Política de Prevenção de Vazamento de Dados

FOLHA DE CONTROLE

Informações Gerais

Título	Política de *Prevenção de Vazamento de Dados*
Número de Referência	POL_VAZ
Número da Versão	V2
Status	Nova
Aprovador	Comitê de Privacidade
Data da Próxima Revisão	1 ano após a data da aprovação

Aprovado pelo Comitê de privacidade em 7 de agosto de 2021

Sumário

Objetivo 4
1 Vigência 4
2 Informações Confidenciais 4
3 Gestão de acessos às informações 4
4 Proteção do Ambiente da Hoobox 4
4.1 Autenticação 5
4.2 Gestão de Incidentes de Segurança da Informação 5
4.3 Prevenção a Vazamento de Informações 5
4.4 Testes de Intrusão 5
4.5 Varredura de Vulnerabilidades 5
4.6 Controle Contra Software Malicioso 5
4.7 Criptografia 6
4.8 Rastreabilidade 6
4.9 Segmentação de Rede 6
4.10 Desenvolvimento Seguro 6
4.11 Cópias de Segurança 6
5 Continuidade dos negócios 6
6 Principais recomendações de segurança aos clientes e usuários 6
6.1 Autenticação e Senha 7
6.2 Antivírus 7
6.3 Engenharia Social 7
6.4 Phishing 7
6.5 SPAM 8
6.6 Falso Contato Telefônico 8

Objetivo

A Política de Prevenção de Vazamento de Dados (“Política”) da Hoobox Robotics Tecnologia do Brasil LTDA (“Hoobox”) visa garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Grupo para o alcance dos objetivos de segurança da informação, se complementando à Política de gestão de incidentes de segurança da Informação e à Política de Resposta a Incidentes.

1 Vigência

Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas da Hoobox, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local.

2 Informações Confidenciais

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela Hoobox é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas.

A Hoobox poderá revelar as informações confidenciais nas seguintes hipóteses sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

3 Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores e terceiros da Hoobox são treinados, periodicamente, sobre os conceitos de segurança da informação, através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética.

4 Proteção do Ambiente da Hoobox

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica da Hoobox por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta

aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

4.1 Autenticação

O acesso às informações e aos ambientes tecnológicos da Hoobox deve ser permitido apenas às pessoas autorizadas, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação. O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

- A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);
- A remoção de autorizações dadas a usuários afastados ou desligados do Grupo, ou ainda que tenham mudado de função; e
- A revisão periódica das autorizações concedidas.

4.2 Gestão de Incidentes de Segurança da Informação

As políticas podem ser vistas nos documentos:

- Política de gestão de incidentes de segurança da Informação, e
- Política de Resposta a Incidentes.

Disponíveis no rodapé do site https://www.neonpass.com.br

4.3 Prevenção a Vazamento de Informações

Utilização de controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

4.4 Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação deverão ser realizados no mínimo anualmente a partir de 2022 ou da assinatura do primeiro contrato com esse requisito, o que acontecer primeiro.

4.5 Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

4.6 Controle Contra Software Malicioso

Todos os ativos (computadores, servidores, etc.) que estejam conectados à rede corporativa ou façam uso de informações do Grupo, devem, sempre que compatível, ser protegidos com uma solução anti-malware determinada pela área de Segurança da Informação.

4.7 Criptografia

Toda solução de criptografia utilizada na Hoobox deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

4.8 Rastreabilidade

Níveis de hierarquia ou identificadores próprios são utilizados para rastrear em todo e qualquer ambiente compartilhado de desenvolvimento para detectar os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.

4.9 Segmentação de Rede

- Computadores que interagem com informações sensíveis, servidores ou banco de dados estarão sempre conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área responsável, que fará a análise e aprovação, enviando para que seja executada pela área responsável.

4.10 Desenvolvimento Seguro

A Hoobox mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas

4.11 Cópias de Segurança

O processo de execução de backups é realizado, periodicamente, nos ativos de informação do Grupo, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

5 Continuidade dos negócios

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

6 Principais recomendações de segurança aos clientes e usuários

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos.

6.1 Autenticação e Senha

O cliente é responsável pelos atos executados com seu identificador (login / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.
Recomendamos que:

- Mantenha a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação; • Bloquear sempre o equipamento ao se ausentar.
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Token e etc.)

6.2 Antivírus

Recomendamos que o cliente mantenha uma solução de antivírus atualizada e instalada no computador utilizado para acesso aos serviços oferecidos pelo Grupo. Além disso, possuir o sistema operacional atualizado com as últimas atualizações realizadas.

6.3 Engenharia Social

A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança do usuário, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

6.4 Phishing

Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de e-mails maliciosos, afim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos e-mails de phishing podem ocorrem das seguintes maneiras:

- Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;
- Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- Quando tentam induzir os usuários a preencher formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

6.5 SPAM

São e-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

6.6 Falso Contato Telefônico

São e-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.