COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

ASPECTOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD), SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Módulo I - Básico

INSTRUTOR:
CHARLES ROGÉRIO VASCONCELOS

ESCON
ESCOLA SUPERIOR DE CONTAS

Objetivo do Treinamento

O objetivo do treinamento é dar prosseguimento às ações previstas pelo Comitê de Segurança da Informação e Comunicação – COSIC, para implantação do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados no âmbito do TCE-RO, em conformidade com o artigo 50 da LGPD, e assim, capacitar o capital humano deste Tribunal, considerando aspectos legais de segurança da informação e privacidade de dados, e ainda, sobre a Lei Geral de Proteção de Dados Pessoais.

Ementa do Curso

Apresentação

- Apresentação do Comitê de Segurança da Informação e Comunicação - COSIC
- Apresentação do Encarregado de Proteção de Dados - DPO
- Apresentação do Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados - PCGSIPD

Informação Corporativa

- Objetivos
- Dado, Informação, Conhecimento e Sabedoria
- Evolução da Cadeia
- Importância Corporativa
- Arquitetura
- Ciclo de Vida
- Classificação
- **Segurança da Informação e Privacidade**
- Conceitos
- Objetivos
- Norma NBR ISO/IEC 27002
- Histórico no Brasil
- Importância de zelar
- Linha do Tempo no TCE-RO
- Pilares da Segurança da Informação
- Segurança Estratégica

Ementa do Curso

Cenário Global

- Incidentes de Segurança da Informação
- Estatísticas
- Sistemas Alvo
- Incidentes em Ambiente Governamental
- Indicadores de Tentativas de Intrusão à Rede do TCE-RO
- Grupos de Segurança e Resposta a Incidentes no Brasil

Ambiente Corporativo Gerenciado

- Política de Segurança da Informação
- Rede Corporativa Gerenciada
- Vulnerabilidades
- Riscos
- Ameaças
- Vírus
- Engenharia Social
- Falsificação de Identidades nas Redes Sociais
- Phishing
- Ransomware

Ementa do Curso

Gerenciamento de Senhas
- Senhas seguras
- Elaborando boas senhas
- Alteração de senhas
- Gerenciamento de senhas
- Ferramentas
- Uso de redes seguras
- Uso inteligente do e-mail corporativo

Aplicando Segurança da Informação
- Proteja seu Dispositivo
- Proteja seu Smartphone

Linhas de Defesa
- Antivírus
- Firewall
- VPN

Cuidados com os Dados
- Backup
- Uso seguro de backup
- Backup pessoal
- Backup corporativo
- Descarte seguro de informação

Ementa do Curso

Lei Geral de Proteção de Dados Pessoais

- O Mundo dos Dados
- Big Data
- Data Science
- Inteligência Artificial
- Artigo 1º
- Tratamento de Dados Pessoais pelo Poder Público
- LGPD e LAI - Harmonização

Conceitos

- Dado Pessoal
- Dado Pessoal Sensível
- Consentimento
- Anonimização
- Tratamento de Dados
- Áreas Afetadas
- O que será preciso fazer?

Ementa do Curso

Atores da LGPD

- Titular de Dados Pessoais
- Agentes de Tratamento
- Encarregado de Proteção – DPO
- Autoridade Nacional de Proteção de Dados – ANPD
- Fluxo de Comunicação entre os Atores
- Cases de Incidentes - LGPD

Sanções Previstas

- Mapeamento de Fluxo de Dados
- *Roadmap* para Implementação
- Fases do Programa
- Cronograma
- Estratégia
- Referências

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Instituição do COSIC

Resolução nº. 287/2019/TCE-RO - Art. 1º Instituir o Comitê de Segurança da Informação e Comunicação - COSIC, que tem como objetivo **estabelecer diretrizes e propor políticas, normas e procedimentos** gerais relacionados à gestão informacional e do conhecimento no âmbito do Tribunal de Contas de Rondônia.

Composição do COSIC

- Art. 2º O Cosic será composto pelos seguintes membros:
- I – O posto de presidente do Comitê será ocupado por um membro da Corte, a ser designado pelo presidente do TCE-RO;
- II – Chefe de gabinete da Corregedoria-Geral;
- III – Chefe de gabinete da Presidência;
- IV – Secretário estratégico de Tecnologia da Informação e Comunicação;
- V – Secretária-Geral de Administração;
- VI – Secretário-Geral de Controle Externo;
- VII – Representante da Assessoria de Segurança Institucional;
- VIII – Representante do Gabinete da Ouvidoria; e
- IX – Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO).

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Nomeação do Encarregado de Proteção de Dados - DPO

Dando cumprimento à Lei Geral de Proteção de Dados Pessoais - LGPD, art. 41, o Tribunal de Contas do Estado de Rondônia, através da portaria nº. 189 de 27 de fevereiro de 2020, nomeou seu Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO).

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Gestores de Segurança da Informação e Privacidade

Atuarão, sob coordenação do DPO, disseminando as boas práticas institucionais relacionadas à segurança da informação e privacidade de dados, além de participar das equipes de trabalho para elaboração da nova Política Corporativa de Segurança da Informação do TCE-RO e adequação à LGPD. Em consonância com o controle 6.1.1 da NBR ISO/IEC 27002.

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Implantar um PCGSIPD (art. 46, 47, 48, 49 e 50 da LGPD) (ISO 27002)

O Programa Corporativo de Gestão da Segurança da Informação e Privacidade de Dados - PCGSIPD será implantado com base nas **normas ISO 27000**, objetivando aumentar o nível de confidencialidade, integridade e disponibilidade das informações do TCE-RO, e adequação à **Lei nº. 13.709/2018** - Lei Geral de Proteção de Dados Pessoais - LGPD, delineando ações para a aplicação de diretrizes visando maximizar o desempenho do Tribunal nos aspectos de segurança da informação e privacidade.

PCGSIPD


PROGRAMA CORPORATIVO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃOE PRIVACIDADE DE DADOS
Política Corporativa de Segurança da Informação
FAMÍLIA ISO 27000
9 Políticas Críticas
15 Políticas Básicas
24 Políticas no Total
Programa de Conformidade à Lei Geral de Proteção de Dados
LGPD
6 Fases Críticas
3 Ações Complementares
9 no Total

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Informação Corporativa

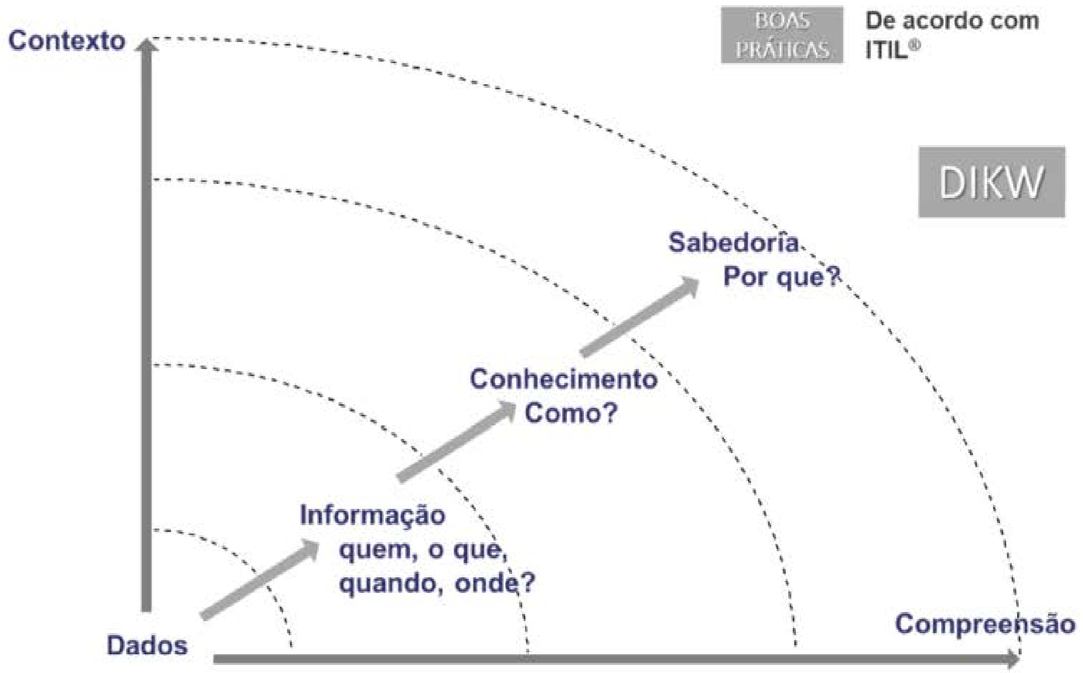
Cadeia

1. Dado
2. Informação
3. Conhecimento
4. Sabedoria

Fonte: Workbook 27001 - Master House Consultoria e Treinamento

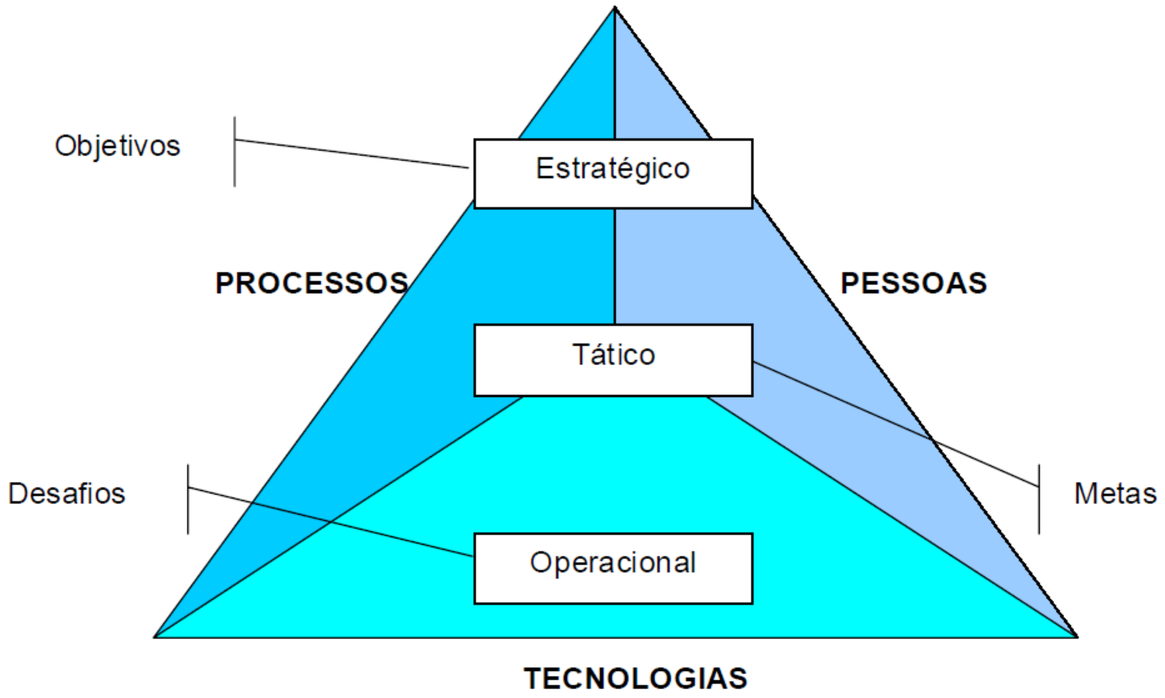
A evolução da cadeia

A evolução dessa cadeia objetiva transformar **dados** em **informações** confiáveis para serem utilizadas como fonte de **conhecimento** para tomar decisões com **sabedoria**.



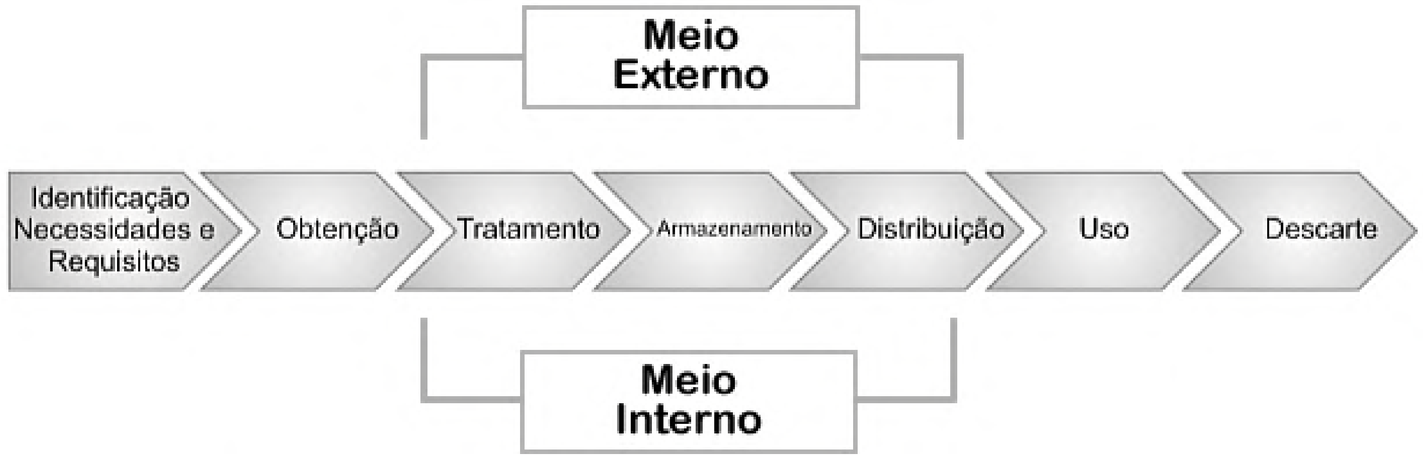
Importância Corporativa

A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário. A informação **tem um valor altamente significativo** e pode representar grande poder para quem a possui. A informação contém valor, pois está integrada com os processos, pessoas e tecnologias.



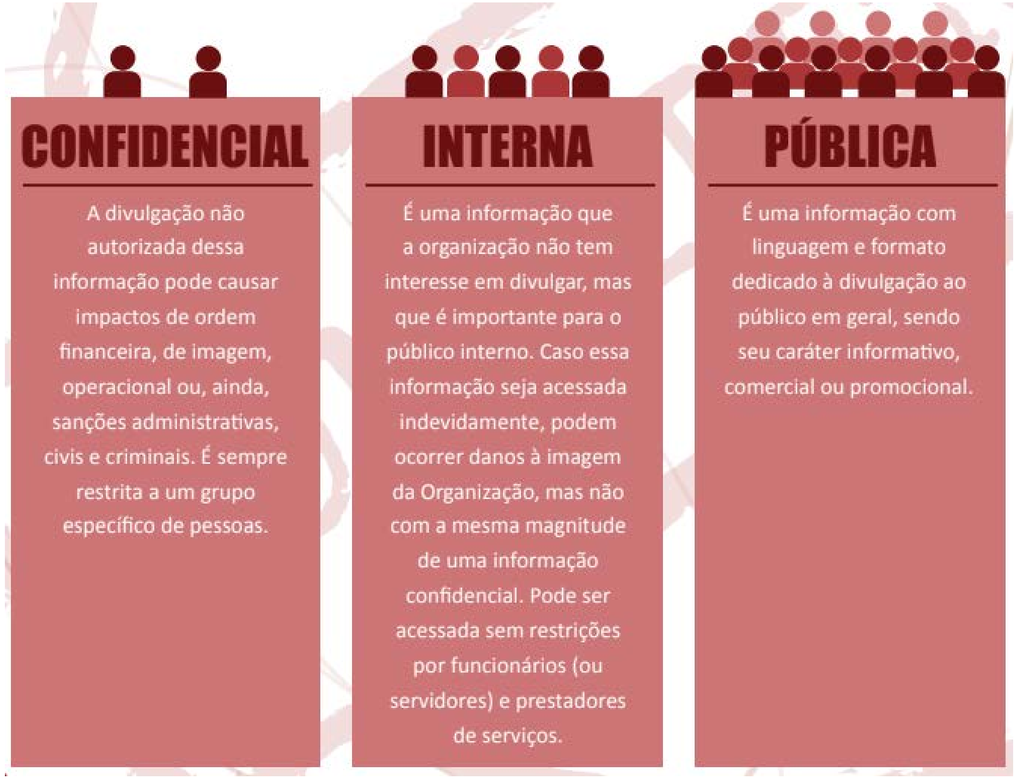
Fonte: Rezende e Abreu, 2000

Ciclo de Vida



Fonte: Curso de Segurança e Auditoria de Sistemas - UNIS

Classificação da Informação



Fonte: Programa de Conscientização - STJ

VÍDEO

- **Programa de Conscientização STJ: Segurança da Informação (link)**

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

EXERCÍCIO

- **Quiz**

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Segurança da Informação e Privacidade

Conceitos

A segurança da informação é obtida a partir da implementação de um **conjunto de controles** adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

Segunda o norma ISO 27002, Segurança da Informação é a proteção da informação contra os mais diversos tipos de ameaças para garantir a **continuidade dos negócios**, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio.

Privacidade

É qualidade do que é privado, do que diz respeito a alguém em particular; intimidade pessoal; vida privada.

Constituição Federal, artigo 5º, inciso X, "são invioláveis a intimidade, **a vida privada**, a honra e a imagem das pessoas [...]".

Código Civil, artigo 21, "**A vida privada** da pessoa natural é inviolável".

Marco Civil da Internet, artigo 3º, princípios:

II - **proteção da privacidade**;
III - **proteção dos dados pessoais**, na forma da lei;

Objetivos da Segurança da Informação

Visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações tratadas pela instituição. (TCU)

Norma NBR ISO/IEC 27002

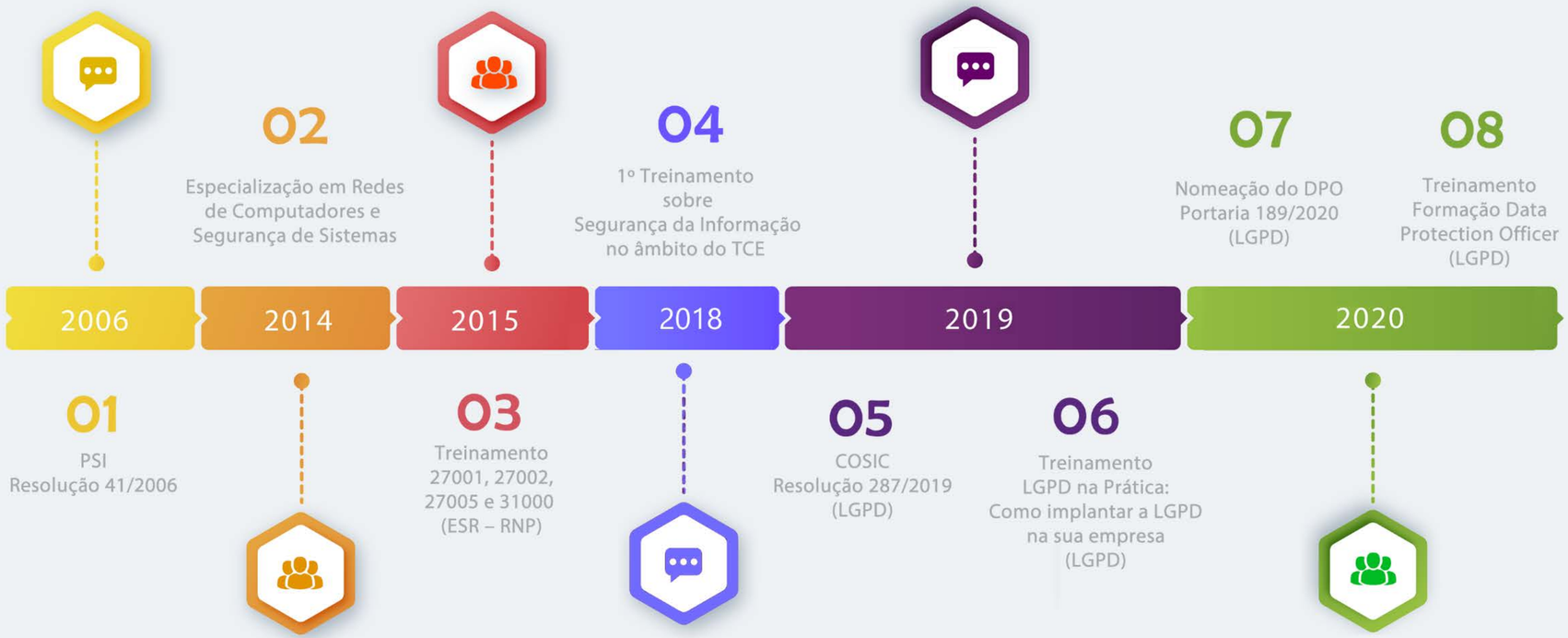
Esta Norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Especifica um código de prática para um Sistema de Gestão de Segurança da Informação.

Importância de zelar pela Segurança de Informações

A informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. (TCU)

Linha do Tempo no TCE-RO



COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Como ter segurança e privacidade nesse mundo tecnológico?

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Pilares da Segurança da Informação

Confidencialidade

Necessidade de garantir que as informações sejam divulgadas somente àqueles que possuem autorização para vê-las.

Integridade

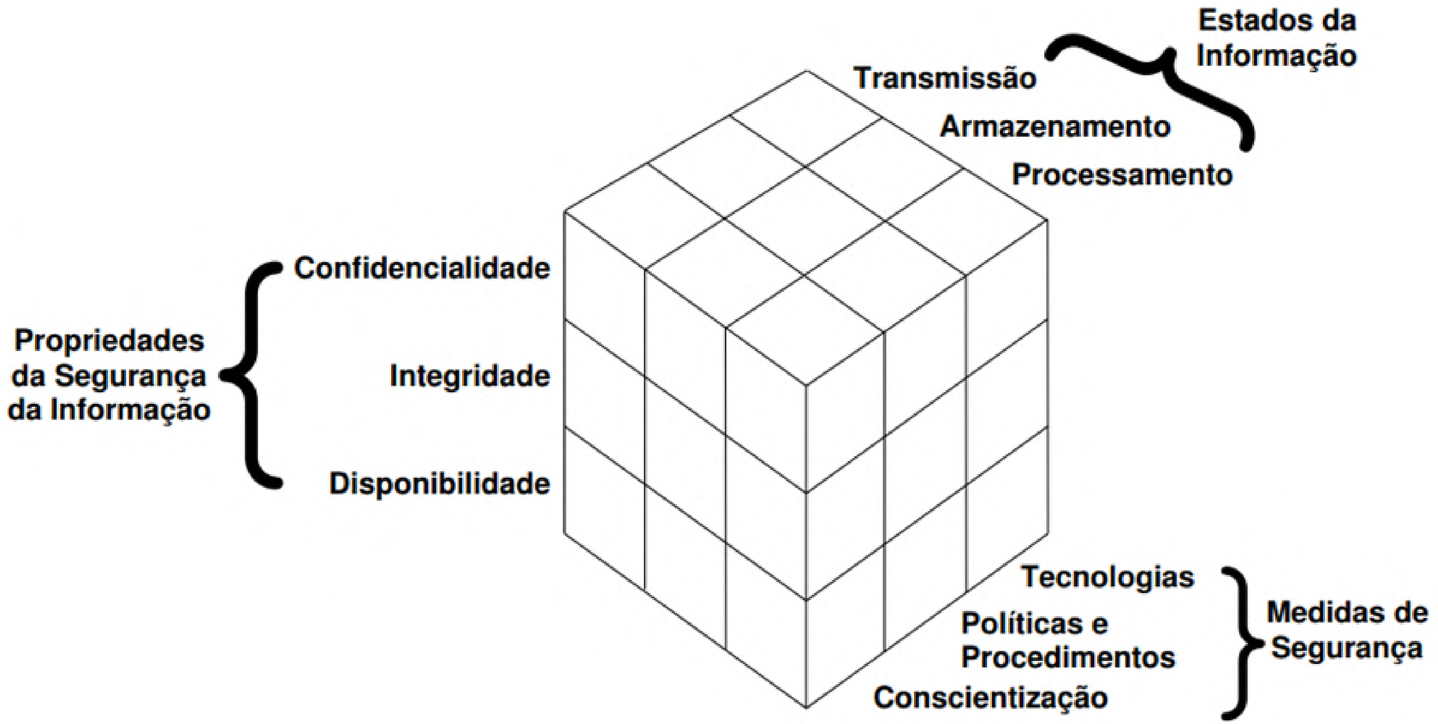
Necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Disponibilidade

Necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

IMPORTANTE: Devem ser adotados cuidados tanto no ambiente corporativo quanto no pessoal.

A Segurança da Informação depende de múltiplos fatores



Fonte: Programa de Conscientização - STJ

Segurança (Estratégica) da Informação

A informação e o conhecimento baseado nessa informação são reconhecidos como **ativos** de informação. São ativos críticos de negócio, sem os quais a maioria das organizações simplesmente deixaria de funcionar. Estes ativos são habilitadores de negócio, recursos vitais, exigindo das organizações proteção adequada.

Para se atingir efetividade e sustentabilidade no mundo interconectado e complexo de hoje, a segurança dos ativos de informação **deve ser abordada nos níveis mais altos da organização, não pode ser encarada apenas como uma especialização técnica da área de TI** e deve ir além das fronteiras corporativas através de seus colaboradores.

Fonte: Programa de Formação de Especialistas para a Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – CEGSIC

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Cenário Global

Incidente de Segurança da Informação

É qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação.
(NBR 27002).

Fonte: NBR ISO/IEC 27002

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Incidentes de Segurança da Informação

EUA indiciam norte-coreano por invasão à Sony e ataque hacker ...
https://tecnologia.uol.com.br/noticias/.../eua-indiciam-norte-coreano-por-invasao-a-so...
6 de set de 2018 - EUA indiciam norte-coreano por **invasão** à Sony e ataque **hacker** ...

Deslogou aí? Facebook admite ataque hacker que afetou 50 milhões .
https://tecnologia.uol.com.br/noticias/.../facebook-descobre-falha-que-afeta-50-milhoe...
28 de set de 2018 - Segundo a companhia, **hackers** aproveitaram uma falha no código da ...

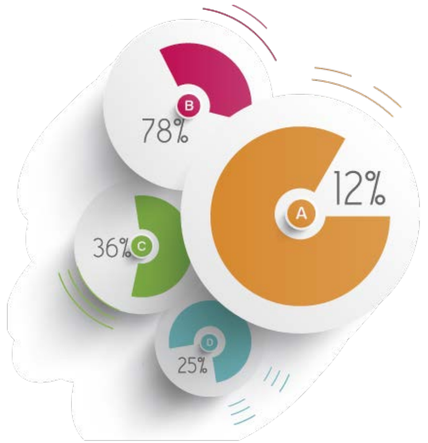
Brasil é país que mais sofre com ataques de ransomware na AL | Blog ...
https://www.kaspersky.com.br › Blog oficial da Kaspersky Lab › Notícias
11 de set de 2017 - Ao todo, os **ataques** do **ransomware** na AL registraram crescimento anual de ...

Vírus sequestra dados de brasileiros e só aceita resgate em bitcoins ...
https://www.techtudo.com.br/noticias/noticia/.../virus-sequestra-dados-de-brasileiros-e-...
30 de mar de 2014 - Uma nova onda de ataques de **hackers** vem obtendo **dados** de ... Vírus

Vulnerabilidade grave é descoberta nos navegadores Firefox e Edge
https://www.welivesecurity.com/.../vulnerabilidade-grave-e-descoberta-nos-navegador...
22 de jun de 2018 - A **vulnerabilidade** foi **descoberta** pelo pesquisador do Google Jake ...

STJ e outros órgãos do governo são alvos de ataques ...
5 dias atrás — Brasil é o país mais atingido por **ataques** de **ransomware** na América ... O **STJ** não foi o único órgão público a **sofrer** investidas digitais nas ...

Brasil sofre seu maior ataque hacker da história | VEJA
5 dias atrás — **Superior Tribunal de Justiça**, Ministério da Saúde e Distrito Federal ... da Polícia Federal, foram alvos de um **ataque** por meio de **Ransomware**.



Fonte: Google

Estatísticas

ATAQUES DIGITAIS NO BRASIL

E-MAILS FALSOS: **33%**

SITES MALICIOSOS: **30%**

SOFTWARES BAIXADOS: **22%**

FONTE: NETSCOUT

PREOCUPAÇÕES

VAZAMENTO DE DADOS: **77,5%**

DANOS AO NEGÓCIO: **66%**

FONTE: NETSCOUT

ATAQUES CIBERNÉTICOS

46,3% consideram a segurança digital uma prioridade

10% sentem que estão totalmente protegidas

70,3% não quantificaram qual seria o impacto

AÇÕES NA JUSTIÇA

2019: **17 mil**

2002: **400**

Fonte: Fortinet

BRASIL

15 BILHÕES
tentativas de ciberataques

Em **3 meses** de 2019

Fonte: Fortinet

Sistemas Alvo (Governo)

Em ataques cibernéticos recentes, grupos de hackers têm considerado sistemas de governo como alvos compensadores, no intuito de provocar diferentes impactos, como:

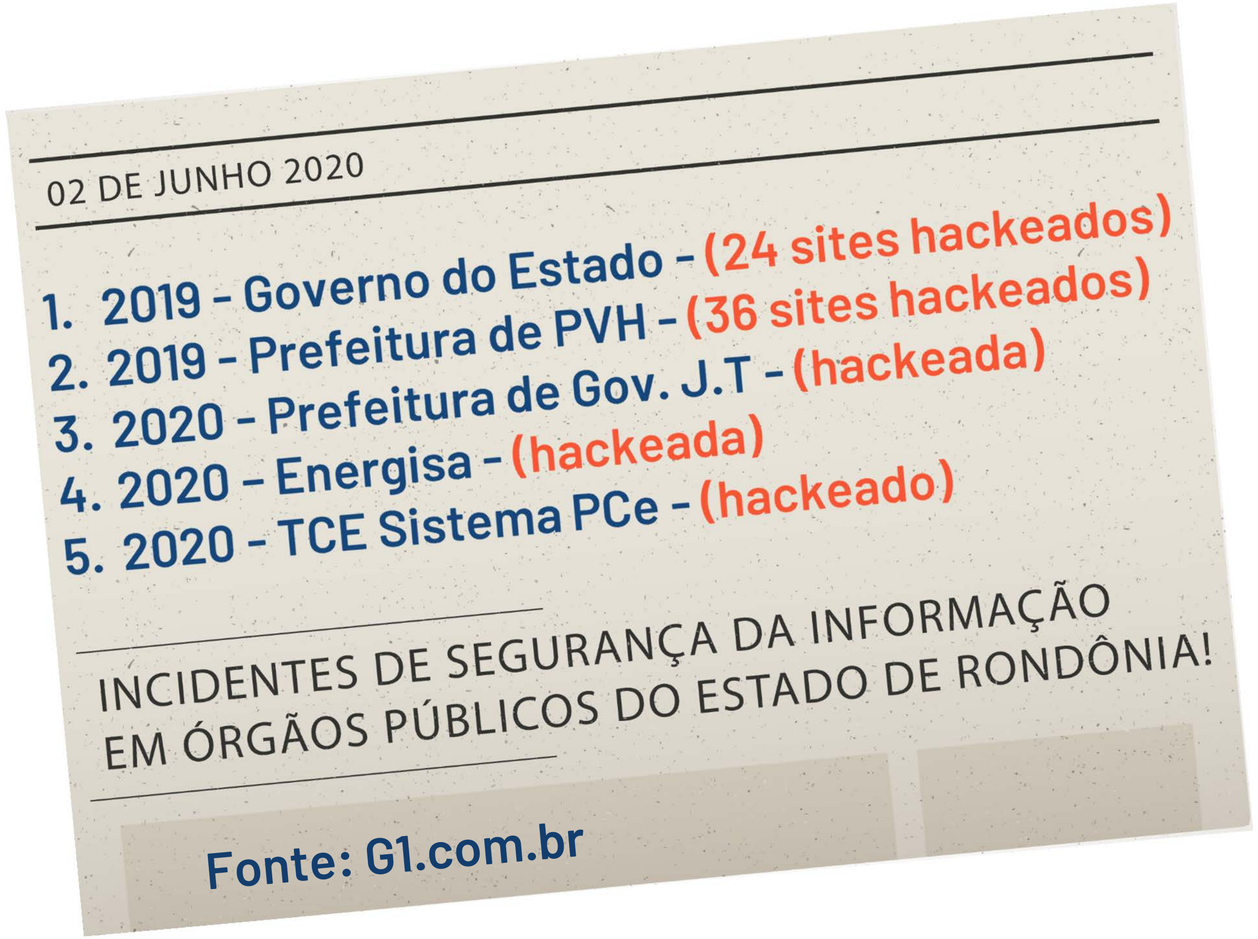
1. Potencial dano à imagem do Governo perante seu público interno e perante a comunidade internacional;

2. O descrédito da população nos serviços públicos;

3. A desconfiança de investidores internacionais na capacidade da administração pública em proteger seus próprios sistemas.

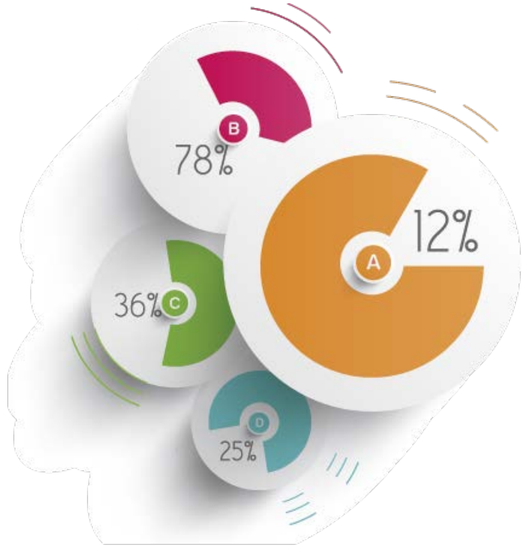
Fonte: Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética

Incidentes em Ambiente Governamental



Tentativas de intrusão à rede do TCE (internet)

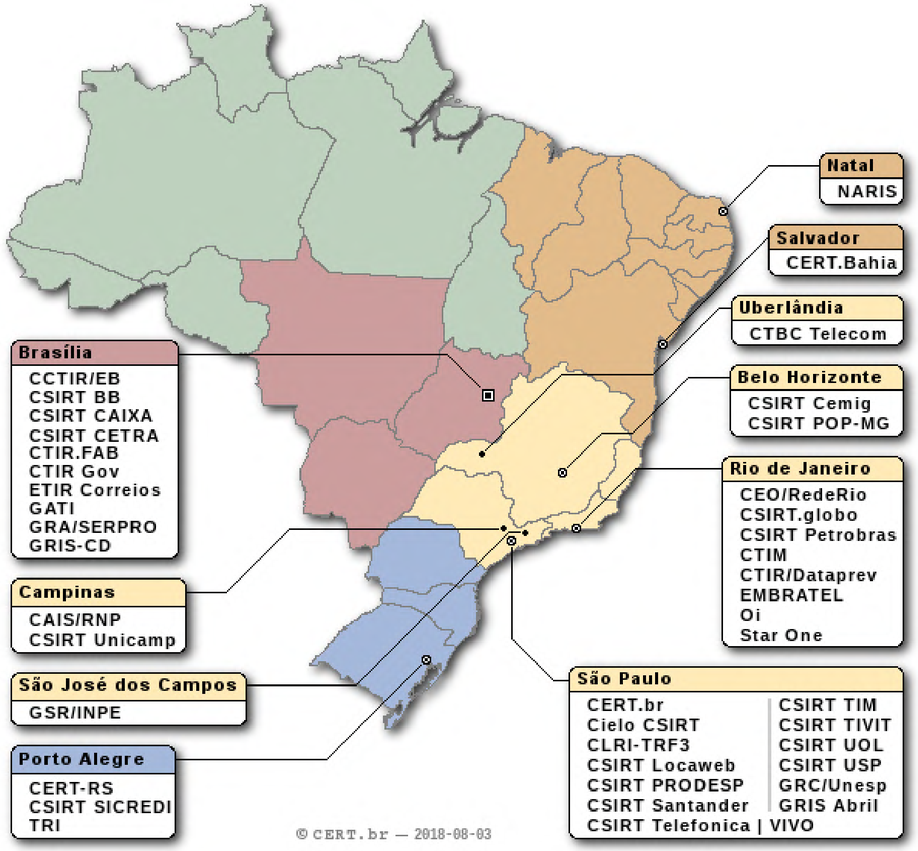
	2017	2018	2019	2020
Ano	2.900.529	1.166.000	259.000	201.000
Mês	241.210	97.167	21.583	40.200
Dia	8.040	3.239	719	1.340



COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON ESCOLA SUPERIOR DE CONTAS

Grupos de Segurança e Resposta a Incidentes (CSIRTs) - Brasil



Fonte: https://www.cert.br/csirts/

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Ambiente Corporativo Gerenciado

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

AMBIENTE CORPORATIVO

Privacidade:
Políticas e processos que governam a coleta, processamento, compartilhamento e eliminação de dados pessoais em conformidade com leis de proteção e regulamentações.

+

Segurança:
Políticas administrativas, técnicas e físicas, processos e controles que protegem a informação em conformidade com padrões, leis e regulamentações.

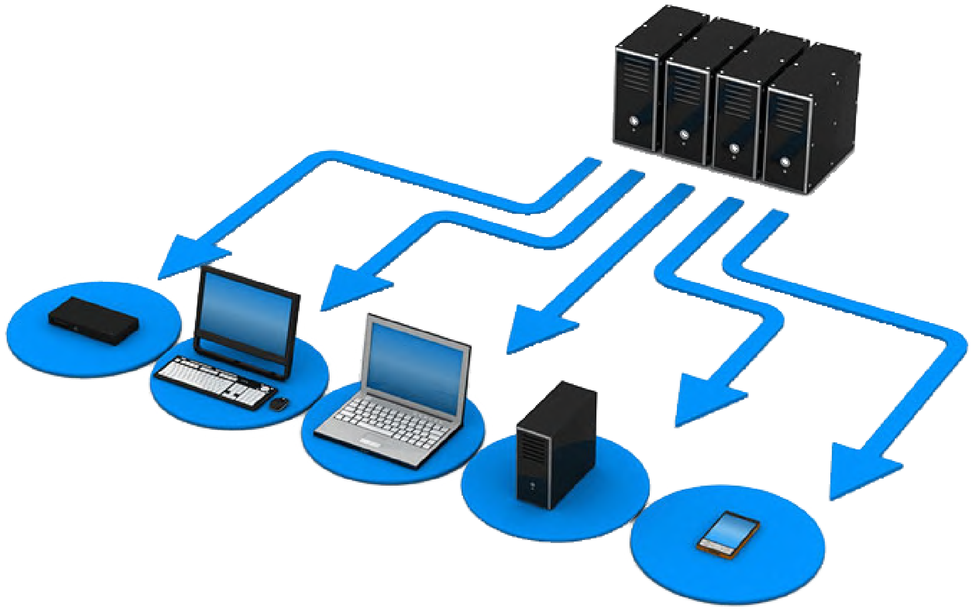
COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Política de Segurança da Informação

- São regras e diretrizes que orientem os colaboradores, clientes e fornecedores 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.

Rede Corporativa Gerenciada



A culpa *in vigilando* é caracterizada pela falta de fiscalização sobre procedimentos exercidos por outrem. (**TCU** - Acórdão 1581/2017 Primeira Câmara)

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON ESCOLA SUPERIOR DE CONTAS

Vulnerabilidades, Riscos e Ameaças

Códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

VÍDEO

- **Ameaças – Fontes Desconhecidas (link)**

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Vulnerabilidade

- Falhas de software e hardware;
- Senhas fracas;
- Uso inadequado;
- Sistemas de backup falhos;
- Portas abertas;
- Falhas em sistemas de logs.

A grande maioria dos incidentes de segurança ocorre por falta de informação, falta de processos e orientação ao recurso humano

Fonte: Google Central de Segurança

Risco

É o potencial de que uma dada **ameaça** venha a explorar vulnerabilidades em um determinado **ativo**, de modo a comprometer a sua segurança.

É o "efeito da incerteza nos objetivos"
(NBR ISO/IEC 31000)

Fonte: Google Central de Segurança

Ameaça

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

O principal meio de propagação é o e-mail e as mídias removíveis

Fonte: Google Central de Segurança.

Ameaça

Engenharia Social

Engenharia social é fazer uso da fraude, influência e persuasão para enganar pessoas, o que pode ser feito fazendo-se uso ou não de tecnologias. Explorando o elo mais fraco da segurança, o fator humano, o engenheiro social pode conseguir praticamente qualquer informação que deseje.

Enganar uma pessoa é uma tarefa relativamente fácil

Fonte: Google Central de Segurança – Vídeo (Google – Como evitar um ataque de engenharia social)

VÍDEO

- Google – Como evitar um ataque de engenharia social (link)

Ameaça

Falsificação de identidade nas redes sociais

Com o crescimento da internet e das redes sociais, têm sido cada vez mais comum os casos de pessoas que criam perfil falso.

Também conhecido como perfil *fake*, que significa “falso”, em inglês

Fonte: Google Central de Segurança

Ameaça

Phishing

É o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. O *Phishing* ocorre por meio do envio de mensagens eletrônicas.

- Páginas falsas de comércio eletrônico ou Internet Banking;
- Páginas falsas de redes sociais ou de companhias aéreas;
- Mensagens contendo formulários;
- Solicitação de recadastramento;
- Mensagens contendo links para códigos maliciosos.

Fonte: Google Central de Segurança

Ameaça

Ransomware

- **Infecta:** computadores, equipamentos de rede e dispositivos móveis;
- **Arquivo malicioso:** via links em e-mails, redes sociais e mensagens instantâneas, baixado de sites na Internet, acessado via arquivos compartilhados ou páginas web maliciosas;
- **Proteção:** sistema atualizado, cuidado com links ou arquivos, backups.

A maioria dos ransomwares faz ataques de *phishing* para conseguir infectar máquinas.

Fonte: Google Central de Segurança

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Gerenciamento de Senhas

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Crie senhas seguras

- Tanto na criação quanto na manutenção de uma senha são necessários alguns cuidados;
- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada.

Ter uma senha fraca ou não saber como mantê-la secreta é o mesmo que não ter senha nenhuma.

Fonte: Google Central de Segurança

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Elementos que você deve usar na elaboração de suas senhas

- Números aleatórios;
- Grande quantidade de caracteres;
- Diferentes tipos de caracteres;
- Utilize uma frase longa;
- Faça substituições de caracteres;
- Crie o seu próprio padrão.

O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Fonte: Google Central de Segurança

Alteração de senhas

- Você deve alterar a sua senha **imediatamente** sempre que desconfiar que ela pode ter sido descoberta ou que o computador no qual você a utilizou pode ter sido invadido ou infectado, ou ainda se o dispositivo foi furtado, roubado ou perdido.

Altere sua senha regularmente como forma de assegurar a confidencialidade. Não há como definir um período ideal para que a troca seja feita, pois depende diretamente de quão boa ela é e de quanto você a expõe.

Fonte: Google Central de Segurança

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

DICA

- **Gerenciando senhas salvas pelo Google: https://passwords.google.com/**

Ferramentas para gerenciar senhas

- **1Password** - https://agilebits.com/onepassword
- **KeePass** - https://keepass.info
- **LastPass** - https://lastpass.com
- **Dashlane** - https://www.dashlane.com
- **Keeper** - https://keepersecurity.com/pt_BR
- **PasswordBox** - https://www.passwordbox.com
- **RoboForm** - https://www.roboform.com

- **DICA**

Fonte: Google Central de Segurança

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

EXERCÍCIO

- **Usando ferramenta para criação de senha forte:**
- **http://testedesenha.com.br/**

Use redes seguras

É bom ter cuidado extra sempre que você acessar a Web usando uma rede que não conhece ou não confia, como a rede Wi-Fi em sua cafeteria local. O provedor de serviços pode monitorar todo o tráfego em sua rede, incluindo suas informações pessoais.

Verifique se o endereço começa com "**https**://", o que indica que sua conexão com o site é criptografada e mais resistente a invasões ou adulterações.

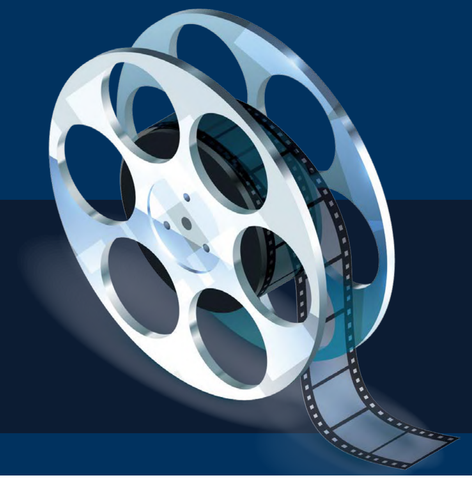
Quando se usa uma rede Wi-Fi pública, qualquer pessoa nas proximidades poderá monitorar as informações transmitidas entre seu computador e o ponto de acesso Wi-Fi, se sua conexão não for criptografada.

Evite realizar atividades importantes, como transações bancárias ou compras, em redes públicas.

Fonte: Google Central de Segurança

VÍDEO

- Segurança em Redes Wi-Fi (link)

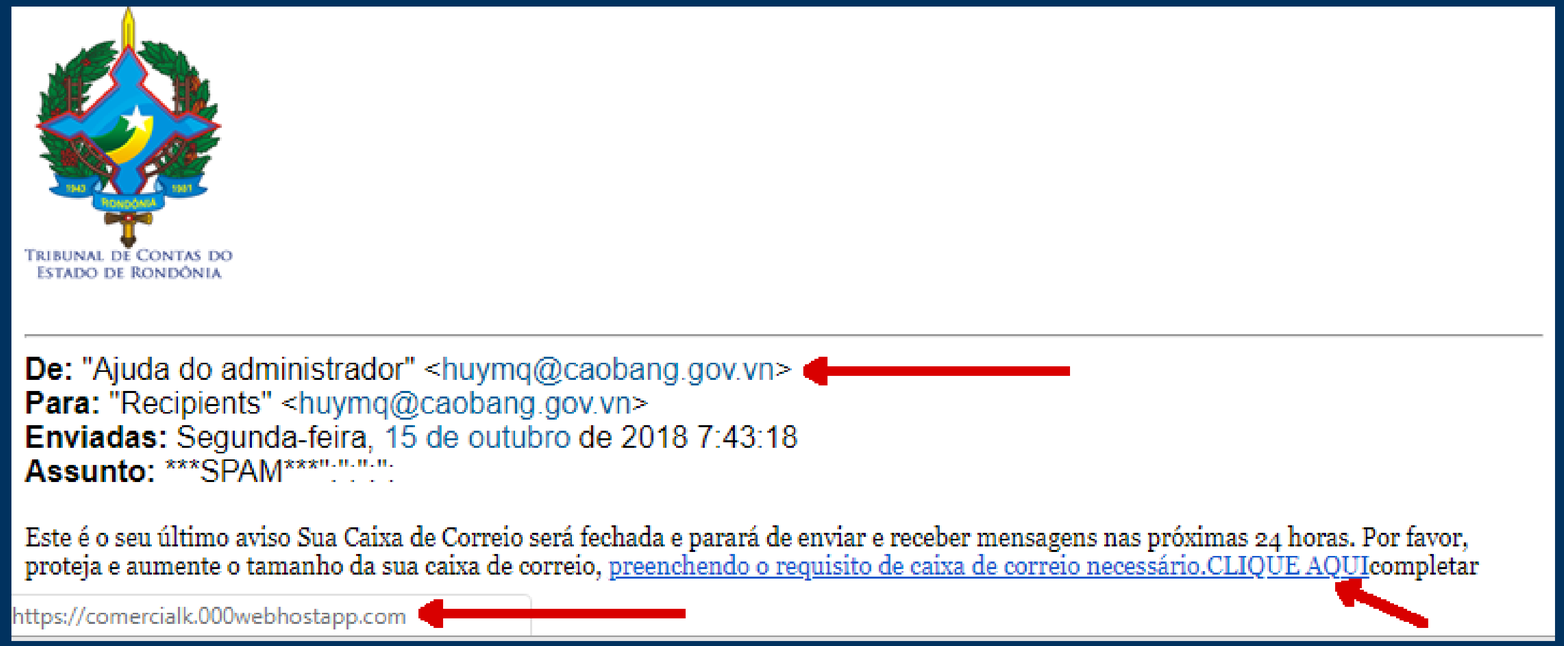


Uso inteligente do e-mail (corporativo e pessoal)

- Seja cuidadoso ao acessar a página de seu webmail para não ser vítima de *phishing*;
- Digite a URL diretamente no navegador e tenha cuidado ao clicar em links recebidos por e-mail;
- Não utilize um site de busca para acessar seu webmail;
- Seja cuidadoso ao elaborar sua senha de acesso;
- Configure opções de recuperação de senha (e-mail alternativo, questão de segurança, nº de celular);
- Evite acessar seu webmail em computadores de terceiros (utilize navegação anônima);
- Utilize conexões seguras ao acessar seu webmail, especialmente ao usar redes Wi-Fi públicas;
- Mantenha seu dispositivo seguro (computador, smartphone, tablet);
- Faça logoff (sair) ao terminar de acessar seu e-mail em computadores de terceiros.

Fonte: Google Central de Segurança

Uso inteligente do e-mail (corporativo e pessoal)



TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA

De: "Ajuda do administrador" <huymq@caobang.gov.vn>
Para: "Recipients" <huymq@caobang.gov.vn>
Enviadas: Segunda-feira, 15 de outubro de 2018 7:43:18
Assunto: ***SPAM***

Este é o seu último aviso Sua Caixa de Correio será fechada e parará de enviar e receber mensagens nas próximas 24 horas. Por favor, proteja e aumente o tamanho da sua caixa de correio, preenchendo o requisito de caixa de correio necessário.CLIQUE AQUIcompletar

https://comercialk.000webhostapp.com

- **Identificando Ameaças**

Uso inteligente do e-mail (corporativo e pessoal)

De: "Walter Luiz Guedes Pereira" <walter.guedes@mds.gov.br>
Enviadas: Quinta-feira, 6 de setembro de 2018 9:19:46
Assunto: Ação Requerida

Querido usuário,

Observe que 95% dos seus e-mails recebidos foram colocados em espera devido à atualização recente do servidor em nosso banco de dados.
Para receber e enviar suas mensagens regularmente sem interrupção

Por favor, pegue um minueto para atualizar sua conta automaticamente: faça login agora

Este e-mail está sujeito a seguir obrigatório, o não cumprimento levaria ao encerramento temporário da conta.

Obrigado por nos ajudar a manter sua conta segura.

Atenciosamente,
Administrador do sistema

mk3.org/interface-novo

- **Identificando Ameaças**

Uso inteligente do e-mail (corporativo e pessoal)

De: "Pagamento realizado com sucesso." <ZEREIS07@HOTMAIL.COM>
Para: "escon" <escon@tce.ro.gov.br>
Enviadas: Terça-feira, 4 de setembro de 2018 7:09:31
Assunto: ***SPAM***=?iso-8859-1?Q?MarcenariaLíderLTDA.?=

escon@tce.ro.gov.br

Pagamento realizado com sucesso. *1650818*

Parabéns seu pedido sera entre no endereço informado na compra. *1650818*

Nota fiscal , lista de produtos e outros detalhes dos produtos no link abaixo. *&nb sp; 1650818*

Download NF

Marcenaria Líder LTDA.

Atenção
Apos o recebimento desse e-mail você recebera seus produtos em ate 8 dias uteis no endereço informado na compra. 1650818

financeiro-lider.duckdns.org/DownloadNF

- **Identificando Ameaças**

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Aplicando Segurança da Informação

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Proteja seu dispositivo

Dicas importantes

- Mantenha os programas instalados com as versões e atualizações mais recentes;
- Use programas originais;
- Use mecanismos de proteção (antivírus, firewall etc);
- Seja cuidadoso ao manipular arquivos (links, e-mails, macros);
- Mantenha seu dispositivo com a data e a hora corretas (logs de segurança);
- Crie um disco de recuperação de sistema (atualização malsucedida, desligamento abrupto);
- Cuidado ao enviar seu dispositivo para serviços de manutenção.

Proteja seu smartphone

Ao acessar redes

- Seja cuidadoso ao usar redes Wi-Fi públicas;
- Mantenha interfaces de comunicação, como bluetooth, infravermelho e Wi-Fi, desabilitadas e somente as habilite quando for necessário;
- Configure a conexão bluetooth para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").

Fonte: Cert.br

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Proteja seu smartphone

Proteja seu dispositivo móvel e os dados nele armazenados

- Aplique atualizações de segurança (SO e APPs);
- Faça backups periódicos dos dados nele gravados;
- Mantenha controle físico sobre ele, principalmente em locais de risco (públicos);
- Use conexão segura sempre que a comunicação envolver dados confidenciais;
- Não siga links recebidos por meio de mensagens eletrônicas;
- Cadastre uma senha de acesso que seja bem elaborada;
- Utilize recursos para que seja localizado e bloqueado remotamente.

Fonte: Cert.br

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

EXERCÍCIO

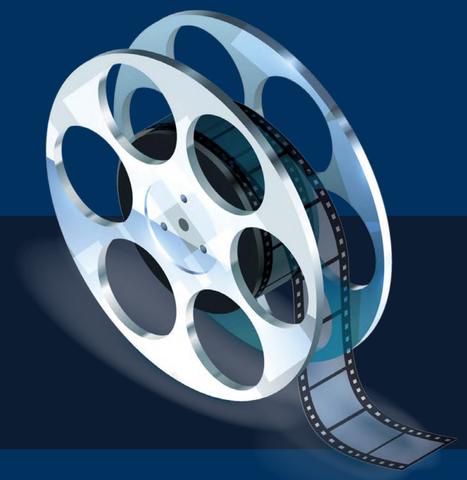
- **Tarefa para casa: Instalar antivírus no smartphone**

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Linhas de Defesa

Vídeo



- Os invasores (link)

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Antivírus

Fonte: Google Central de Segurança

Antivírus

Os antivírus ou antimalwares são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional;

Utilizar mais de um antivírus não vai deixar o sistema mais protegido;

Versões Gratuitas x Versões Pagas:
A principal diferença é que, via de regra, as versões pagas oferecem proteções extras para aumentar a proteção.

Fonte: Google Central de Segurança

Firewall

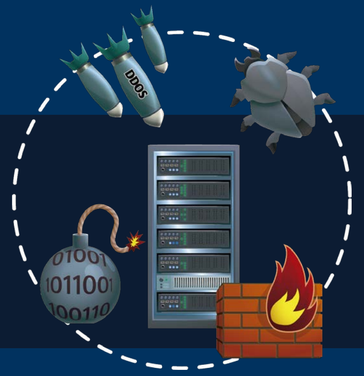
Fonte: Google Central de Segurança

Firewall

Pessoal

É um tipo específico de firewall que é utilizado para proteger um computador contra acessos não autorizados vindos da Internet.

Quando bem configurado, o firewall pessoal pode ser capaz de: registrar tentativas de acesso aos serviços do sistema; bloquear o envio de informações coletadas por invasores; bloquear tentativas de invasão; analisar continuamente o conteúdo das conexões filtrando códigos maliciosos e evitar que um código malicioso já instalado possa se propagar.



O Sistemas Operacionais Windows possui firewall pessoal integrado

Fonte: Google Central de Segurança

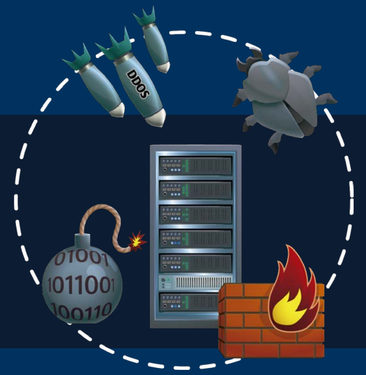
Firewall

Corporativo

É um mecanismo de segurança para redes de computadores. Implementado em hardware e/ou software, atua basicamente como um filtro de proteção entre duas ou mais redes de forma a controlar o fluxo de dados entre elas e com isso evitar que acessos nocivos ou não autorizados aconteçam.

Todo firewall tem as suas vulnerabilidades e a cada nova versão os fabricantes procuram corrigi-las. Contudo, os hackers também se atualizam e acabam encontrando novos meios nessa guerra de gato e rato.

Risco: Firewalls são configurados por seres humanos



Fonte: Google Central de Segurança

VPN – Rede Privada Virtual

Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Em geral utilizam criptografia e outros mecanismos de segurança para proteger os dados em trânsito

Acesso remoto à rede corporativa
deve ser feito a partir de VPN

Fonte: Google Central de Segurança – Vídeo: VPN

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Cuidado com os Dados

VÍDEO

- **Backup em nuvem (link)**

Backup (cópia de segurança)

É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Fonte: Cert.br

Uso seguro de backup

Fazer backup é tão necessário que inúmeros softwares existentes no mercado, muitos deles livres, se dedicam exclusivamente a isso, tornando essa prática mais fácil e eficiente. Alguns, inclusive, permitem gerar imagens completas de discos rígidos e partições.

Apesar das vantagens de se gerar cópias de segurança, se esse não for um processo organizado, bem planejado, pode tornar-se inútil ou mesmo perigoso. Portanto, há uma série de fatores que devem considerados.

Fonte: Cert.br

Uso seguro de backup

Não basta ter backup:

- Deve ser adequado às necessidades;
- Importante conhecer as opções existentes.

Determinar:

- O que copiar? Onde copiar? Quando copiar? Como copiar?

Fonte: Cert.br

Uso seguro de backup

Backup pessoal:

- Qual o valor dos seus dados?
- Como protege-los?
- Arquivos podem ser apagados acidentalmente;
- Equipamentos podem: Ser perdidos, furtados ou roubados; Apresentar mau funcionamento (HD);
- Ser invadidos e seus arquivos apagados;
- Você pode usar programas integrados do SO para fazer backup;
- Enviar uma cópia para seu e-mail ou repositório externo de arquivos;
- Certifique-se de que esteja sendo feito;
- Tenha cuidado para não perder seus pendrives;
- Criptografe seus backups.

Fonte: Cert.br

Uso seguro de backup

Backup corporativo:

Tão necessário quanto a proteção dos dados originais, é a proteção das cópias de segurança. As cópias devem estar em um local distante dos dados originais para que, em caso de desastre, a recuperação seja possível. Esse local precisa receber uma proteção e um controle de acesso adequados e todo acesso tem que ser monitorado.

Tipo	Descrição	Vantagens	Desvantagens
Completo	Copia todos os dados; serve como referencial para os demais tipos	Mais básico e completo; cópia de todos os dados em um único conjunto de mídia; recuperação simples	Mais demorado; ocupa mais espaço
Incremental	Copia apenas os dados alterados ou criados após o último completo ou incremental	Menor volume de dados; mais rápido; ocupa menos espaço de armazenamento	Recuperação mais complexa (primeiro um completo e depois todos os incrementais)
Diferencial	Copia os dados alterados ou criados desde o último backup completo	Recuperação mais rápida que o incremental (precisa só do último completo enquanto o incremental precisa do completo e dos incrementais)	Ocupa mais espaço que o incremental e menos que o completo; gasta mais tempo que o incremental e menos que o completo
Progressivo	Similar ao incremental mas com maior disponibilidade dos dados	Recuperação automatizada e mais eficiente (não precisa descobrir os conjuntos a serem recuperados)	Recuperação mais lenta que o diferencial e o completo (precisa analisar diferentes conjuntos para terminar o processo)

Descarte seguro de informações

Quando uma mídia apresenta defeito ou ainda quando dados críticos lá armazenados não têm mais utilidade, se faz necessário a existência de procedimentos operacionais que estabeleçam o descarte seguro, evitando assim que informações sensíveis acabem divulgadas.

Já descarte seguro é aquele que torna impossível a recuperação dos dados, seja por destruição da mídia (trituração ou incineração) ou por algum tipo de formatação especial, onde todos os dados são sobrescritos.

Fonte: Cert.br

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Descarte seguro de informações

No Windows, quando você apaga um arquivo, ele não é realmente apagado. Na primeira vez, ele é armazenado na Lixeira, que te dá uma segunda chance nas vezes em que você não queria realmente deletar o arquivo.

Caso você esvazie a Lixeira, então os arquivos são “desalocados” do seu disco rígido (HD). Mais uma vez, no entanto, eles não são apagados: o espaço que eles ocupam é simplesmente marcado como disponível para uso.

Fonte: Cert.br

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

EXERCÍCIO

- Quiz 2

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

TCE-RO

FUNDAMENTOS

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

BIG DATA

É a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados (estruturados ou não) grandes demais para serem analisados por sistemas tradicionais.

VÍDEO

- **BIG DATA (link)**

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

DATA SCIENCE

É a coleta de grande volume de dados (estruturados ou não) de diversas fontes, que visa a extração de conhecimento para subsidiar a tomada de decisões.

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS


GDPR
Maio 2018
Maio 2018
edpb
Padrão Chinês
PRC Cybersecurity Law
CCPA
Juno 2018
Agosto 2018
LGPD
Japão
Jan 2019
Julho 2019
LGPD

Lei 13.709/2018

- **Art. 1º.** Esta Lei dispõe sobre o tratamento de dados pessoais, **inclusive nos meios digitais**, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

- Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Características

Dispõe sobre a proteção do tratamento de **dados pessoais,** inclusive nos meios digitais, e altera a Lei nº 12.965/2014 (Marco Civil da Internet)

Inspirada na legislação europeia (*General Data Protection Regulation – GDPR*)

Sofreu alteração através da lei nº 13.853, de 8 de julho de de 2019

- Criação da Autoridade Nacional de Proteção de Dados (ANPD)
- Alteração do período de vacância da lei para 24 meses

Entrou em vigor em 18 de setembro de 2020


LGPD
O QUE ALGUNS ACHAM QUE É
TERMO DE CONSENTIMENTO
POLÍTICA DE PRIVACIDADE
CLÁUSULA PADRÃO
BANNER DE COOKIES NO SITE
PROGRAMA DE GOVERNANÇA
TRANSPARÊNCIA
BASES LEGAIS
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS
MINIMIZAÇÃO
CONSCIENTIZAÇÃO
GARANTIA DE DIREITOS
MONITORAMENTO CONTÍNUO
PREVENÇÃO
RESPOSTA À INCIDENTES
BOAS PRÁTICAS
AVALIAÇÃO E GESTÃO DE RISCOS
PROCESSOS E POLÍTICAS
SEGURANÇA
RELAÇÃO DE CONFIANÇA
BOA-FÉ
O QUE REALMENTE É
ALINE FUKE FACHINETTI

VÍDEO

- Lei Geral de Proteção de Dados Pessoais (link)

Do tratamento de dados pessoais pelo poder público?

Lei 13.709/2018 - Capítulo IV (arts. 23 a 32).

LGPD e LAI - Harmonização, interação e complementariedade

Ambas as leis são inspiradas pelo valor da transparência da atividade pública, pelo qual o indivíduo, pessoa natural, tem a possibilidade de exercer a defesa de seus direitos e garantias fundamentais contra o Estado e exercer o efetivo controle da atividade pública.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON ESCOLA SUPERIOR DE CONTAS

Conceitos

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado Pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, **dado referente à saúde ou à vida sexual, dado genético ou biométrico**, quando vinculado a uma pessoa natural

LGPD Lei Geral de Proteção de Dados Pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

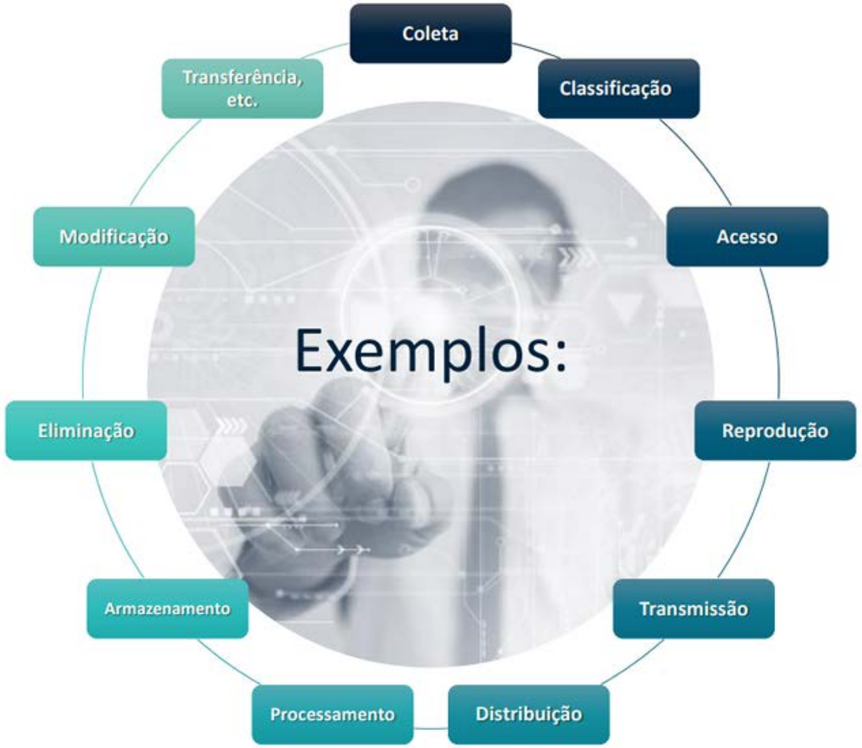
Conceitos

Consentimento: **manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade determinada**

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

LGPD
Lei Geral de Proteção de Dados Pessoais

Tratamento



Toda operação realizada com dados pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

LGPD
Lei Geral de Proteção de Dados Pessoais

Due Diligence sobre dados pessoais

Identificação dos dados (pessoal, sensível, criança, público, anonimizado), departamentos, meios (físico ou digital), operadores internos e externos para mensuração de exposição da empresa à LGPD

Auditoria sobre o Tratamento

Aderência das 20 atividades de tratamento (art. 5º, X) de dados (coleta, controle, eliminação, etc.) aos princípios gerais previstos no Art. 6º da LGPD, mediante revisão e criação de documentos (contratos, termos, políticas) para uso interno e externo

Gestão do Consentimento e Anonimização

Controle do consentimento e anonimização para atender possível solicitação do titular e da ANPD

O que será preciso fazer?

LGPD
Lei Geral de Proteção de Dados Pessoais

Gestão dos Pedidos do Titular

Criação de banco de dados para controle dos pedidos dos titulares dos dados (acesso, confirmação, anonimização, consentimento, portabilidade etc.)

Relatório de Impacto

Atendimento à ANPD e demais órgãos do Sistema Nacional de Proteção do Consumidor que poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais

Segurança dos Dados

Adoção das medidas de segurança da informação aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas

O que será preciso fazer?

LGPD
Lei Geral de Proteção de Dados Pessoais

Governança do Tratamento

Criação de regras de boas práticas e de governança que estabeleçam procedimentos, normas de segurança, ações educativas e mitigação de riscos no tratamento de dados pessoais

Plano de Comunicação – Incidente de Segurança

Comunicação aos órgãos fiscalizatórios (ANPD, Procon, Senacon) e à imprensa sobre incidente de segurança que acarrete risco ou dano

Validação do término do tratamento

Adoção das providências necessárias à eliminação dos dados tratados e verificação de eventual conservação dos dados com a elaboração de documentos que evidenciem a eliminação

O que será preciso fazer?

LGPD
Lei Geral de Proteção de Dados Pessoais

Certificação

Certificação por auditoria especializada das práticas relacionadas à LGPD

Data Protection Officer (Encarregado)

Identificação do encarregado (Pessoa Física ou Jurídica) e sua capacitação para exercer as atividades previstas na LGPD

Gestores de Segurança da Informação e Privacidade

Atuarão, sob coordenação do DPO, disseminando as boas práticas institucionais relacionadas à segurança da informação e privacidade de dados

O que será preciso fazer?

LGPD
Lei Geral de Proteção de Dados Pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Conhecendo os Atores da Lei

Titulares de Dados Pessoais

Agentes de Tratamento (Controlador/Operador)

DPO Encarregado de Proteção

Autoridade Nacional de Proteção de Dados

LGPD
Lei Geral de Proteção de Dados Pessoais

Titular de Dados Pessoais

Art. 5º, V
Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Agentes de Tratamento

Art. 5º, VI, VII

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado - Data Protection Officer - DPO

Art. 5º, VIII - Atividades

Recepcionar e atender demandas dos titulares dos dados.

Interagir com a ANPD.

Orientar servidores e contratados quanto a práticas de proteção de dados.

Encarregado - Data Protection Officer - DPO

Características

Ser detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados.

Ter autonomia técnica e profissional no exercício do cargo.

Reportar ao mais alto nível de direção da organização.

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Autoridade Nacional de Proteção de Dados - ANPD

Sua atuação está pautada em 3 pilares principais:

FISCALIZAÇÃO

Direcionada para formatar normas e procedimentos, deliberar sobre a interpretação da LGPD e solicitar informações relacionadas ao tratamento de dados pessoais;

SANÇÃO

Poderá instaurar processo administrativo quando houver descumprimento da LGPD, estando incumbida de aplicar as sanções previstas na Lei;

EDUCAÇÃO

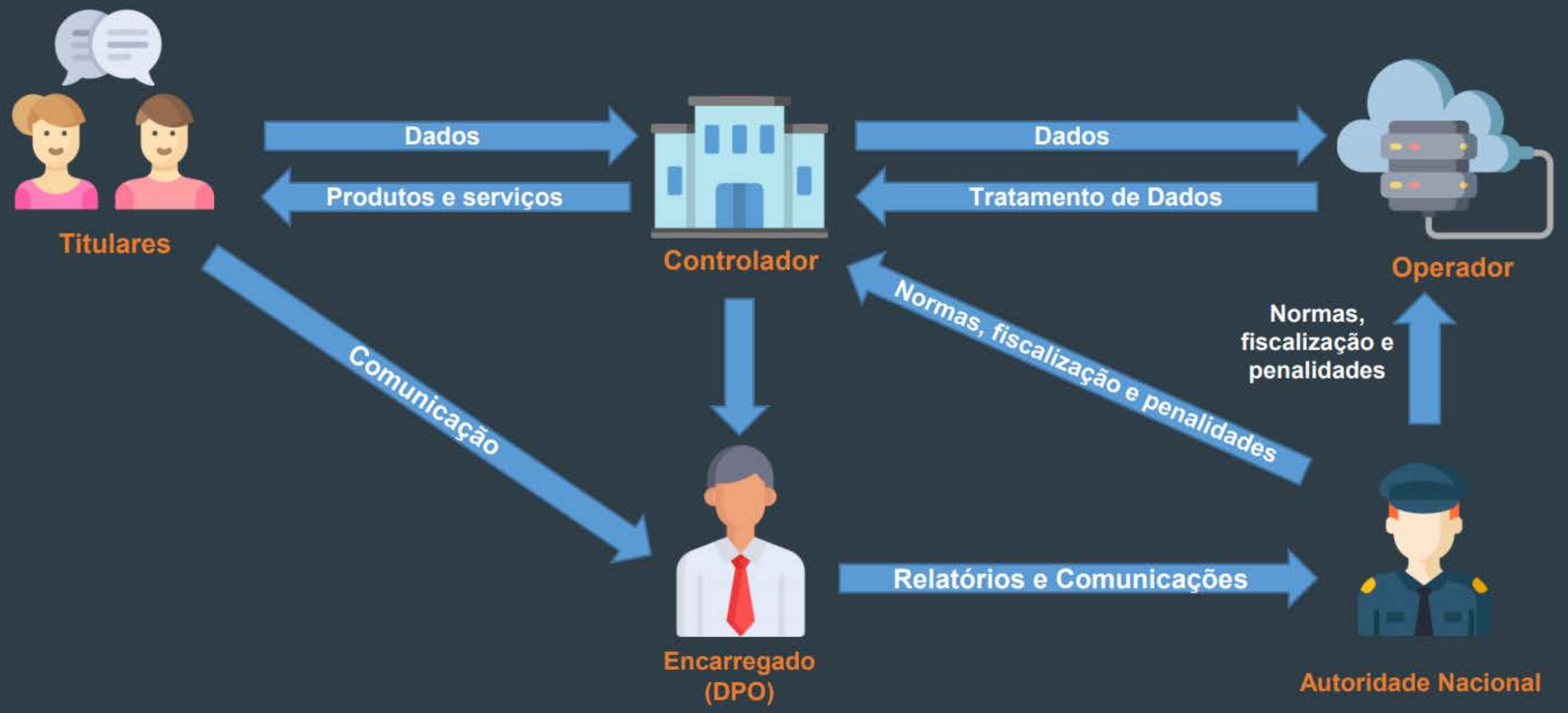
Encarregada de disseminar informações sobre a LGPD e desenvolver medidas de segurança, criar diretrizes para interpretação da lei, encorajar a definição de padrões para produtos e serviços, como forma de facilitar o controle de titulares sobre seus dados pessoais, além de elaborar estudos sobre melhores práticas nacionais e internacionais de proteção de dados pessoais, entre outros.

LGPD
Lei Geral de Proteção de Dados Pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Fluxo



LGPD
Lei Geral de Proteção de Dados Pessoais

Operadora VIVO

Ministério Público investiga Vivo por uso ilegal de dados pessoais de clientes

Por Ares Saturno | 04 de Abril de 2018 às 08h43

O Ministério Público do Distrito Federal e Territórios (MPDFT) instaurou uma investigação a fim de averiguar a legalidade no trato com os dados pessoais dos mais de 73 milhões de usuários da operadora Vivo.

Em nota, a operadora móvel comentou que cumpre rigorosamente a legislação vigente e não promove qualquer uso ilegal dos dados pessoais de seus clientes. Por meio de sua assessoria, "a Vivo assegura que as informações de seus clientes não são, em hipótese alguma, transferidas ou compartilhadas com anunciantes".

Segundo a ação iniciada pelo MPDFT, os dados pessoais dos clientes foram compartilhados com anunciantes da Vivo Ads, plataforma de marketing para telefonia móvel da operadora. Os promotores de justiça Paulo Roberto Binicheski e Frederico Meinberg são os responsáveis pela abertura do inquérito civil público que, por enquanto, só tem o intuito de verificar se a tratativa dos dados pela operadora está dentro da legalidade. Para isso, a empresa será notificada a enviar um representante para ser ouvido dentro da investigação.

Hering

Hering pode ser multada em quase 100 milhões de reais

Luiza Tozzato, editado por Renato Santino 03/09/2019 19h09

A loja conceito da Hering, a Hering Experience, localizada no Morumbi Shopping, na zona sul de São Paulo, apresenta algumas tecnologias para melhorar o modo de consumo de seus clientes. O estabelecimento possui câmeras de reconhecimento facial que captam as reações dos clientes às peças expostas pelo local. Além disso, sensores identificam quais os locais de preferência do cliente ao circular pela loja.

No início da semana foi instaurado um processo pelo Departamento de Proteção e Defesa do Consumidor, que investiga indícios de coleta de dados dos clientes sem o seu consentimento prévio. A ação judicial prevê que a empresa deverá ser intimada a prestar esclarecimentos sobre o destino dos dados coletados. O órgão quer entender com quem seriam compartilhadas essas informações.

Em nota, Hering afirma que diferentemente do que foi apontado, a loja não realiza reconhecimento facial, mas, sim, detecção facial, por meio do qual estima apenas o gênero, a faixa etária e o humor dos consumidores, de forma anônima. Caso a Hering seja considerada culpada das acusações, a empresa poderá ser multada em até 97 milhões reais.

Banco Inter

Início » Brasil » Banco Inter vazou dados de quase 20 mil clientes, diz investigação do MP

Banco Inter vazou dados de quase 20 mil clientes, diz investigação do MP

Instituição financeira pode ser condenada a pagar R$ 10 milhões por não proteger informações de correntistas

O Banco Inter vazou dados pessoais de 19.961 correntistas, de acordo com uma investigação do Ministério Público do Distrito Federal e Territórios (MPDFT). A Comissão de Proteção dos Dados Pessoais moveu nesta segunda-feira (30) uma ação civil pública contra a instituição financeira, que pode ser condenada a pagar uma indenização de R$ 10 milhões.

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Sanções

Advertência

Com prazo para medidas corretivas

Multa Simples ou Diária

Até 2% da receita do grupo no brasil no último exercício limitado a R$ 50 milhões, **por infração**

Publicização

Após apurada e **confirmada a infração**

Bloqueio

Dos dados pessoais **relacionados à infração**

Eliminação

Dos dados pessoais **relacionados à infração**

LGPD
Lei Geral de Proteção de Dados Pessoais

Mapeamento do fluxo de dados nas unidades do TCE-RO

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON ESCOLA SUPERIOR DE CONTAS

Roadmap para implementação

LGPD Lei Geral de Proteção de Dados Pessoais

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Programa de Conformidade à LGPD

LGPD
Lei Geral de Proteção de Dados Pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

LGPD
Lei Geral de Proteção de Dados Pessoais

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Estratégia Organizacional

UTILIZAR O MODELO PDCA

Processo contínuo / Vigilância ostensiva

ENVOLVER AS ÁREAS

Negócio / Tecnologia / Jurídico

LGPD
Lei Geral de Proteção de Dados Pessoais

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

EXERCÍCIO

- **Quiz 3**

Referências

- Cartilha de Segurança para a Internet - CERT.br
- Gestão de Segurança da Informação - GSCI-UNB
- Internet das Coisas - CERT.br
- Política Corporativa de Segurança da Informação - TCU
- Referencial Básico de Gestão de Riscos - TCU
- Cartilha de Segurança da Informação - STJ
- Implantando a Gestão de Segurança da Informação - TCU
- Classificação da Informação no Banco Central do Brasil - Banco Central do Brasil
- Guia de Estudos de Segurança e Auditoria de Sistemas - UNIS
- Central de Segurança – Google
- Lei 13.709/2018

COSIC
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ESCON
ESCOLA SUPERIOR DE CONTAS

Obrigado!

charles.vasconcelos@tce.ro.gov.br
Encarregado de Proteção de Dados - DPO / TCE-RO

ESCON

ESCOLA SUPERIOR DE CONTAS

Escola Superior de Contas Conselheiro José Renato da Frota Uchoa – ESCon