Introdução

A Política de Segurança Cibernética visa prover a metodologia necessária a fim de:

- ✓ Instituir processos e controles para prevenir e reduzir as vulnerabilidades e atender aos demais objetivos relacionados à segurança cibernética;
- ✓ Garantir a proteção dos ativos associados aos negócios críticos, definindo processos para o tratamento de incidentes cibernéticos;
- ✓ Avaliar a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem para garantir a segurança das operações.

Boas Práticas

Procurando sempre as melhores soluções tecnológicas para a utilização dos nossos canais de relacionamento eletrônico, a área de Segurança da Informação tem a responsabilidade de garantir a proteção dos dados, a privacidade, a integridade, a disponibilidade e a confidencialidade das informações sob sua guarda ou de propriedade.

Dicas para usar a Internet de forma segura:

Use senhas para proteger seus dados

- Proteja suas senhas e seus dispositivos utilizados na validação de suas transações. Uma maneira fácil e eficaz de prevenir que pessoas não autorizadas acessem seus dados;

- Certifique-se de que todos os computadores e *notebooks* exijam uma senha criptografada para inicializar.

- Ative proteção por senha ou biometria para dispositivos móveis;

- Utilize dois fatores de autenticação (2FA) para sites que exijam dados pessoais, como bancos e *e-mail*, quando disponível a opção;

- Evite usar senhas comuns como nomes de familiares, datas comemorativas e senhas “camufladas” que possam facilitar o criminoso adivinhar (p@ssw0rd, s3nh@);

- Mantenha sua senha segura, fazendo a troca no mínimo a cada 90 dias dos seus sistemas ou altere sempre que possível ou quando suspeitar de um ataque bem-sucedido.

Um gerenciador de senhas pode ajudar (como *keepass*, *lastpass*). Ele permite a gestão de uma única senha master, onde é possível através dela acessar as outras senhas;

Previna dados – *malware*

Você pode proteger a si mesmo (seu computador) contra os danos causados por *malwares* (*softwares* mal-intencionados, incluindo vírus), adotando técnicas simples:

- Mantenha o *software* antivírus em seus dispositivos eletrônicos (computador, *notebook* e celular) atualizado. Instale somente *softwares* confiáveis e autênticos. Evite realizar *download* de aplicativos de terceiros de fontes desconhecidas;

- Aplique as atualizações de *software* fornecidas pelo fabricante, quando disponível e possível;

- Ative o seu *firewall* (incluído na maioria dos sistemas operacionais) para criar uma zona segura entre sua rede e a internet.

Evite engenharia social

Engenharia social é um método de ataque, onde alguém consegue persuadir, principalmente através de *e-mails*, se aproveitando da ingenuidade ou confiança do usuário, para obter informações privilegiadas (como dados bancários e senhas) que podem ser utilizadas para ter acesso não autorizado a seus dispositivos eletrônicos ou informações.

- Fique atento ao abrir arquivos com extensões .zip, .scr, .exe de origem não confiável, procedência desconhecida ou duvidosa. O cuidado reduzirá o impacto de ataques bem-sucedidos;

- Não acesse sua conta bancária por meio de links contidos em e-mails.

- Nunca informe dados de cartão de crédito e/ou outras informações pessoais em ligações telefônicas.

Evite ataques de *phishing*

Em ataques de *phishing*, os golpistas enviam e-mails falsos solicitando informações pessoais (como dados bancários) ou contendo links para sites maliciosos, tentando se passar por outra pessoa ou empresa confiável.

- Fique atento: Não clique em links que não sejam legítimos. O fraudador utiliza "mascaramentos" para a vítima acreditar que o link seja verdadeiro (verifique sempre se a ortografia e gramática estão corretas)

- Verifique o endereço de *e-mail* do remetente é aparentemente legítimo ou está tentando se passar por alguém conhecido.

Dispositivos seguros (celulares, PCs e *notebooks*)

Smartphones e *notebooks* (que são usados diariamente em qualquer lugar) precisam de MAIS proteção do que os equipamentos de *desktop*. Por isso:

- Configure seus dispositivos eletrônicos para que, quando perdidos ou roubados, possam ser rastreados, apagados ou bloqueados remotamente;

- Sempre utilize conexão 3G, 4G ou *Wi-Fi* particulares (preferencialmente o seu ou de sua empresa) ao enviar dados confidenciais, nunca se conecte a redes públicas de *Wi-Fi*;

- Procure substituir por alternativas quando os dispositivos eletrônicos deixarem de ser suportados por fabricantes. Mantenha seus dispositivos e aplicativos sempre atualizados.

- Importante ter um antivírus instalado no seu computador ou celular. Após a instalação, mantenha sempre atualizado.

Backup dos seus dados

Faça backups regularmente de seus dados críticos, e teste se eles podem ser restaurados. O backup reduzirá o risco de quaisquer roubo de dados, danos físicos, incêndios ou até mesmo *ransomware*.

- Identifique o que precisa ser copiado, incluindo arquivos, *e-mails*, contatos salvos no seu dispositivo.

- Certifique-se de que o dispositivo que contém o *backup* não esteja permanentemente conectado ao dispositivo que contém a cópia original;

- Realize *backup* de seus dados e armazene em um local separado do original.