**SO**

**AULA 1 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**Definição**

Documento formal que estabelece diretrizes, normas e procedimentos para garantir a proteção das informações de uma organização. Ele determina prevenção e respostas para se proteger de ataques.

**Objetivos**

**Confidencialidade**

É garantir que apenas pessoas, sistemas ou processos tenham acesso a algumas informações.

Ex:

* Dados do cliente acessíveis apenas pelo setor de vendas.
* Documentos estratégicos da empresa com acesso restrito.

Como garantir:

* Controle de acesso
* Autenticação forte
* Treinamento e conscientização
* Políticas e procedimentos

Caso ferida:

* Vazamento de dados pessoais ou financeiros;
* Espionagem corporativa;
* Perda de confiança de clientes e parceiros;
* Multas e penalidades legais;
* Danos à reputação da organização.

**Integridade**

É garantir que a informação permaneça exata, ou seja, que a informação não seja alterada durante seu ciclo de vida (criação, armazenamento, processamento e transmissão).

Exemplos:

* Um relatório financeiro deve refletir exatamente os valores lançados sem edições maliciosas.

Como garantir:

* Logs e trilhas de auditoria;
* Assinaturas digitais e checksums;
* Sistemas de versionamento;
* Backups regulares.

Caso ferida:

* Decisões com base em informações erradas;
* Prejuízos financeiros ou operacionais;
* Fraudes internas e externas;
* Problemas legais;
* Perda de confiança dos clientes, parceiros e usuários.

**Disponibilidade**

É garantir que a informação esteja acessível e utilizável pelas pessoas autorizadas sempre que necessário.

Exemplo:

* Backups acessíveis quando há perda ou corrupção de dados.

Como garantir:

* Infraestrutura confiável;
* Política de backups;
* Planos de contingência e continuidade;
* Manutenção preventiva e monitoramento.

Caso ferida:

* Interrupção das operações da empresa ou serviço;
* Perda de vendas, produtividade, reputação;
* Insatisfação de clientes ou parceiros;
* Multas e sanções em setores reguladas (como financeiro e saúde).

**Autenticidade**

É garantir que a informação realmente veio da fonte que afirma e garantir que não foi adulterada no caminho.

Exemplos:

* Um e-mail assinado digitalmente por um gerente, garantindo que foi ele quem enviou.
* Um funcionário acessando o sistema com o seu login e senha, provando sua identidade.

Como garantir:

* Autenticação forte;
* Certificados digitais;
* Assinaturas digitais.

Caso ferida:

* Acesso não autorizado por usuários falsos ou mal-intencionados;
* Phishing e roubo de credenciais, levando a fraudes e vazamento de dados;
* Disseminação de informações falsas atribuídas a fontes confiáveis;
* Danos à reputação da empresa e perda de confiança por parte de clientes e parceiros.

**Legalidade**

É garantir que a informação esteja em conformidade com leis, normas e regulamentações.

Exemplo:

* Cumprir a Lei Geral de Proteção de Dados (LGPD) ao tratar dados pessoais de clientes e funcionários.

Como garantir:

* Políticas internas claras;
* Treinamento e conscientização;
* Registro de consentimento.

Caso ferida:

* Sanções legais e multas elevadas (previstas pela LGPD);
* Danos à imagem institucional e perda de confiança;
* Responsabilização civil e criminal de gestores ou responsáveis pelo tratamento das informações.

**Objetivos Complementares**

* Não repúdio: Garante que uma ação ou comunicação não possa ser negada por quem a realizou.
* Privacidade: Trata do direito do indivíduo controlar como suas informações pessoais são coletadas, usadas e compartilhadas.
* Responsabilidade: Garante que pessoas e organizações sejam responsabilizadas por suas ações sobre dados e sistemas.

**Importância**

* Proteger ativos de informação contra ameaças internas e externas;
* Minimizar riscos de incidentes de segurança;
* Garantir a continuidade dos negócios;
* Estabelecer cultura de segurança na organização;
* Atender requisitos legais e regulatórios.

**Escopo**

O escopo define o que vai ser atingido pela política de segurança.

O escopo determina:

* Quais informações são protegidas pela política;
* Quais sistemas são cobertos;
* Quais unidades organizacionais devem seguir a política.

Elementos comuns que geralmente fazem parte desse escopo:

* Informações digitais e físicas;
* Sistemas operacionais e aplicativos;
* Infraestrutura de rede e comunicações;
* Dispositivos de armazenamento e processamento;
* Ambientes de desenvolvimento, teste e produção;
* Relações com fornecedores e parceiros.

**Objetivo**

**Responsabilidades**

Evitar omissões e garantir que cada pessoa saiba o que se espera.

**Diretoria:**

* Aprovar a política e garantir sua integração às estratégias da empresa;
* Apoiar a alocação de recursos para segurança da informação.

**Segurança da Informação**

Cargos como DPO, CISO, TI são responsáveis por:

* Desenvolver, revisar e atualizar as Políticas de Segurança da Informação;
* Monitorar o cumprimento da política e conduzir auditorias internas;
* Tratar incidentes de segurança.

**Gestores de áreas**

Gestores/Líderes devem:

* Garantir que os funcionários conheçam as diretrizes da política
* --

**Colaboradores em geral**

Devem:

* Conhecer e seguir as diretrizes da política.
* ...

**Fornecedores e terceiros**

Os fornecedores e terceiros devem seguir as seguintes **responsabilidades:**

* Cumprir as cláusulas de segurança acordadas em contrato com a empresa;
* Usar os sistemas e dados da organização de forma segura e autorizada.

**Exemplos de Política**

* **Política de Senhas**
* **Política de Classificação da Informação**
* **Política de Acesso**
* **Política de Dispositivos Móveis**
* **Política de Resposta a Incidentes**

**Tabela RACI**

Ferramenta de gestão de projetos que ajuda a definir e comunicar as funções e responsabilidades de cada membro da equipe em relação a tarefas, entregas e marcos.

R – Responsável

A – Aprovador

C – Consultado

I – Informado