PROGRAMA
LGPD 13.709
CONSULTORIA ESPECIALIZADA

APOSTILA EPISÓDIO-6
A LGPD E O TI / SI

A área de **TI - Tecnologia da Informação** se apresenta em uma posição significativamente importante e com altíssimo grau de vulnerabilidade, perante a Lei Geral de Proteção de Dados - LGPD, face ao conjunto de dados que por ela transitam.

Desta forma, a atenção deverá estar voltada em assegurar por meio de rotinas, processos e procedimentos, o fiel cumprimento da Lei Geral de Proteção de Dados (LGPD), no propósito de garantir a proteção absoluta dos dados.

Para tanto, partindo da alta gerencia, faz-se necessário disseminar orientações interdepartamentais, dando suporte às áreas envolvidas, de forma a privilegiar e ter como ponto de partida a revisão sistêmica dos processos e procedimentos internos, que levem ao pleno atendimento da lei quanto à garantia da segurança das informações, com o especial cuidado voltado para que estas estejam protegidas a ataques de hacker e/ou a compartilhamento não permitido, assegurando assim que a organização esteja em conformidade com o atendimento da legislação, livre de incidentes e isenta de penalidades.

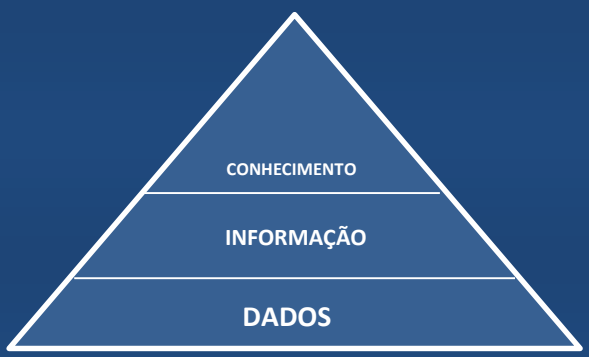
DEFINIÇÃO DE DADO:

Conjunto de atributos. Uma série de fatos discretos. Exemplo:

- CPF, Nome, Endereço, Idade, Sexo
- Escolaridade, Renda presumida, Entre outros....

O dado não possui significado relevante e não conduz a nenhuma compreensão.

DEFINIÇÃO DE INFORMAÇÃO



A informação é a ordenação e organização dos dados de forma a transmitir significado e compreensão dentro de um determinado contexto. É o conjunto ou consolidação dos dados de forma a fundamentar o conhecimento.

É um conjunto de dados que tem significado em algum contexto. É a compreensão dos relacionamentos entre dados.

A informação pode responder a uma das 4 perguntas: **QUEM** - **O QUÊ – QUANDO – ONDE**

"INFORMAÇÃO É O RESULTADO DE APLICAR CONTEXTO AOS DADOS"

COMO ALCANÇAR A SEGURANÇA DA INFORMAÇÃO?

A **SI - Segurança da Informação** é alcançada através da implementação ou revisão do conjunto de controles, rotinas e procedimentos, em especial voltados a: Políticas, Processos, Procedimentos, Estrutura organizacional, Funções de software, hardware, backup's, entre outros.

Algumas recomendações de segurança :

- ✓ **Controles de acesso**: barreiras que impeçam ou limitem o acesso a informações, que estejam em ambiente controlado, geralmente eletrônico
- ✓ **Assinatura digital:** controles individuais rigidos por logs de acesso (por usuário)
- ✓ **Honeypot**: ferramenta que tem a função de propositadamente vir a simular falhas de segurança em determinado sistema e identificação do invasor
- ✓ **Protocolos seguros**: uso de protocolos que garantam satisfatório grau de segurança e de acompanhamento do fluxo da informação
- ✓ **Anonimização:** ou pseudoanonimização dos dados pessoais.

SISTEMA DE INFORMAÇÃO: Descreve o **Processamento**, o **Armazenamento** e a **Transferência** de Informações. *Não deve ser entendido como Sistema de TI.*

Formas da Informação:

- Impressa ou escrita
- Transmitida por correio eletrônico ou por qualquer meio digital
- Verbal (conversas ou apresentações)
- Armazenada eletronicamente (Planilhas, Banco de dados, back-up....)
- Armazenada fisicamente (Arquivos, gavetas., papéis sobre a mesa....)
- Apresentada em filmes e/ou vídeos.

A Forma da informação irá impor restrições às medidas necessárias para sua proteção.

O objetivo do Sistema de Informação é *entender* e *analisar* como ocorre o impacto da adoção das tecnologias de informação nos processos de decisão gerenciais e administrativos das organizações. Pode trabalhar com diversos elementos. Entre eles estão software, hardware, banco de dados, sistemas especialistas, sistemas de apoio etc.

Nele estão inclusos todos os processos informatizados, que podem disponibilizar a informação correta e fazer a organização funcionar de maneira adequada.

TECNOLOGIA DA INFORMAÇÃO ≠ SISTEMA DE INFORMAÇÃO

Tecnologia da Informação (TI) é usada para:

COLETAR --- TRANSFERIR --- ARMAZENAR --- PROCESSAR

Tecnologia da Informação refere-se, de modo geral, à coleção de recursos de informação de uma organização, seus usuários e a gerencia que os supervisiona, inclusive a infraestrutura de TI e todos os outros sistemas de informação em uma organização.

A introdução de Sistema da Informação/Tecnologia da Informação em uma organização irá provocar um conjunto de alterações, nomeadamente em nível das relações da organização com o meio envolvente (analisadas em termos de eficácia) e em nível de impactos internos na organização (analisados através da eficiência).

A Tecnologia da Informação é um recurso valioso e provoca repercussões em todos os níveis da estrutura organizacional.

Segurança da Informação é de fundamental importância para qualquer empresa, principalmente para o setor de TI.

Mais do que estratégica, a *Segurança da Informação* é essencial para a proteção do conjunto de dados da corporação.

Segurança da Informação diz respeito ao *conjunto de ações* para *proteção* de um grupo de dados, protegendo o *valor* que ele possui, seja para um indivíduo específico no âmbito pessoal, seja para uma organização.

É a preservação da **CONFIDENCIALIDADE**, da **INTEGRIDADE** e da **DISPONIBILIDADE** das informações.

A Segurança da Informação não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma.

É importante lembrar que a Segurança da Informação também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

A Gestão de Risco eficiente é aquela realizada de fora para dentro da organização. Porque é imune a políticas, influências ou interesses pessoais.

Segundo a definição do que é gerenciamento de riscos da ISO 31.000, uma gestão de risco eficaz deve atender os seguintes princípios:

- Proteger e criar valor para as organizações.
- Ser *parte integrante de todos os processos* organizacionais.
- Ser considerada no processo de tomada de decisão.
- Abordar explicitamente à incerteza.
- Ser *sistemática*, estruturada e oportuna.
- Basear-se nas melhores informações disponíveis.
- Estar alinhada com os contextos *internos* e *externos* da organização e com o perfil do risco.
- Considerar os fatores humanos e culturais.
- Ser *transparente* e *inclusiva*.
- Ser *dinâmica*, *interativa* e capaz de reagir às mudanças.
- Permitir a melhoria contínua dos processos da organização.

A **PSI - Política de Segurança da Informação** é o documento que orienta e estabelece as diretrizes organizacionais no que diz respeito à proteção de ativos de informação, devendo, portanto, ser aplicado a todas as esferas de uma instituição.

Uma boa **PSI** deve conter ***regras e diretrizes que orientem os colaboradores, clientes e fornecedores*** (bem como a própria TI da organização) com relação aos padrões de comportamento ligados à segurança da informação, condições de instalações de equipamentos, restrições de acesso, mecanismos de proteção, monitoramento e controle, entre outros cuidados imprescindíveis aos processos de negócio.

O objetivo é preservar as informações quanto à ***integridade***, ***confidencialidade*** e ***disponibilidade***.

O QUE DEVE ESTAR PRESENTE EM UMA PSI

Um bom documento que trate de política da segurança da informação deve conter, além dos *objetivos*, *princípios* e *requisitos* do documento, as seguintes normatizações:

- **Responsabilidades dos colaboradores:** Diz respeito à imposição dos limites de uso, bem como às responsabilizações em caso de má utilização dos recursos de TI da empresa. Nesse trecho, poderão ser inseridos regramentos com relação à impossibilidade de uso de dispositivos externos em

equipamentos corporativos, informações sobre websites de acesso proibido, recomendações de preservação do maquinário da empresa, etc.

- **Responsabilidades da área de TI:** Organizar a logística da TI da organização, configurar os equipamentos, instalar softwares e implementar os controles necessários para cumprir os requerimentos de segurança estabelecidos pela política de segurança da informação são fundamentais para que o documento elaborado tenha vida e funcionalidade na dinâmica da organização.

- **Informações ligadas à logística da implementação da TI na organização:** Refrigeração de data centers, gestão de aplicações, organização física dos ativos de rede, recomendações de procedimentos, etc. Tudo o que for relacionado à implementação da infraestrutura de TI na organização pode ser descrito nesse capítulo, o qual servirá como norte nessa seara.

- **Tecnologias de defesa contra ciberataques:** Big Data Analytics contra crackers, firewall, criptografia, controles de acesso, backups, auditorias, monitoramento de rede: esses são apenas alguns mecanismos de defesa utilizados nas empresas de sucesso para controle de dados sigilosos e que devem ser descritos em um documento de segurança da informação.

Os seguintes itens formam a base para os documentos de politicas.

REGULAMENTOS	• Deverão ser mais detalhados que um documento de politicas • São obrigatórios • O não cumprimento pode levar a procedimentos disciplinares
PROCEDIMENTO	• Descrevem em detalhes como medidas particulares devem ser realizadas • Exemplo: politica da mesa limpa
DIRETRIZES	• Fornecem orientações • Não são obrigatórias mas servem como consulta
NORMAS	• Definem PADRÕES • A ISO/IEC 27001 é uma norma para configurar a PSI na organização.

Como garantir que a Política de Segurança da Informação funcione na prática.

- **Planejamento**: fundamental para que seja definido o perfil da empresa, suas peculiaridades, vulnerabilidades potenciais e necessidades específicas de proteção, que irão circundar o documento a ser elaborado;

- **Levantamento** minucioso dos sistemas de proteção da empresa e seus ativos críticos, listando quais os principais fatores de riscos e possíveis deficiências;
- **Integração de toda a equipe**: desenvolva um trabalho de endomarketing para ajudar na conscientização de que *segurança da informação é responsabilidade de todos*. Da alta cúpula aos estagiários, todos na empresa devem ter ciência de suas responsabilidades para evitar a violação de dados;
- **Ter o auxílio** de uma *empresa especialista em segurança da informação*, tanto na elaboração do documento quanto no gerenciamento de riscos, detecção de fraudes e *serviços gerenciados de segurança*, é essencial para assegurar proteção em alto nível dos serviços computacionais da organização;
- **Revisão e monitoramento** constante acerca da implementação efetiva das normas previstas.

CÓDIGO DE CONDUTA

Deve ser utilizado para estabelecer as responsabilidades de segurança da informação do funcionário ou parte externa quanto a *confidencialidade*, *proteção de dados*, *ética*, uso apropriado dos equipamentos e recursos da organização, assim como as praticas respeitosas esperadas pela organização.

O código de conduta poderá conter as sanções que são impostas em caso de descumprimento e se incidentes de segurança surgirem como resultado.

O "Código de Conduta" poderá definir:

- Que e-mails pessoais não são permitidos
- Terceiros devem cumprir todos os requisitos de segurança da informação
- Para utilização dos e-mails corporativos a pessoa declara entender a legislação e aderir ao acordo de confidencialidade
- Conscientizar os funcionários sobre ameaças de segurança como malware, pishining e spams
- Utilização de telefone fixo ou móvel para fins pessoais só serão permitidos dentro do estipulado pela organização.

POLÍTICAS DE SEGURANÇA

Algumas políticas que poderão ser implementadas:

Política para o uso de dispositivos móveis: Deverá considerar:

- Registros dos dispositivos móveis

- Restrição quanto a instalação de softwares e conexão aos serviços de informação
- Controle de acesso com técnicas criptográficas
- Proteção contra códigos maliciosos
- Desativação, bloqueio e exclusão de forma remota
- Backups

Politica de trabalho remoto: Deverão ser considerados

- A organização somente deverá permitir o trabalho remoto com base em uma avaliação de risco
- Autorização
- Provisão de equipamento
- Segurança da informação para trabalho remoto .

Gerenciamento de Incidentes de Segurança da Informação:

Detectar, *Relatar*, *Avaliar*, *Responder*, *Tratar* e *Aprender*"

Para que uma organização realmente consiga minimizar os impactos ocasionados por incidentes de segurança da informação, é importante que esse seja um processo estruturado. E para isso, convém que os procedimentos envolvidos na notificação, registro, monitoramento e resolução de incidentes, bem como os responsáveis por esses procedimentos, estejam descritos em um documento formal aprovado pela direção.

Um dos assuntos que o plano deve abordar é o da priorização de ações em caso de incidentes. O importante é que a ordem de execução dessas ações esteja ajustada para uma resolução de problemas que seja mais eficiente e que ocorra num menor tempo possível.

Recomenda-se ainda que o plano de gestão de incidentes de segurança da informação defina os controles de auditoria, utilizados tanto na investigação de incidentes quanto na determinação das causas e notificação.

NOTIFICAÇÃO: Para que os incidentes de segurança da informação possam ser notificados o mais rapidamente possível, quando de sua ocorrência, a organização precisa possuir canais de comunicação formais, acessíveis, de fácil utilização, que estejam sempre disponíveis e que, preferencialmente, preservem a identidade da pessoa que acusou o incidente.

A escolha da forma como esse canais de comunicação serão implementados (e-mail, formulário, sistemas específicos etc.) deve envolver, além dos setores de tecnologia e segurança da informação, os proprietários da informação.

Em ambientes de alto risco, deve ser avaliada a adoção de alarmes de coação, que são aqueles dispositivos que, quando acionados, sinalizam de forma secreta a ocorrência de um incidente de segurança.

RESPONSABILIDADES: Os funcionários, fornecedores e terceirizados precisam ter consciência de que possuem responsabilidades para com a notificação de incidentes de segurança da informação e também com os procedimentos utilizados nessa notificação.

O QUE É SISTEMA DE GESTÃO EM SEGURANÇA DA INFORMAÇÃO - SGSI?

O conceito de segurança da informação se refere à proteção de um determinado conjunto de dados para preservar o valor que ele possui, seja para um indivíduo, seja para uma organização. Nesse sentido, a gestão é a *prática de adoção de estratégias*, *métodos*, *ações* e *ferramentas* para alcançar esse objetivo.

O papel do gestor está diretamente relacionado por isso. Cabe a ele definir de que forma a segurança da informação será tratada, sistematicamente. Em outras palavras, é preciso planejar a estratégia e monitorar o cumprimento das práticas adotadas pela empresa.

Para nortear esse processo, é importante ter em vista os quatro pilares da segurança da informação:

- confidencialidade;
- integridade;
- disponibilidade;
- autenticidade.

Isso significa que as informações devem ser mantidas continuamente ao alcance de quem está autorizado a acessá-las e, ao mesmo tempo, protegidas contra vazamentos, ataques e danos em geral.

A organização deve definir quais são os pontos de controle e as possíveis ameaças. No primeiro caso, a infraestrutura de TI (softwares e hardwares), as redes lógicas e até mesmo os dados pessoais devem fazer parte desse escopo. Já as ameaças podem variar de acordo com esses pontos de controle e a dinâmica de trabalho da companhia.

A gestão define, então, as melhores práticas de segurança a serem adotadas *por todos os colaboradores*. O uso de e-mail e a navegação na internet, por exemplo, podem ser limitados de acordo com aquilo que for considerado adequado para a companhia.

O mesmo se aplica ao acesso à rede da empresa, seja via Wi-Fi em dispositivos móveis, seja por cabos de rede, USB, WDMI etc.

PROGRAMA
LGPD 13.709
CONSULTORIA ESPECIALIZADA

CAPACITAÇÃO GRATUITA

No intuito e democratizar as informações sobre a Lei 13.709/18 – LGPD, disponibilizamos, **SEM NENHUM CUSTO**, aos colaboradores da sua empresa, nosso "*Curso Básico Passo a Passo Adequação LGPD*", inclusive com avaliação final e emissão de **Certificado de Participação**.

Este curso, On-Line e disponível em plataforma profissional, já formou algumas centenas de profissionais nas mais diversas áreas.

Para maiores detalhes e inscrição de seus colaboradores, entre em contato por qualquer um dos canais abaixo.

contato@lgpd13709.com.br
www.lgpd13709.com.br
www.lgpd4me.net
1144850215 (voz e WhatsApp)

PROGRAMA
LGPD 13.709
CONSULTORIA ESPECIALIZADA