POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

SUMÁRIO

1. OBJETIVO

A presente Política de Segurança Cibernética objetiva estabelecer procedimentos para que haja a mitigação de riscos das infraestruturas Críticas e segurança nas redes, estabelecendo conceitos básicos fundamentais, princípios, normas e meios para disseminar informações que versam acerca do armazenamento seguro das informações, bem como, reduzir a vulnerabilidade a incidentes, além de contar com o mapeamento de possíveis riscos, a hierarquia de infraestruturas críticas e definição de procedimentos e padrões a serem seguidos contra ameaças e riscos voltados à segurança cibernética.

Esta Política demonstra o zelo e compromisso da JUSTWEB TELECOMUNICAÇÕES para com seus assinantes, visando primordialmente, a segurança e a privacidade. Além de abranger todos os aspectos e princípios que tratam a legislação acerca da Política de Segurança Cibernética, portanto, o objetivo principal do provedor é prezar pela prevenção, além de detectar e evitar possíveis incidentes.

2. DIRETRIZES

2.1 A JUSTWEB visa promover a disseminação de informações de Segurança CIbernética pertinentes à proteção destas, de modo que, estabelece na presente Política procedimentos e normas afim de minimizar os riscos e seguir os princípios básicos da segurança.

2.2 A Política de Segurança deverá ser disseminada aos profissionais e colaboradores da JUSTWEB, resguardando o compartilhamento de informações sensíveis apenas àqueles que executam a presente Política, e orgãos competentes mediante solicitação.

2.3 Todas as informações pessoais coletadas e armazenadas pela Prestadora indispensáveis à utilização do serviço, será confidencial e permanecerá em sigilo, salvo se solicitado por órgãos competentes, afim de instruir investigações.

2.4 Indícios de descumprimentos da Política de Segurança devem, impreterivelmente, ser comunicado à JUSTWEB, para que haja a investigação e estudo acerca da irregularidade.

2.5 A presente Política deverá ser revisada e, se necessário atualizada, em prazo não superior à um ano, seguida de sua publicação em sua página na internet contendo às informações não sensíveis.

2.6 As diretrizes definidas na presente Política devem ser seguidas por todos os prestadores de serviços, fornecedores, contratados e clientes que, de alguma forma, utilizam informações da JUSTWEB.

3. DEFINIÇÕES

Segue definições relevantes para o entendimento da presente Política de Segurança e disseminação de informações aos usuários.

3.1 Ameaça: Causa de um incidente indesejado, decorrente de um dano que possa explorar a vulnerabilidade intencional e danificar um ativo.

3.2 Confidencialidade: Meio de assegurar o sigilo de informações àqueles que, não estão autorizados a ter acesso.

3.3 Espaço Cibernético: Conjunto de canais de comunicação de internet e redes, relaciona-se por exemplo, com o armazenamento, processamento e compartilhamento de ações.

3.4 Incidente: Ação ou omissão, que permita o acesso não autorizado, a interrupção das operações, bem como a destruição, dano ou alteração da informação protegida, assim como a disseminação e publicação indevida desta informação.

3.5 Infraestruturas Críticas: Serviços e sistemas que, se forem interrompidos ou destruídos, ocasionarão sérios impactos ao Provedor.

3.6 Risco: A possibilidade de corromper um sistema, por meio de ameaças e vulnerabilidades, ou seja, as consequências de um incidente que comprometa a execução do sistema.

3.7 Segurança Cibernética: Meios para a realização da segurança de operações, que garante a resistência a eventos capazes de comprometer a integridade e autenticidade dos dados.

3.8 Vulnerabilidade: Conjunto de fatores que ocasionam um incidente indesejado, o qual pode resultar em risco para o sistema.

4. PRINCÍPIO DA SEGURANÇA DA INFORMAÇÃO

Sabemos que, a Segurança Cibernética visa a proteção de informações e arquivos contra diversos tipos de ataques. Assim sendo, é indispensável a preservação dos princípios básicos de segurança nas condutas e procedimentos nas redes e serviços de telecomunicações. Quais sejam:

4.1 Confidencialidade: Se relaciona com o sigilo da informação, ou seja, somente pode ser acessada por pessoas que possuem autorização, sendo uma ferramenta de confidencialidade é a Criptografia.

4.2 Autenticidade: Este princípio garante a veracidade da autoria da informação, apesar de não garantir a veracidade da informação, algumas das ferramentas deste princípio é a biometria, assinatura e o certificado digital.

4.3 Disponibilidade: A Informação deve ser disponível sempre que necessário, algumas das ferramentas que garantem a disponibilidade é o nobreak, firewall e backup.

4.4 Integridade: Este princípio impede que a informação seja alterada por pessoas não autorizadas, assim, deve-se fazer o uso de ferramentas como a Assinatura Digital e Backup (nos casos de informações corrompidas e perdidas).

5. CAPACITAÇÃO E RESPONSABILIDADE DOS COLABORADORES

5.1 A Prestadora afim de capacitar da melhor maneira possível seus colaboradores, vem frequentemente, disseminando a cultura de Segurança Cibernética por meio de treinamentos, conforme disposto abaixo:

CURSO DE BOAS PRÁTICAS E CIBERSEGURANÇA DA INTERNET

COLABORADOR/ TÉCNICO	CARGA HORÁRIA	DATA
DAVI JORGE LEITE SANTOS	3 HRS	30/11/2021
FABIANO MARTINS DE OLIVEIRA	3 HRS	30/11/2021
FABIO AUGUSTO MIRANDA MENDES	3 HRS	30/11/2021
FLAVIA MENDES ALCÂNTARA	3 HRS	30/11/2021
LETICIA SILVA DE OLIVEIRA	3 HRS	30/11/2021
MAIKE RIBRAS BATISTA	3 HRS	30/11/2021
PAULO CESAR DE MORAIS JUNIOR	3 HRS	30/11/2021
RAFAEL SARAIVA HERINGER	3 HRS	30/11/2021
RICHARD MARTINS SERAFIN	3 HRS	30/11/2021
SAULO GUADALUPE	3 HRS	30/11/2021
DAVI JORGE LEITE SANTOS	3 HRS	30/11/2021

5.2 Os profissionais e colaboradores são responsáveis pela utilização dos recursos disponibilizados pela Prestadora, bem como pelas informações sobre websites de acesso proibido e informações pessoais dos Assinantes.

5.3 Os equipamentos que forem disponibilizados pela Prestadora, devem ser transportados de forma segura.

5.4 Todos os colaboradores deverá assinar o Termo de Ciência, Sigilo e Confidencialidade das informações sempre que solicitado pela JUSTWEB.

5.5 É vedado a utilização e armazenamento de informações da empresa e de seus clientes sem autorização ou de modo indevido.

6. RECOMENDAÇÕES DE SEGURANÇA AOS USUÁRIOS

A disseminação de informação é indispensável para que haja um ambiente cada vez mais seguro e confiável. Neste sentido, é notório também que, os clientes e usuários possuem inteira responsabilidade pelos atos que executam em seu IP.

Diante disso, é disponibilizado no site **WWW.JUSTWEB.COM.BR** uma cartilha com as principais recomendações e cuidados a serem tomados por cada um dos usuários, a fim de disseminar dicas relevantes quanto à Segurança.

Podemos citar como exemplo recomendações quanto a senhas, falsos contatos telefônicos, spam e phishing, conforme segue:

- Senhas: Recomendamos mantê-las em completo sigilo, não anotar e sim memorizá-las, alterar sempre que se sentir inseguro, além de criar senhas de difícil adivinhação.
- Contatos Telefônicos: Desconfie sempre de contatos telefônicos que solicitem dados, pois, há muita fraude em ligações falsas, as quais são solicitadas informações pessoais.

- Spam: Se refere ao recebimento de e-mails não solicitados, estes que são enviados em massa e possui como finalidade a publicidade e disseminação de informações falsas ou ilegais.
- Phishing: Técnica de engenharia social utilizada para enganar o usuário através de envio de e-mail ou mensagens aparentemente reais, objetivando obter informações pessoais do usuário, como por exemplo número de RG, CPF e dados bancários, para posteriormente, cometer fraudes eletrônicas.

Portanto, afim de prezar sempre pela disseminação de informações relevantes para nossos Assinantes, disponibilizamos uma cartilha com demais informações e recomendações a serem seguidos por estes. Caso tenha interesse em recebê-la basta entrar em contato pelos seguintes canais de atendimento: **(31)3017-7112, 08004941234**, ou acesse **www.justweb.com.br.**

7. PROCEDIMENTOS ADOTADOS PARA ANÁLISE E MITIGAÇÃO DE VULNERABILIDADES

A Prestadora informa abaixo os procedimentos e controles adotados para identificação das vulnerabilidades, bem como para a análise dos riscos e das ameaças no que tange à Segurança Cibernética.

- Serviço Walled Garden bloqueio de BOGONS, mitigação de ataque DDoS e geração de gráficos referentes à vulnerabilidades de rede;
- Servidor de Netflow gera gráficos e alertas referentes à vulnerabilidades da rede, entrada e saída;
- Servidor de varredura de vulnerabilidade em dispositivos finais que utilizam-se de protocolos como NMAP e NETSTAT;
- Envio de Cartilhas e Notificações aos clientes;
- Respostas aos e-mails de órgãos reguladores;

No mesmo sentido, a prestadora estabelece alguns procedimentos e controles para a mitigação das vulnerabilidades e riscos em casos de incidentes, quais sejam:

Aplicação de Firewall; Envio de notificação ao usuário detentor do IP; Utilização das ferramentas de mitigação e gráficos de rede; e, a atualização de versões de equipamentos.

8. PLANO DE RESPOSTA A INCIDENTES E INFORMAÇÕES ACERCA DA SEGURANÇA CIBERNÉTICA

A JUSTWEB TELECOMUNICAÇÕES, define abaixo as seguintes ações em casos de incidentes:

1º Passo: Análise de qual a modalidade do ataque;
2º Passo: Identificação do(s) destino(s) do ataque(s);
3º Passo: Ação
1- Criação de Firewall internos a rede;
2- Utilização das ferramentas aplicadas internas a rede;
4º Passo: Acompanhamento da rede;
5º Passo: Identificação do protocolo atacado;
6º Passo: Correção do problema;

Ainda, a Prestadora define alguns meios de compartilhar informações sobre incidentes relevantes e demais informações referentes à Segurança Cibernética, como por exemplo: Assessoria de Cibersegurança; Utilização de um Sistema privado para troca de informações; Realização de reuniões para alinhamento do ocorrido e possíveis correções; além de conscientização da equipe técnica sobre os incidentes e demais treinamentos.

9. DOCUMENTOS TÉCNICOS DE SEGURANÇA DA INFORMAÇÃO

Para abranger todos os requisitos necessários, a Presente Política se relaciona com uma lista documentos sensíveis, a qual ficará arquivada e será utilizada somente, quando solicitada por orgãos competentes e reguladores.