Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política de Firewall.

Objetivo

Estabelecer medidas de proteção ao tráfego de rede interno e externo da Instituição, com a finalidade de garantir quais tipos de pacotes de dados poderão trafegar no âmbito da Instituição.

Visão Geral

Sistemas de firewall são dispositivos de hardware ou programas de software que controlam o fluxo de tráfego entre redes, servidores e sistemas informáticos. Eles protegem os recursos internos contra eventuais intrusões e acessos indevidos, constituindo uma parte essencial do sistema de segurança da informação da Instituição.

1. Diretrizes dos Sistemas de Firewall

A Instituição protege os seus recursos e ativos de informática utilizando-se de uma abordagem em camadas físicas e/ou lógicas, estabelecendo-se um perímetro de segurança da rede interna da Instituição. Deste modo, o design de segurança da rede inclui a funcionalidade de firewall em todos os lugares da rede onde possam existir eventuais vulnerabilidades.

Há também a inclusão de outras áreas além do perímetro de segurança da rede, com o fito de fornecer uma camada adicional de segurança e proteger os

EMBRASI

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

dispositivos que são colocados diretamente em redes externas à Instituição, também conhecida como “zona desmilitarizada”.

2. Implementação dos Sistemas de Firewall

O Responsável pela Segurança da Informação deve sempre aprovar e testar todas as assinaturas e licenças dos sistemas de firewall utilizados pela Instituição, bem como monitorar as conexões de rede e alterações nas configurações destes sistemas de firewall, que serão revistos e atualizados sempre quando novos aplicativos ou servidores forem implementados dentro da rede.

Devem ser criados diagramas de infraestrutura da rede que possibilitem a identificação de conexões entre ambientes que contenham quaisquer dados confidenciais ou sigilosos da Instituição, posicionando os sistemas de firewall entre conexões da zona desmilitarizada (DMZ) e da rede interna.

3. Configuração Geral dos Sistemas de Firewall

O Responsável pela Segurança da Informação deve configurar como os sistemas de firewall realizarão o controle do tráfego de entrada e saída de rede, observando as seguintes diretrizes:

- Revisão e desenvolvimento regular de uma lista dos tipos de tráfego da Instituição e em quais circunstâncias eles devem ser protegidos;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

- Bloqueio de todo o tráfego de entrada e saída não autorizado, diminuindo o risco de ataques cibernéticos e o volume de tráfego transportado pela rede interna;
- Restrição do tráfego de entrada e saída ao que é estritamente necessário para as informações e dados confidenciais, negando-se de forma específica todos os outros tipos de tráfego;
- Implementação de medidas antifraude, a fim de detectar e bloquear o ingresso na rede interna de endereços IP de origem fraudulenta;
- Implementação de uma zona desmilitarizada (DMZ) e a instalação de sistemas de firewall de perímetro desta rede que forneça serviços, protocolos e portas/serviços autorizados ao público externo à Instituição.
- Utilização de tecnologias de inspeção de pacotes, como por exemplo, a filtragem dinâmica de pacotes, visando que apenas as conexões estabelecidas sejam permitidas na rede.

Os métodos autorizados pela Instituição para mascarar o endereçamento IP devem incluir configurações NAT (Network Address Translation), remoção ou filtragem de anúncios de rota para redes privadas e uso interno do espaço de endereço.

4. Licenciamento, Manutenção e Suporte

As ações de manutenção, tais como (i) atualizações de software, (ii) atualizações de configuração de firewall, e (iii) logs de segurança, devem ser devidamente registradas e retidas por um período a ser definido pelo Responsável pela Segurança

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

da Informação, a fim de permitir investigações adequadas sobre incidentes relacionados a eventuais ameaças de segurança da informação.

O Responsável pela Segurança da Informação deve garantir o licenciamento de softwares, bem como o rastreamento e a documentação relacionadas, incluindo processos e procedimentos que suportem:

- Monitoramento proativo e implementação de medidas, visando apoiar esta Política;
- Existência de medidas que impeçam o usuário de desabilitar ou modificar as configurações de firewall utilizadas pela Instituição;
- Definição de exceções a esta Política, que será realizada pelo Responsável pela Segurança da Informação a partir de uma avaliação específica;
- Medidas de segurança adicionais para assegurar a continuidade dos sistemas de firewall caso os softwares utilizados pela Instituição sejam desabilitados ou desativados.