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 Antivírus e Malware.

Objetivo

Estabelecer as diretrizes e procedimentos para a abordagem e prevenção de vírus de computador, worm, spyware, malware e outros tipos de softwares maliciosos.

Visão Geral

O aumento do número de incidentes de segurança da informação pode gerar consequências graves aos negócios e processos da Instituição, sendo necessário a adoção de medidas para evitar que esses softwares maliciosos explorem quaisquer vulnerabilidades nos sistemas e plataformas da Instituição.

1. Diretrizes de Utilização de Antivírus

O Responsável pela Segurança da Informação ou seus designados devem garantir que:

- Existam procedimentos e ferramentas para proteger, detectar e relatar softwares maliciosos, incluindo (i) implantação de programas, sistemas e metodologias de antivírus; (ii) bloqueio do acesso não-autorizado a redes e computadores; (iii) melhora da conscientização geral dentro da Instituição acerca do uso seguro de

EMBRASI

sistemas e programas computacionais; e (iv) tomada de boas práticas que visem a detecção precoce e a mitigação de incidentes de segurança da informação.

- O pessoal de Tecnologia da Informação seja treinado e proficiente no uso das soluções de segurança usadas para proteger contra *softwares* maliciosos;
- Os usuários finais estejam cientes das políticas de segurança aplicadas em suas estações de trabalho.

2. Gestão de Vulnerabilidades em Ativos Informáticos

Todos os ativos baseados em estações de trabalho ou servidores utilizados pela Instituição devem estar conectados à rede. As unidades autônomas, também conhecidas como computadores externos, devem utilizar *softwares* de proteção antivírus, devidamente aprovados e configurados de acordo com as diretrizes estabelecidas por esta política e pela Política de Segurança da Informação (PSI).

Na gestão de vulnerabilidades em ativos informáticos, os seguintes procedimentos devem ser observados:

- O software de proteção antivírus não deve, em qualquer hipótese, ser desativado ou ignorado, salvo por autorização expressa do Responsável pela 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:		

- As configurações do software antivírus não devem, em qualquer hipótese, ser alteradas, salvo por autorização expressa do Responsável pela Segurança da Informação;
- A frequência de atualizações automáticas do sistema operacional, de aplicativos ou programas não pode ser reduzida em qualquer hipótese, salvo por autorização expressa do Responsável pela Segurança da Informação;
- Todos os servidores conectados à rede devem utilizar o software antivírus aprovado e configurado pelo Responsável pela Segurança da Informação;
- Todos os gateways de correio eletrônico, dispositivos e servidores devem usar software antivírus, antimalwares e antispam aprovados e configurados pelo Responsável pela Segurança da Informação, devendo seguir os ditames da Política de Segurança da Informação;
- Qualquer ameaça que não seja automaticamente limpa, colocada em quarentena e posteriormente excluída pelo software de antivírus constitui um incidente de segurança e deve ser reportada ao Responsável pela Segurança da Informação;
- As atualizações de assinatura de antivírus devem ocorrer em uma frequência definida pelo responsável pela segurança da informação, devendo ocorrer no mínimo uma vez ao mês.

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

3. Instalação e Gerenciamento de Aplicativos

Todos os softwares autorizados devem ser instalados pela equipe responsável dentro da Instituição, sendo vedada a execução de softwares não autorizados.

4. Licenciamento, Manutenção e Suporte

As ações de manutenção, tais como (i) atualizações de software; (ii) atualizações de definição de antivírus; e (iii) log de infecções, devem ser devidamente registradas e retidas por um período a ser definido pelo Responsável pela Segurança 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:

- Instalação de software antivírus em todos os sistemas;
- Varredura regular de ameaças, capaz de detectar, remover e proteger contra tipos próprios de software malicioso;
- Monitoramento proativo e implementação de medidas, visando apoiar esta política;

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

- Existência de medidas que impeçam o usuário de desabilitar ou modificar as ferramentas de antivírus 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 da proteção antivírus caso os softwares de proteção utilizados pela Instituição sejam desabilitados ou desativados.