SEGURANÇA DA INFORMAÇÃO

VOCÊ SABE O QUE É?

SUA EMPRESA PODE ESTAR VULNERÁVEL!

FAÇA A LEITURA DO QR CODE E ACESSE O CONTEÚDO DE FORMA DIGITAL E VEJA MUITO MAIS.

SEGURANÇA DA INFORMAÇÃO CORPORATIVA

SEGURANÇA DA INFORMAÇÃO

É a proteção de um conjunto de informações, em prol de preservar o valor que possuem para um indivíduo ou organização.

SUA IMPORTÂNCIA

Desde que a informação deixou de ser algo sem valor e passou a valer muito dinheiro, foi necessário a criação da Segurança da Informação, onde não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados.

BASE DA SEGURANÇA DA INFORMAÇÃO

Confidencialidade: Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade: Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente).

Disponibilidade: Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Autenticidade: Propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.

Não repúdio: Propriedade que garante a impossibilidade de se negar a autoria em relação a uma determinada transação realizada anteriormente.

MECANISMOS DE SEGURANÇA

Controle Físico: São barreiras que limitam o contato ou acesso direto a informação ou a infra estrutura que garante a existência da informação que a suporta. Exemplos desses mecanismos físicos são: portas, cadeados, trancas, paredes, blindagem, guardas, etc...

Controle Lógico: São barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

DICAS DE PREVENÇÃO CORPORATIVA

Bons equipamentos: Roteadores, Switchs, Firewalls.

Softwares originais e atualizados: Sistema Operacional, Antivírus, Firewall e demais softwares sempre originais.

Infra-estrutura: Bem planejada para segurança das informações.

Cópias das informações: Backups periódicos.

.

Sistema de Gestão de Segurança da Informação (SGSI) com uma boa Política de Segurança da Informação: Verificação de fontes que transmitam algo para sua empresa, criação de boas senhas, fiscalização do ciclo de vida da informação, autorização a determinada informação por

determinada pessoa, IPS (Intrusion Prevention System) forma de segurança de rede que trabalha para detectar e prevenir ameaças identificadas. Os sistemas de prevenção contra invasões monitoram continuamente sua rede, procurando possíveis incidentes maliciosos e capturando informações sobre eles, entre várias outras normas e boas práticas que podem ser encontradas na ISO 27001 e ISO 27002, registradas e documentadas para implementação na empresa.

VULNERABILIDADES E ATAQUES

Ataques cibernéticos ou físicos estão entre as principais preocupações das empresas sérias que se preocupam com os prejuízos que podem sofrer, já que sempre existe o risco de criminosos tentarem invadir o sistema ou adentrar a empresa disfarçados para conseguirem acessar e coletar dados e informações privadas.

Os criminosos podem rastrear dados de acesso da organização, instalar malwares, capturar dados da rede corporativa e afetar arquivos sigilosos. Um ataque famoso dentre os diversos outros que existem é o do tipo DDos (Distributed Denial of Service), a execução ocorre quando um computador mestre utiliza milhares e até mesmo milhões de outros computadores para atacar determinado site, sistema ou servidor, enviando pacotes com intuito de sobrecarregar o sistema e deixá-lo fora do ar e inutilizável, violando o princípio da disponibilidade e causando prejuízos financeiros como físicos. Mediante a este tipo de ataque e a milhares de outros que existem no mundo do crime tecnológico, investir na prevenção e segurança contra qualquer tipo de ataque é indispensável.

LEI GERAL DA PROTEÇÃO DE DADOS

A Lei Geral da Proteção de Dados (LGPD), de número 13.709/18, aprovada em 2019, realiza a regulamentação de como as empresas no Brasil deverão utilizar dados pessoais enquanto informações relacionadas à pessoa natural identificada ou não. A LGPD determina uma transformação no sistema de proteção de dados brasileiros e estabelece regras detalhadas para coleta, utilização, manipulação e armazenamento dos dados pessoais, incluindo a relação entre clientes e fornecedores de produtos e serviços, funcionário e empregador, relações comerciais transnacionais e nacionais, além de abranger outras relações nas quais quaisquer tipos de dados pessoais sejam coletados, tanto no ambiente digital quanto no físico. A lei aplica-se a todos os setores empresariais, afetando todo corporativo socioeconômico brasileiro.

ONDE INVESTIR

Quando falamos em Segurança da Informação, não estamos tratando apenas da proteção da informação em formato eletrônico, mas também de todas as formas de dados, como dados e informações físicas. O nível de segurança necessário corresponde diretamente à importância e ao valor dessas informações e aos prejuízos que a perda ou uso indevido das mesmas poderia acarretar para a empresa.

Manter todos os recursos importantes funcionando corretamente também é um dos motivos para investir na segurança da informação da empresa. Um exemplo são as salas de acesso restrito, que além de proteção contra incidentes como alagamentos ou incêndios, restringe o acesso a colaboradores da área de TI e pessoas autorizadas (Regras que devem ser estabelecidas na Política de Segurança). Equipamentos de segurança como o nobreak, que mantêm os sistemas de informação funcionando em situações de queda de energia também são importantes, entre outros como, dispositivos para backups e vários outros métodos de manter suas informações seguras e salvas.

PRESERVAÇÃO DAS INFORMAÇÕES

As informações da empresa não devem ser apenas protegidas, mas também preservadas. Afinal, se tratam de dados importantes para a administração dos negócios, podendo virem a ser consultadas a qualquer momento.

Cada transação realizada na empresa através de sistemas de informação precisa ser devidamente registrada e mantida em sigilo para proteger os dados de clientes, fornecedores e também da própria organização, a salvo de ataques e exposição. Informações bem preservadas são sinônimo de segurança jurídica e oferecem o suporte apropriado para a tomada de decisões.

CONCLUSÃO

A Segurança da Informação é uma necessidade real para as empresas que prezam pela credibilidade e que não desejam sofrer ataques contra suas informações, ataques os quais podem vir a acarretar em prejuízos enormes como financeiros, judiciais e materiais.
Hoje: A informação não é mais somente informação, a informação é igual a dinheiro!