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 Acesso Remoto e à Rede.

Objetivo

Estabelecer regras para acessar e usar a infraestrutura de rede em ambientes internos e externos à Instituição. Estas regras são necessárias para preservar a integridade, a disponibilidade e a confidencialidade das informações confidenciais armazenadas e tratadas pela Instituição.

Visão Geral

O aumento exponencial dos fluxos de dados em rede, na chamada era da informação, leva à necessidade do desenvolvimento e melhoramento contínuo da infraestrutura de rede utilizada pela Instituição.

Desta maneira, é crucial a manutenção dos pilares da segurança da informação, sobretudo no que diz respeito ao acesso às informações mantidas pela Instituição, inclusive em regime de trabalho remoto.

1. Diretrizes de Acesso à Rede

Os integrantes da Instituição autorizados têm acesso permitido apenas aos recursos e sistemas aprovados pelo Responsável pela Segurança da Informação, devendo agir em conformidade com a Política de Segurança da Informação.

EMBRASI

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:		

Os integrantes não envolvidos diretamente no gerenciamento de sistemas de segurança da informação não estão autorizados a:

- Ampliar ou retransmitir os serviços de rede utilizados pela Instituição sem autorização expressa do Responsável pela Segurança da Informação;
- Instalar ou modificar qualquer *hardware* ou *software* de rede sem a expressa autorização do Responsável pela Segurança da Informação;
- Executar programas de quebra de senhas, farejadores de pacotes, ferramentas de mapeamento de rede ou scanners de porta.
- O Responsável pela Segurança da Informação deve garantir que existam procedimentos e controles que gerenciem:
- A autorização ou supervisão de funcionários que trabalham com informações confidenciais;
- As descrições de trabalho que determinam o nível apropriado de acesso às informações confidenciais mantidas pela Instituição;
- As salvaguardas técnicas que permitem o gerenciamento do acesso às informações confidenciais;
- Os atributos de classificação dos dispositivos de acesso às informações confidenciais mantidas pela Instituição;

EMBRASI

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

- O logoff automático em todos os dispositivos.

2. Diretrizes de Acesso Remoto à Rede

As seguintes diretrizes se aplicam ao gerenciamento de pessoal e ao uso de acesso remoto:

- Os integrantes deverão entrar em contato com o Responsável pela Segurança da Informação para obter métodos e softwares aprovados e adequados para se conectar remotamente aos sistemas internos da Instituição;
- Todos os dispositivos utilizados para o acesso remoto devem ser inspecionados antes de sua utilização, a fim de garantir que o dispositivo esteja devidamente atualizado com todos os pacotes de segurança aplicáveis e com os softwares de proteção contra vírus e malware instalados, conforme diretrizes especificadas na Política de Antivírus e Malware;
- O Responsável pela Segurança da Informação determinará a metodologia de acesso remoto adequada, incluindo medidas de autenticação de senha em dois fatores, cartão inteligente ou *token*, em conjunto com senhas consideradas fortes, conforme diretrizes especificadas na Política de Senhas;
- Os usuários devem garantir que os dispositivos usados para fins de trabalho remoto não sejam compartilhados ou utilizados em atividades inadequadas ou fora do escopo de trabalho;

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

- Os usuários com credenciais de acesso às informações confidenciais da Instituição devem garantir que seu dispositivo de trabalho remotamente conectada não compartilhe conexão com outra rede privada ou pública de internet;
- Os usuários com credenciais de acesso às informações confidenciais da Instituição devem garantir que sua conexão de acesso remoto seja utilizada apenas para as atribuições do seu trabalho;
- Os dispositivos pessoais só devem ser conectados remotamente seguindo as diretrizes da Política de BYOD e com a autorização expressa do Responsável pela Segurança da Informação.