados, homologados e licenciados pela instituição, existindo um padrão de software que deve ser obedecido por todos os colaboradores. Não é permitido o uso ou instalação de programas que não foram adquiridos, homologados e licenciados pela empresa.

Uso de Correio Eletrônico (E-mail)

O e-mail se limita exclusivamente aos negócios, não podendo nenhuma mensagem conter comentários abusivos, obscenos ou difamatórios ou qualquer outro material que possa trazer má publicidade ou constrangimento público a empresa, nossos clientes ou prestadores de serviços.

Deve-se evitar a utilização do e-mail para troca de mensagens confidenciais ou estratégicas para os negócios da instituição.