

CURSO

SECURITY BASIC

Segurança básica para Operadores LGPD

Planejamento e
preparação do
ambiente operacional
de computadores,
laptops, notebooks.

Uso pessoal em
teletrabalho ou em
pequenas empresas.



08 HORAS DE DEDICAÇÃO

Aplicação do framework "Estado da Arte em Segurança de TIC"



Como as empresas são protegidas.



MÁQUINAS DE ELEVADO RISCO



- ÚTIL PARA TODOS
 - POSSIBILITA O TRANSPORTE
 - PODE CAUSAR ACIDENTES E MORTES
 - É DE COMPLEXA OPERAÇÃO
- REQUER HABILITAÇÃO ESPECIAL**

=



- ÚTIL PARA TODOS
 - POSSIBILITA A DEFESA NACIONAL
 - PODE CAUSAR ACIDENTES E MORTES
 - É DE COMPLEXA OPERAÇÃO
- REQUER HABILITAÇÃO ESPECIAL**

=



- ÚTIL PARA TODOS
- POSSIBILITA TRABALHO PRODUTIVO
- PODE CAUSAR INJURIA, DIFAMAÇÃO, FURTOS, ACIDENTES E MORTES EM LARGA ESCALA
- É DE COMPLEXA OPERAÇÃO

NÃO

REQUER HABILITAÇÃO ESPECIAL



**Riscos profissionais
por atitudes
pessoais.**

**Crimes Propositais ou Acidentais por
imprudência, negligência ou Imperícia.**

**REGULAMENTOS E LEIS NO MUNDO CONTEMPORÂNEO
IMPUTAM RESPONSABILIDADES AS PESSOAS.**

CONTROLADOR



OPERADORES

**AGENTES DE
TRATAMENTO DE
DADOS PESSOAIS**

Precisamos assumir a
responsabilidade dos
nossos atos.



INFORMÁTICA AVANÇADA

Curso Online

Precisamos estar
preparados e habilitados no uso
de recursos computacionais
seguros.

USUÁRIOS DE
COMPUTADORES

VAMOS INICIAR

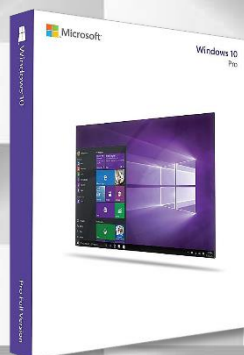
SECURITY BASIC

Segurança básica para Operadores LGPD

Como é composto um computador?



**HARDWARE OU
ELETRÔNICA**



**SOFTWARE SISTEMA
OPERACIONAL
WINDOWS (SO)**



**COMPUTADOR
PRONTO PARA
TRABALHO**

**TUDO NO COMPUTADOR
DEPENDE DO HARDWARE
E SOFTWARE DO SISTEMA
OPERACIONAL (SO) PARA
FUNCIONAR**

COMPUTADOR= HARDWARE + SO

- OS DOIS SÃO CONFIGURÁVEIS EM TERMOS DE PROTEÇÃO DE USO.



O HARDWARE TEM O “BIOS” PARA PODER CONFIGURAR PARAMETROS DE PROTEÇÃO DA MÁQUINA NA PARTE DA ELETRÔNICA.

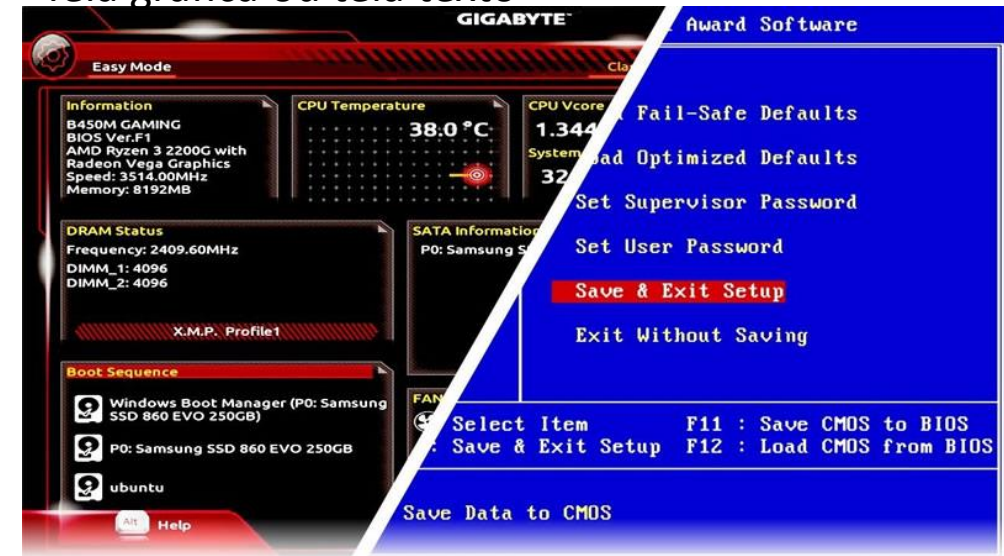


O “SO” SISTEMA OPERACIONAL, É UM SOFTWARE QUE POSSUI UM PAINEL DE CONTROLE E UTILITÁRIOS QUE PERMITEM CONFIGURAR A SEGURANÇA DA MÁQUINA .

BIOS* - Basic Input/Output System

- ❑ ASUS = F2
- ❑ LENOVO = pressione (Fn +) F2.
- ❑ ACER = F2
- ❑ HP = pressione repetidamente a tecla F10
- ❑ DELL = F2
 - ❑ Modelos mais antigos utilizam a tecla Delete, Insert ou até mesmo F10.
- ❑ Macbook = Pressione "Command", "Option" e as letras "O" e "F" simultaneamente antes que o sistema inicie.

Tela gráfica ou tela texto

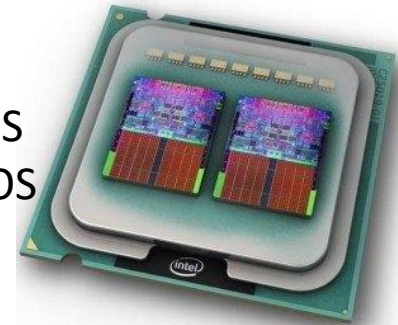


*BIOS é firmware, gravado em uma memória não volátil, usado para realizar o boot do hardware durante o processo de inicialização e para fornecer serviços de tempo de execução para sistemas operacionais e programas. No BIOS é possível fazer diversos ajustes, configurações de segurança e desempenho – requer conhecimento técnico.

CAPACIDADE DE PROCESSAMENTO PROTEGIDO



2 PROCESSOS
SIMULTÂNEOS



4 PROCESSOS
SIMULTÂNEOS

4 CORES



WORLD'S 1ST 12-CORE GAMING CPU
AMD RYZEN™ 9 3900X

12 Cores
24 Threads

4.6 GHz Boost
3.8 GHz Base

70 MB
Total Cache

105W TDP





**SISTEMA OPERACIONAL
CONFIGURAÇÕES**

ALGUMAS MELHORES PRÁTICAS PARA A SEGURANÇA BÁSICA

FUNDAMENTAL - REGRAS

- ❑ Manter o sistema atualizado é a primeira Regra Básica de Segurança.
- ❑ Não confie em Atualizações Automáticas – Atualize várias vezes ao dia.
- ❑ Conheça o **Painel de Controle e Configurações** – Sistema e Segurança.
- ❑ Busque entender e tenha domínio sobre a Segurança de sua máquina.

MELHORES
PRÁTICAS
PARA A SEGURANÇA



SEGURANÇA EMBARCADA DO WINDOWS - ESPECIFICAÇÃO (tudo configurável)

- ❑ Anti-Vírus Nativo – um dos melhores da atualidade – Nota Máxima
- ❑ Exploit Protection e Anti-Ransomware (sequestro de dados)
- ❑ Sistema Firewall de controle da Máquina (todas as Redes)
- ❑ Sistema Proxi de Aplicativos e Navegação WEB segura
- ❑ Isolamento do Núcleo do Sistema (memória fechada)
- ❑ Controle básico de Privacidade de Dados Pessoais do usuário
- ❑ Criptografia Nativa AES 256 e Criptografia global BitLocker
- ❑ WIP proteção de Informações da plataforma (sistema)



Windows Defender Antivírus 08/2020.

Nota MÁXIMA

Proteção= 6

Performance= 6

Usabilidade= 6



Windows 10: August 2020					
Producer	Certified	Protection	Performance	Usability	
AhnLab	V3 Internet Security 9.0		6	6	6
avast	Free AntiVirus 20.5 & 20.6		6	5.5	6
AVG	Internet Security 20.5 & 20.6		6	5.5	6
Avira	Antivirus Pro 15.0		6	6	6
Bitdefender	Internet Security 24.0		6	6	5.5
BullGuard	Internet Security 20.0		6	6	5.5
eset	Internet Security 13.1 & 13.2		6	5.5	6
F-Secure	SAFE 17		6	6	6
GDATA	Internet Security 25.5		6	6	6
kaspersky	Internet Security 20.0		6	6	6
McAfee	Total Protection 23.0		6	6	6
Microsoft	Defender Antivirus 4.18		6	6	6

Tests for business users

More >

- Android Antivirus >
- MacOS Antivirus >
- Windows Antivirus >

Internet of Things (IoT)

More >

- Smart Home >
- IP Cameras >
- Smart Watches & Fitness-Tracker >
- Other >

Subscribe to the AV-TEST Newsletter

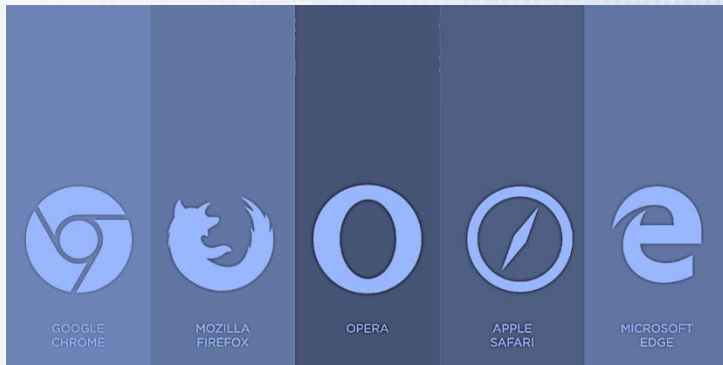
Well-informed on security

More >

SEGURANÇA DE NAVEGAÇÃO WEB

SISTEMAS WEB BROWSER

ALGUMAS
MELHORES
PRÁTICAS
PARA A SEGURANÇA



A Segurança do seu computador depende de vários fatores e de como é usado.

Um ponto de vital importância é o uso seguro de navegadores ou web browsers.

Tudo que se consulta, visita ou se faz na Internet conecta a sua máquina a grande nuvem web e aos seus inúmeros riscos e perigos on-line.

FUNDAMENTAL – REGRAS

- ❑ Mantenha seus navegadores web browsers sempre atualizados
- ❑ Use o “sistema browser” mais adequado para a sua finalidade de uso / navegação
- ❑ Conheça as características de cada sistema browser, suas origens e concepção
- ❑ Estude e evolua usando mecanismos de busca mais adequados

SEGURANÇA EMBARCADA DE ALGUNS NAVEGADORES

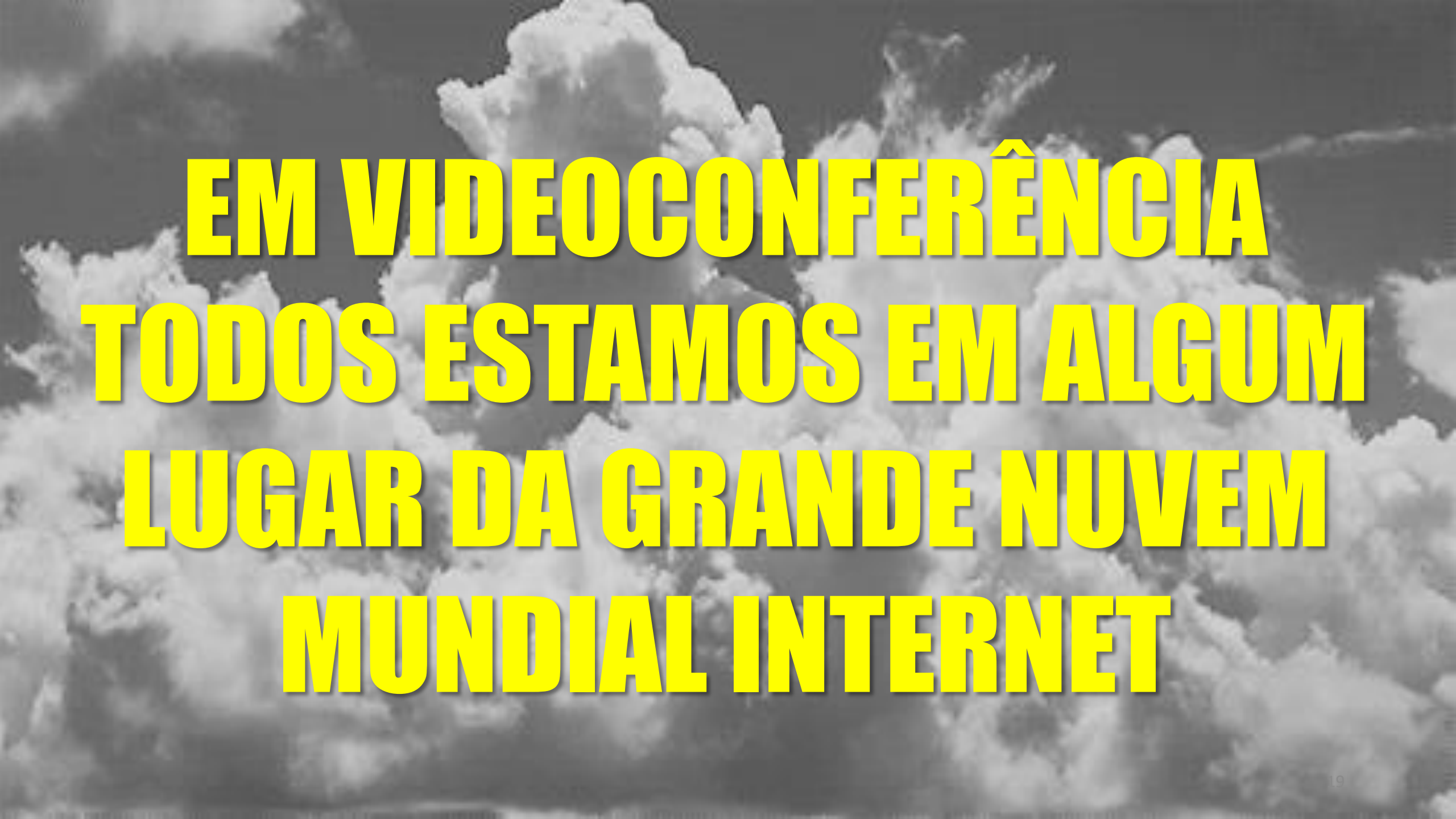
- ❑ Microsoft Edge 2020 – Usa Chromium e outros softwares livre
- ❑ Google Chrome - Usa Chromium e outros softwares livre
- ❑ Comodo Dragon - Usa Chromium e outros softwares livre
- ❑ Opera – Usa o motor Blink da Norueguesa Opera Software
- ❑ Mozilla Firefox – Usa motor evolutivo do Netscape
- ❑ Tor – Especializado – NRL (United States Naval Research Laboratory) e EFF (Electronic Frontier Foundation) – Super Seguro e Privado – só para “user “avançados
- ❑ SAFARI – Código fechado da Apple Inc.
- ❑ ...

Todos possuem suas características de segurança configurável.



SEGURANÇA EM VIDEOCONFERÊNCIAS





**EM VIDEOCONFERÊNCIA
TODOS ESTAMOS EM ALGUM
LUGAR DA GRANDE NUVEM
MUNDIAL INTERNET**

FUNDAMENTAL – REGRAS

- ☐ Conheça as opções de sistemas de videoconferência do mercado – avalie seu uso
- ☐ Use para negócios privados preferencialmente sistemas que permitam chave própria
- ☐ Nunca deixe no desktop e-mails ou aplicativos confidenciais abertos em segundo plano
- ☐ Evite colocar em chat de Lives informações pessoais ou de sua máquina
- ☐ Nunca entre em atividades de Internet Banking enquanto participa de Lives
- ☐ Tenha total domínio e controle sobre sua câmera, seu microfone e do desktop
- ☐ Muito cuidados com o que está aberto no desktop na hora de compartilhar telas

SEGURANÇA EMBARCADA - SISTEMAS DE VIDEOCONFERÊNCIA

- ☐ Microsoft Teams – criptografia da Microsoft
- ☐ Google Meet – criptografia da Google
- ☐ Zoom Cloud Meeting - criptografia da Zoom
- ☐ Cisco Webex Meetings – criptografia da Cisco
- ☐ Whereby Meeting – criptografia da whereby
- ☐ jit.si Meeting – criptografia da jit.si + possibilidade de **chave privada**
- ☐ ...

**NENHUMA É
90%
SEGURA**



BASIC SECURITY

CYBER SECURITY



NÍVEL DE CONHECIMENTO

1

2

3

4

5

6

7

8

9

10



SECURE
CONTROLS
FRAMEWORK

S|P Security | Privacy



TeleTrust

Pioneers in IT security.

Bundesverband IT-Sicherheit e.V.



Guia Estado da Arte em Segurança de TIC



3	Medidas técnicas e organizacionais (TOMs)
3.1	Informação geral
3.2	Medidas técnicas
3.2.1	Avaliação da força da senha
3.2.2	Reforçando senhas fortes
3.2.3	Autenticação multifator
3.2.4	Procedimentos criptográficos
3.2.5	Criptografia de disco
3.2.6	Criptografia de arquivos e pastas
3.2.7	Criptografia de e-mail
3.2.8	Protegendo a comunicação de dados eletrônicos com PKI
3.2.9	Uso de VPNs (camada 3)
3.2.10	Criptografia de camada 2
3.2.11	Troca de dados baseada em nuvem
3.2.12	Armazenamento de dados na nuvem
3.2.13	Uso de serviços móveis de voz e dados
3.2.14	Comunicação através de mensagens instantâneas
3.2.15	Gerenciamento de dispositivo móvel
3.2.16	Segurança do roteador
3.2.17	Monitoramento de rede usando Sistema de Detecção de Intrusão
3.2.18	Proteção de tráfego da Web
3.2.19	Proteção de aplicativo da Web
3.2.20	Acesso remoto à rede / manutenção remota
3.2.21	Proteção do servidor
3.2.22	Plataforma de detecção e resposta de endpoint
3.2.23	Usando a internet com isolamento da web
3.24	Detecção e análise de ataque (SIEM)
3.3	Medidas organizacionais
3.3.1	Padrões e normas
3.3.2	Processos

Os principais pontos do Guia foram traduzidos para o Português



Medidas Técnicas e Organizacionais “TOMs”



- **Technical and Organisational Measures** - especifica de forma objetiva que as questões de segurança do ambiente de tratamento de dados deva ser avaliada, ajustada e apoiada por medidas técnicas e administrativas, para que possam alcançar os resultados esperados. Ex.: Temos um sistema Antivírus instalado pela área de TIC, mas não há uma Norma Interna e controles administrativos, que especifiquem a execução sistemática de pesquisa de vírus nas máquinas da organização, portanto, existe um grande risco de que o Antivírus não cumpra o seu papel.
- **Medidas TO** – alguns exemplos a seguir:

Medidas Técnicas e Organizacionais “TOMs”

• Força das Senhas

Senha, chave ou password é a questão mais básica a ser tratada por TOM. O problema é disciplinar o ser humano e fazê-lo entender a importância e a “responsabilidade” de usar um padrão seguro e forte desse tipo de instrumento de segurança. Essa TOM é super importante para a organização e em especial para a vida privada do colaborador.

Boas senhas devem ter: mínimo de 16 dígitos – com números, letras MAIÚSCULAS e minúsculas e ainda símbolos especiais como !@\$%, por exemplo.

EM QUANTO TEMPO DESCOBRIRIAM SUA SENHA?

Com os computadores de hoje 2022 divida o tempo por 40 e não se assuste.

TAMANHO DA SENHA	SÓ NÚMEROS	MIX DE LETRAS MINÚSCULAS E MAIÚSCULAS	MIX DE LETRAS MINÚSCULAS, MAIÚSCULAS E NÚMEROS	MIX DE LETRAS MINÚSCULAS E MAIÚSCULAS, NÚMEROS E SÍMBOLOS
Pequena (3 a 5 caracteres)	INSTANTANEAMENTE	INSTANTANEAMENTE	ATÉ 3 SEGUNDOS	ATÉ 10 SEGUNDOS
Média (6 a 10 caracteres)	ATÉ 40 SEGUNDOS	ATÉ 169 DIAS	ATÉ 1 ANO 09 dias	ATÉ 928 ANOS
Grande (12 a 15 caracteres)	ATÉ 46 DIAS	ATÉ 28 MILHÕES DE ANOS	ATÉ 1 BILHÃO DE ANOS	ATÉ 2 TRILHÕES DE ANOS

Oriar o hábito de usar no mínimo 16 caracteres =128 bits - para facilitar a vida de todos no uso de sistemas criptográficos simétricos, que passarão a ser trivial na vida das pessoas.



Medidas Técnicas e Organizacionais “TOMs”



- **Autenticação Multifator**

Multi-factor authentication (MFA) and two-factor authentication (2FA) – são sistemas que ampliam a capacidade de autenticação de identidade dos usuários de sistemas computacionais. É muito usada no cotidiano em serviços bancários. O primeiro fator de autenticação é a “senha” que o usuário sabe. O Segundo fator é o código que um dispositivo do usuário pode mostrar (token ou QRcode), o terceiro fator pode ser o que somente “o usuário é” através da validação biométrica; datiloscópica, reconhecimento facial ou reconhecimento da voz, etc.

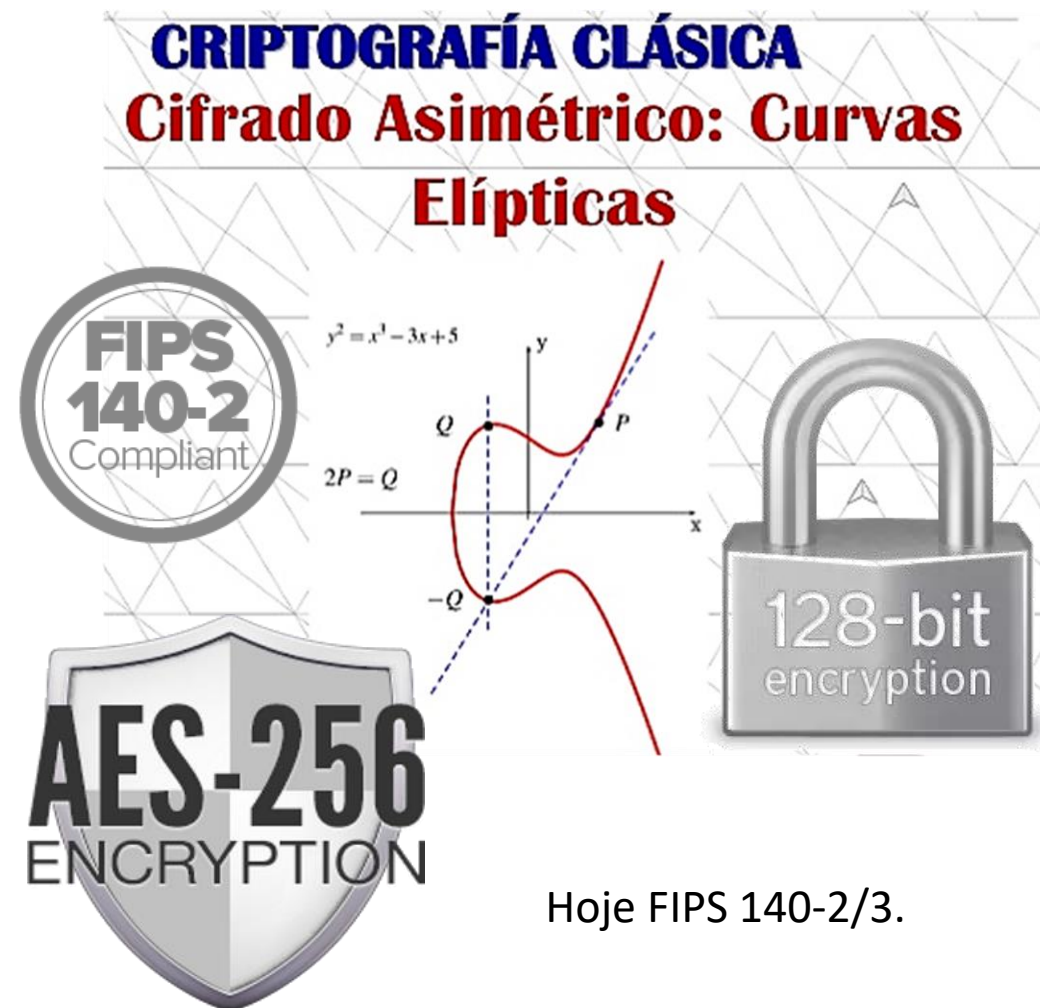
Usamos 3FA na LGPD, em sistemas de multi-criptografia forte.

Medidas Técnicas e Organizacionais “TOMs”

• Procedimentos Criptográficos

Criptografia é fundamental para garantir a segurança de dados. O uso de algoritmos de alta reputação e amplo domínio público é essencial para os melhores resultados. Sugerimos usar o algoritmo “Rijndael” ou **Advanced Encryption Standard (AES)**, ou Padrão de Criptografia Avançada, *em português*) – esse é o padrão do FIPS exigido pela RGPD. O AES usa chaves de 128, 192 ou 256 bits, ou seja, 16 caracteres para 128 bits, 24 caracteres para 192 bits e 32 caracteres para chaves de 256 bits. O AES pode operar de forma simétrica, assimétrica e com base em curvas elípticas.

Outros algoritmos também podem ser aplicados, como criptografia homomórfica.



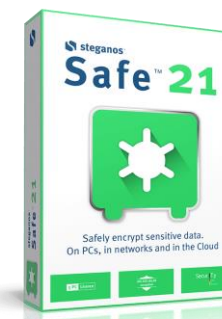
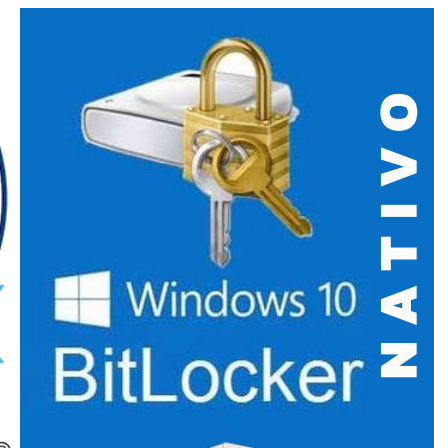
Hoje FIPS 140-2/3.

Medidas Técnicas e Organizacionais “TOMs”

- **Procedimentos Criptográficos**
- **Discos** – Todos os discos de computadores devem ser criptografados – de forma nativa no Windows ou através de utilitários.
- **Arquivos e Pastas** – Todos os arquivos e pastas, mesmo em discos criptografados, devem ser também criptografados de forma adicional. Neste caso sugerimos usar uma ferramenta ou utilitário diferente do nativo da máquina.

Teríamos no caso a “Bi-Criptografia” na máquina.

Para a LGPD usamos produtos diferenciados e TAMBÉM freewares – Open Source.



Não estamos recomendando estes softwares apenas indicando como exemplos.

Medidas Técnicas e Organizacionais “TOMs”

- **Procedimentos Criptográficos**

- Criptografia de e-mails

A criptografia de e-mails é uma das grandes necessidades para a proteção de dados, em especial dados pessoais.

Muitos sistemas de e-mail podem operar com criptografia padrão. É importante conhecer os meios de proteção e as opções de e-mails seguros gratuitos do mercado mundial.



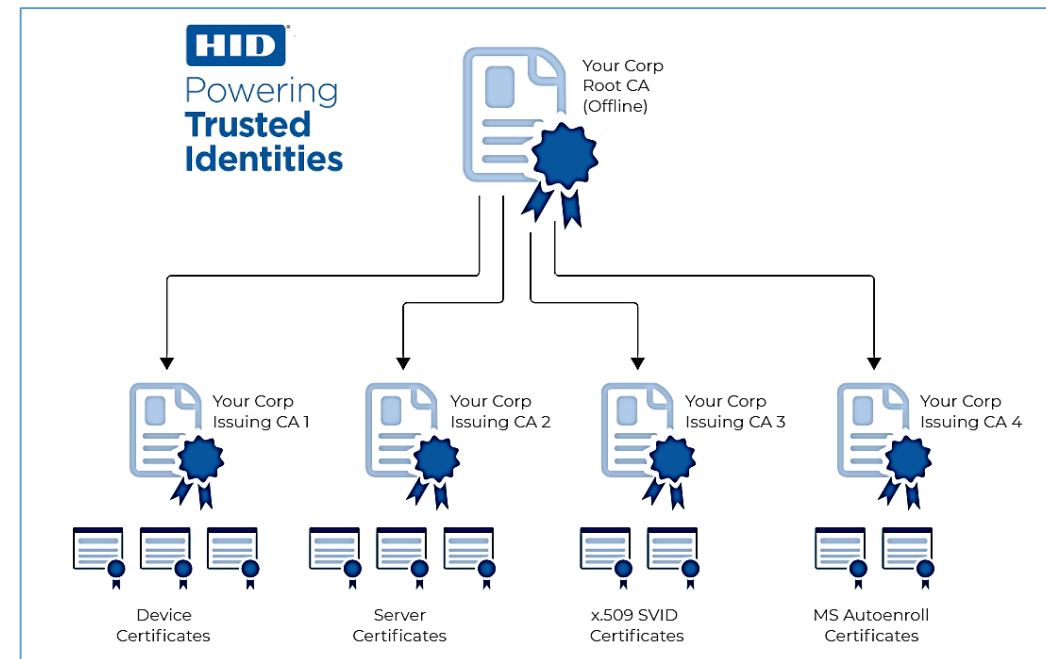
Medidas Técnicas e Organizacionais “TOMs”

- Procedimentos Criptográficos
- Usando Chaves Públicas PKI

O uso de PKI (Infraestrutura de chave pública) ou PKI Gerenciada (pública WAN ou privada LAN) está se tornando uma obrigação no mundo empresarial. Hoje é possível em redes LAN/WAN incluir um serviço via software da CERTIFICADORA que conecta seu ambiente AD e a AC SaaS da CERTIFICADORA, simplificando e automatizando o provisionamento de certificados DIGITAIS sem a necessidade de possuir uma AC local da Microsoft.

Conheça: <https://www.globalsign.com/pt-br/managed-pki>
<https://www.globalsign.com/pt-br/authentication/networks-vpns>
<https://www.websecurity.digicert.com/pt/br/pki/managed-pki-service>
<https://www.hidglobal.com.br/solutions/identity-access-management/identity-lifecycle-management/hydrantid-managed-pki-service>

Esta é uma solução LGPD para trabalho remoto nas empresas com VPNs e Certificados Digitais

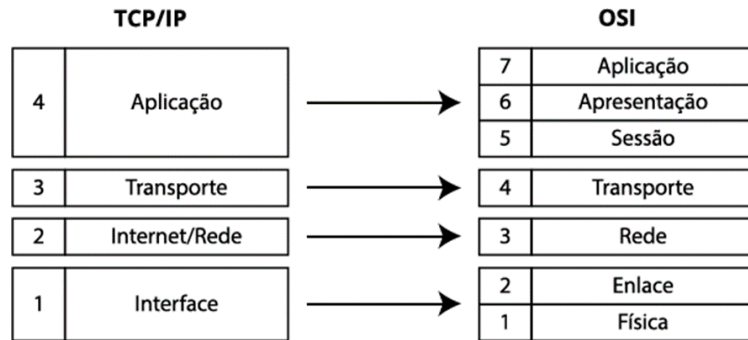


 **digicert**[®]

 **GlobalSign**[®]
GMO INTERNET GROUP

 **Powering Trusted Identities**

Medidas Técnicas e Organizacionais “TOMs”



- **Uso de VPNs (camada 3 OSI - Rede)**

O objetivo é usar serviços ou processos de comunicação com tunelamento de dados enviados através das Camadas de Enlace (L2TP, PPTP, L2F) e Rede (IPSec). IPSec é um protocolo definido pelo IETF utilizado para transferir dados de maneira segura na Camada de Rede. Ele é uma extensão do protocolo de internet IP, proporcionando segurança, garantindo a privacidade e integridade dos dados enviados.

O Encapsulated Security Payload (ESP) é um protocolo que protege os dados do pacote IP da interferência de outros, criptografando o conteúdo utilizando algoritmos de criptografia simétrica (pode ser o AES).

Contrate um bom serviços de VPN de Rede e fique mais tranquilo.

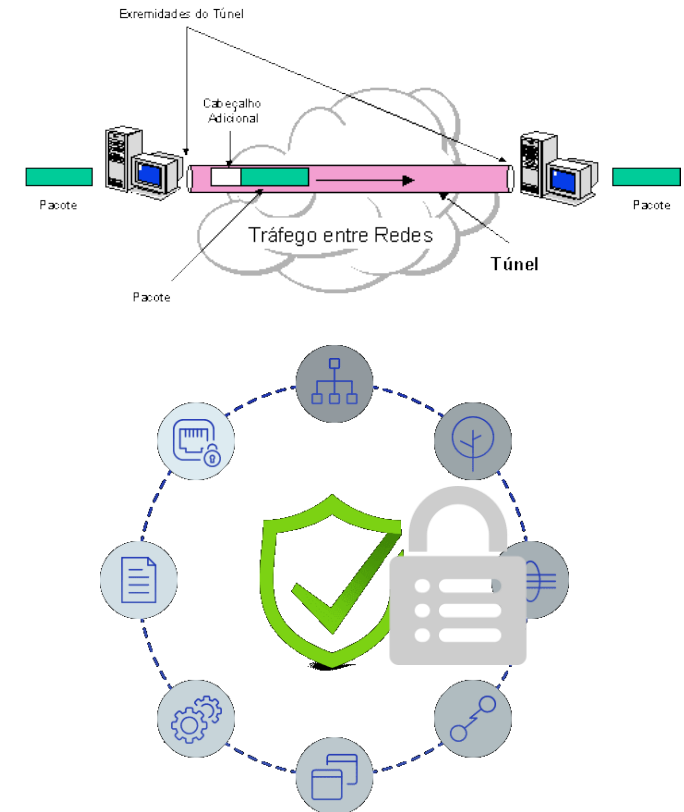


Medidas Técnicas e Organizacionais “TOMs”

- **Criptografia de camada 2 (enlace/interface)**

A criptografia da camada 2 é uma solução de segurança alternativa às VPNs da camada 3, que são utilizadas na carga útil de quadros Ethernet em vez de pacotes IP. Os cabeçalhos de IP não precisam ser processados (o que economiza tempo) e a carga na capacidade da linha é muito menor do que a criptografia através da camada 3 ou superior devido ao sobrecarga de criptografia. ***É uma solução Recomendada.***

Uma rede baseada em Ethernet (ponto a ponto, hub-spoke ou totalmente em malha) por meio de cabos dedicados (cobre / fibra de vidro) ou um serviço de camada 2 fornecido por provedores de rede (por exemplo, serviços Carrier Ethernet) é necessário para uso. A configuração de protocolos e parâmetros deverá ser do Gestor de Redes da organização.



Solução de criptografia entre roteadores e dispositivos físicos de Rede.

Medidas Técnicas e Organizacionais “TOMs”

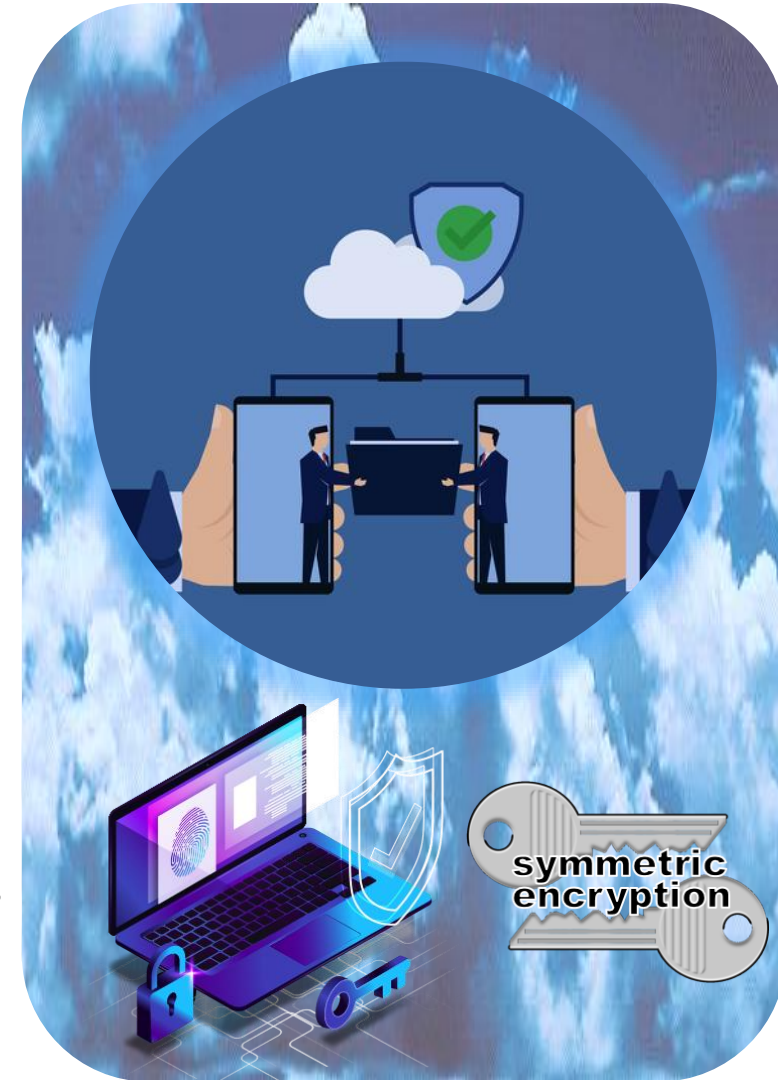
- **Troca de dados em nuvem**

Os dados em um serviços de troca de dados baseado em nuvem são suscetíveis às seguintes ameaças:

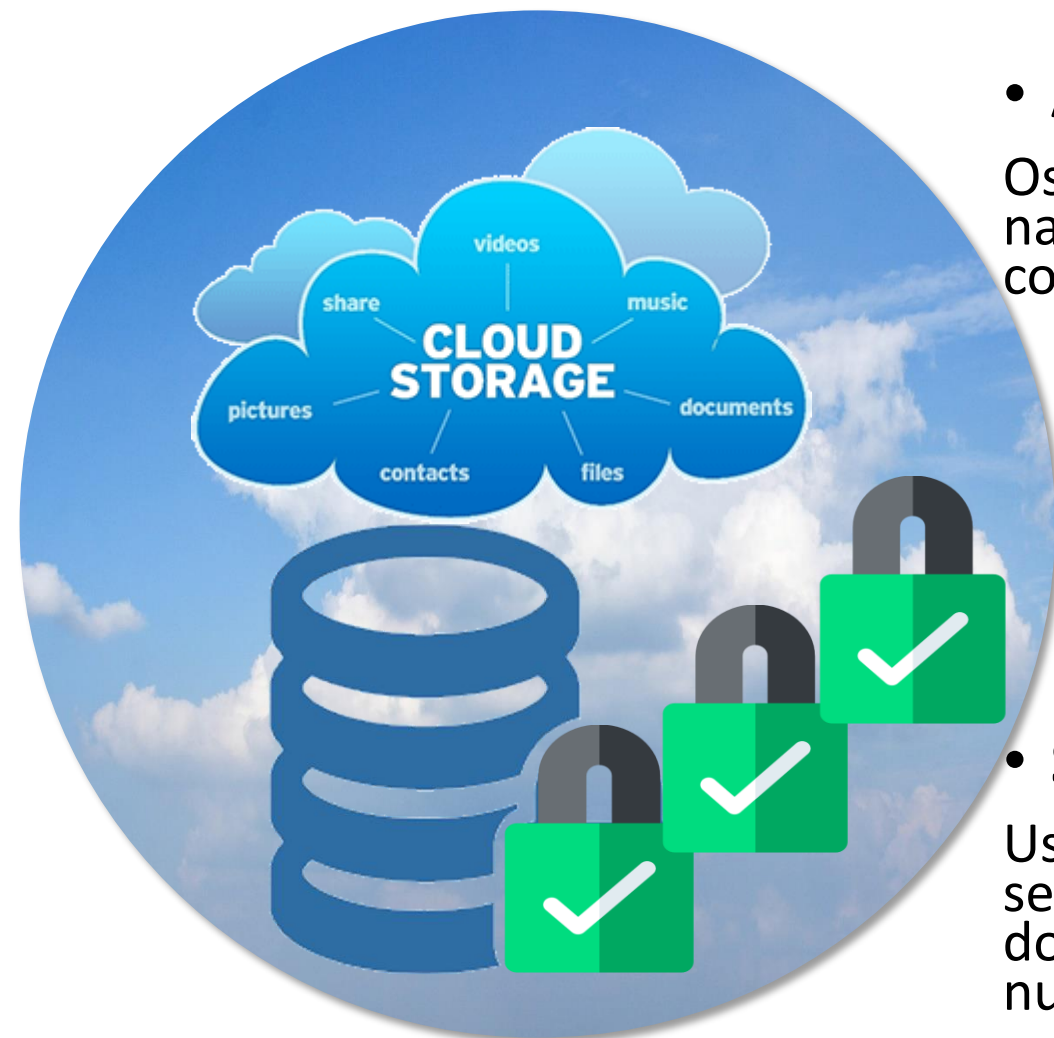
- Acesso não autorizado e inspeção pela operadora do serviço
- Hacking por terceiros enquanto os dados são transportados pela internet – para depósito e para baixar
- Furto ou uso não autorizado ou hackeada a identidade que foi acordada com o serviço de nuvem.

- **Como proteger**

- Tenha sempre “Confiança ZERO” – (Zero Trust) em serviços cloud.
- Use sua própria criptografia para proteger os dados enviados.
- Remeta a senha por e-mail ou outros meios de mensagens.
- Todos os documentos do Office podem ser protegidos de forma nativa, mas também é possível usar outras ferramentas mais fortes ou avançadas.
- A segurança depende dos dois lados – remetente e destinatário.



Medidas Técnicas e Organizacionais “TOMs”



- **Armazenamento de dados em nuvem free**

Os dados confidenciais ou não, armazenados ou processados nas nuvens são suscetíveis a muitas formas de comprometimento, incluindo:

1. acesso não autorizado à nuvem (por usuários externos e internos);
2. acesso por administradores de nuvem externos ou centros de dados;
3. interceptação durante a transmissão entre a organização e a nuvem;
4. furto de armazenamento em nuvem;
5. Perda de dados por falha de serviços de manutenção.

- **Segurança**

Use apenas para serviços temporários, nunca para backup, e sempre que necessário criptografados conforme a criticidade dos dados armazenados. Evite colocar dados confidenciais em nuvens, a não ser com multi-criptografia forte.

Para atender a LGPD usamos multi-criptografia forte em todos os tratamentos de dados pessoais.

Advanced Security



Medidas Técnicas e Organizacionais “TOMs”

- **Uso de serviços móveis – voz e dados**

A telefonia fixa e móvel clássica hoje também é uma das formas mais diretas e pessoais de comunicação, apesar das aplicações de chat e webconferências. No entanto, apresenta vários riscos e oferece vetores de ataques em potencial. A grande maioria das chamadas telefônicas feitas de telefones fixos (IP ou não) também envolvem o participação de um telefone celular (de origem ou de destino). Telefonia celular e comunicação por esse meio tem segurança ZERO. Evite fazer transações de negócio via telefones celulares.

USE SISTEMAS COMPATÍVEIS DE CRIPTOGRAFIA PARA EQUIPAMENTOS MÓVEIS – PODEM SER NATIVOS OU APPs

Smartphones modernos com qualquer sistema operacional podem ser configurados para usar criptografia nativa confiável.



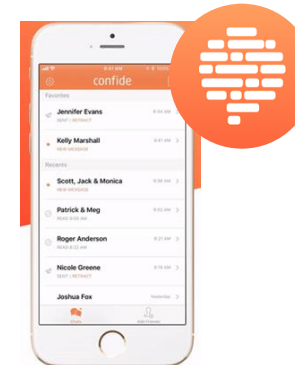
Medidas Técnicas e Organizacionais “TOMs”

• Sistemas de mensagens

A privacidade online nunca foi tão discutida como nos dias atuais. Com o aumento da espionagem, muitos usuários estão trocando seus tradicionais serviços de mensagens (SMS) e e-mails por soluções seguras. O aumento da demanda por serviços seguros fez com que várias empresas de tecnologia desenvolvessem aplicações que prometem trocas de mensagens criptografadas pelos usuários. Há vários aplicativos para os principais sistemas móveis disponíveis. Os riscos ainda existem:

1. Gravar, analisar e modificar o conteúdo por um terceiro não autorizado (man-in-the-mid-ataque - **dle**).
2. Furto de identidade dentro de um sistema de comunicação.(Clone WhatsApp, por exemplo).
3. Roubo/Furto de equipamento para análise posterior de dados de mensagens instantâneas sem autorização.

A proteção é similar ao uso de e-mails em dispositivos móveis.



Confide - App aplicativo confidencial de mensagens. Combinamos a criptografia de ponta a ponta com mensagens que desaparecem e são protegidas contra captura de tela para garantir que a sua comunicação seja privada e realmente permaneça assim.

Medidas Técnicas e Organizacionais “TOMs”

- **Gerenciamento de dispositivos móveis**

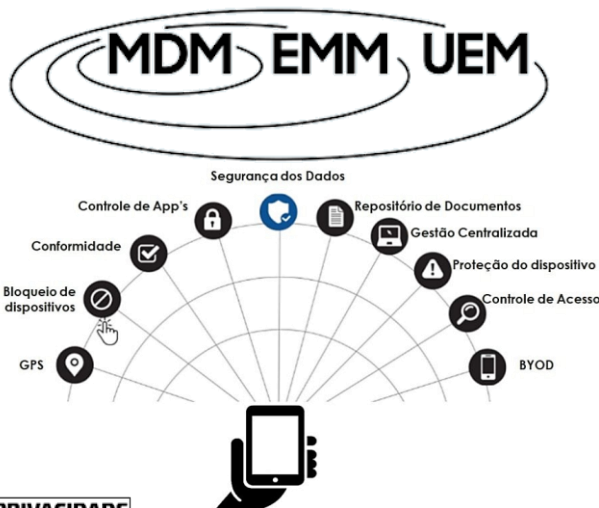
O uso de soluções de gerenciamento de dispositivos móveis (MDM) reduz os riscos de segurança que surgem devido a uso controlado de dispositivos móveis para fins comerciais. As soluções de MDM tornam possível centralizar a administração e configuração dos dispositivos móveis usados. Sempre haverá riscos operacionais e de controle. As seguintes contramedidas são recomendadas:

- Criptografia de comunicação de voz e dados por meio de aplicativos ou hardware adequados e confiáveis que atendem aos padrões de criptografia atuais e regras de proteção de dados aplicáveis para criptografia end-to-end.
- A configuração central dos terminais pela organização emissora ou que apóia BYOD por meio de sistemas de gerenciamento de dispositivo móvel (MDM / EMM) para evitar o acesso indesejado do usuário a atividades de aplicativos que levam à infecção do telefone celular.
- Para níveis mais altos de confiabilidade, o uso de telefones celulares com sistemas operacionais reforçados que certifique-se de que o microfone e o alto-falante sejam usados apenas pelo aplicativo de criptografia e evite qualquer malware de hackear a chave de criptografia.

 MobiLock Pro



 SOTI
MOBICONTROL



<https://www.capterra.com.br/directory/30584/mobile-device-management/software>

Medidas Técnicas e Organizacionais “TOMs”

• Segurança do Roteador

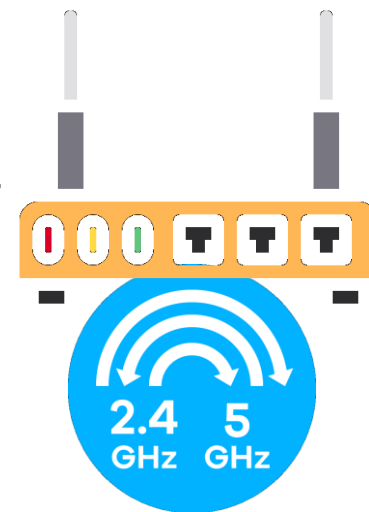
"Customer Premise Equipment" (CPE) é o equipamento usado para conectar assinantes a uma Rede Internet do provedor de serviços (ISP). Exemplos de CPE incluem modems (cabos, xDSL, fibra) e roteadores WiFi, entre outros.

Os roteadores têm o objetivo de redirecionar os dados de maneira confiável e segura, ao mesmo tempo que os protegem contra o acesso não autorizado.

Devido a vulnerabilidades no software embutido e nas configurações padrão, o CPE (roteador) tem sido o alvo de uma variedade de abusos:

As seguintes ameaças / riscos podem comprometer os roteadores:

1. Manipulação de configuração;
2. Ataques usando brechas conhecidas na segurança e aquelas que não foram fechadas;
3. Ataques usando lacunas de segurança recentemente descobertas (exploits de dia zero);
4. Ataques por meio de conexões de telefonia IP;
5. Furto (especialmente roteadores de comunicação externa / móvel);
6. Ataques de disponibilidade (ataques DoS);
7. Acesso por meio de interfaces não documentadas (ver as chamadas "portas traseiras");
8. Execução de código de terceiros e integração em botnets;
9. Ataques via WLANs inadequadamente protegidas.



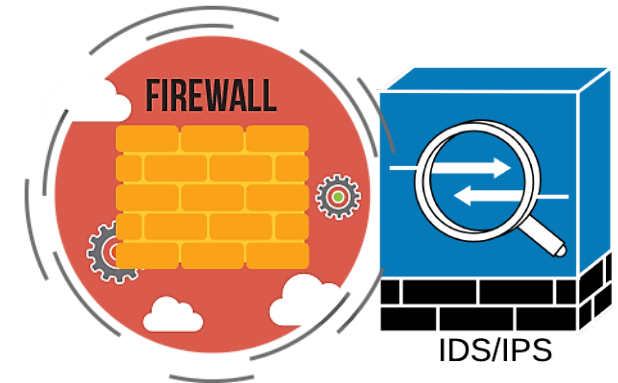
<https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1.pdf>

Medidas Técnicas e Organizacionais “TOMs”

• Monitoramento de Redes IDS/IPS (appliance H/S)

Sistema de detecção de intrusão (IDS) ou sistema de prevenção de intrusão (IPS). O objetivo de ambos os sistemas é detectar intrusão e propagação de malware antes que o dano ocorra, se possível. IDS e IPS são utilizados para prevenir:

1. Vazamento de informações devido à interceptação remota de dados confidenciais nas redes
2. Uso indevido de serviços e protocolos de comunicação
3. Acesso indevidos de terceiros à rede de TI ou aos sistemas de TI
4. Exploração de oportunidades para acessar sistemas de TI vinculados
5. Manipulação de informações ou software
6. Contaminação geral de malware na rede de TI



Medidas Técnicas e Organizacionais “TOMs”

• Proteção de tráfego WEB

Ao visitar um site infectado, o malware é carregado e ativado no sistema local sem ser notado pelo usuário (downloads by-drive).

Os invasores também usam servidores da Web fornecidos especialmente que muitas vezes imitam outro site. No caso de “Phishing”, essas cópias falsas de sites conhecidos são fornecidas com o objetivo de obter informações confidenciais informações do usuário, geralmente nomes de usuário e senhas, além de informações bancárias, cartão de crédito informações, endereços, etc.

Filtros da web protegem contra esses ataques, bloqueando os sites em questão e analisando os dados carregados por sites para malware e códigos maliciosos.

O Windows nativamente usa um Firewall e Sistema Proxi de Aplicativos para navegação WEB segura, mas nem sempre é suficiente.

Se a Microsoft detectar um ataque de ransomware, você receberá um e-mail ou notificação. Para se recuperar de ransomware, corrupção de arquivos, ataques mal-intencionados ou exclusões acidentais, restaure seu OneDrive para uma hora anterior.



Microsoft

quatro maneiras de se manter seguro online

Com a presença e sofisticação crescentes de ameaças online, como vírus, ransomware e golpes de phishing, é importante ter a proteção certa. A Microsoft oferece ferramentas de segurança avançadas para ajudar a manter suas informações seguras e privadas.

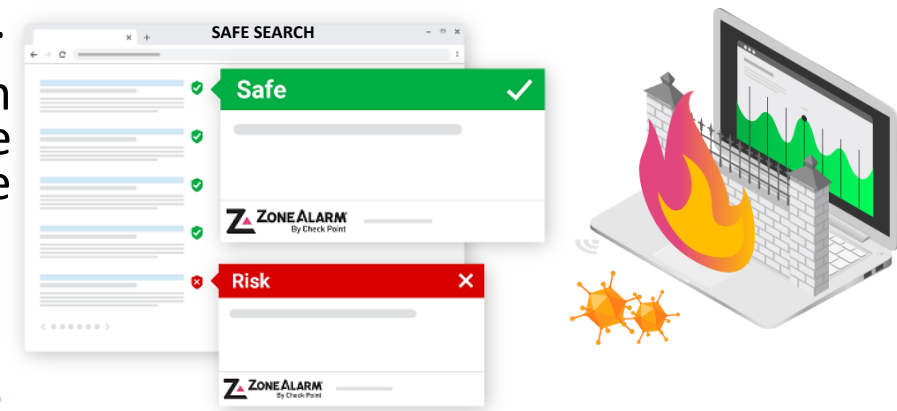
1. Evitar vírus e golpes de phishing

- 35%** Malwares e vírus atacam seu computador ao visitar sites mal-intencionados ou baixar arquivos infectados. 35% de todos os computadores globais são infectados por malware.
- 23%** Os hackers usam scams de phishing para tentar roubar sua identidade ou o seu dinheiro enviando e-mails de aparência oficial para obter informações pessoais confidenciais. 23% das pessoas abrem e-mails de phishing.
- Para se manter seguro, use Outlook.com para enviar e receber e-mails. O Outlook.com usa técnicas avançadas de detecção para verificar a presença de vírus em anexos e avisa se você clicar em um link suspeito.

Detectamos um link não seguro.

O Microsoft bloqueou o link <http://www.unsafe>

[Retornar ao Outlook](#)



<https://www.zonealarm.com/software/free-firewall>

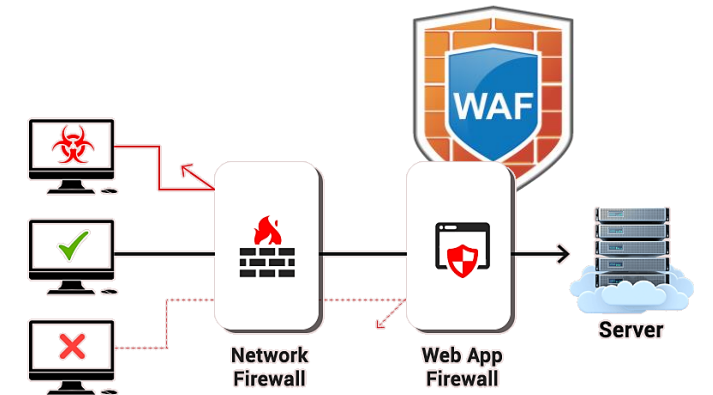
<https://www.zonealarm.com/software/web-secure-free>

Medidas Técnicas e Organizacionais “TOMs”

• Proteção de Aplicativos WEB

Os servidores que hospedam sites da Web são uma das principais formas de espalhar malware. Os servidores da web infectados são frequentemente usados onde o operador não está diretamente envolvido no ataque. Uma grande porcentagem de servidores web tem brechas de segurança através das quais eles podem ser atacados por hackers e que, em seguida, armazenam malware no sistema, geralmente os chamados root kits.

Para a **Proteção** use um Web Application Firewall (**WAF**) para proteger os aplicativos da web (homepages, lojas online, home banking portais, etc.) de ataques. O WAF inspeciona a comunicação entre usuários e aplicativos da web no nível do aplicativo e bloqueia o tráfego de dados potencialmente prejudicial, como injeções de SQL ou entre sites scripts. O termo "Web Service Firewall" (**WSF**) também é amplamente utilizado para comunicação máquina a máquina em comunicação na Internet.



WebKnight

Open Source Web Application Firewall for IIS

imperva



modsecurity

Open Source Web Application Firewall



Medidas Técnicas e Organizacionais “TOMs”

• Acesso remoto à Rede e Manutenção remota

As redes remotas precisam ser acessíveis pela Internet para fins de manutenção ou atualização de softwares.

Em um ambiente industrial, esses participantes são componentes de controle de máquina, como PLC, drive unidades e painéis operacionais. Em caso de manutenção ou atualização de software, o usuário remoto deve acessar esses sistemas online com as ferramentas do fabricante (como software de programação PLC).

Contra quais ameaças à segurança de TI a medida é usada?

- Acesso não autorizado à rede da empresa ou ao seu computador
- Acesso não autorizado a sistemas de destino
- O acesso remoto não pode ser rastreado
- Captura de dados ou exposição durante uma sessão de manutenção remota

Dependendo da aplicação, conexões puras de terminal também podem ser estabelecidas e lidas por meio de manutenção remota. Isso inclui acesso à Web, RDP, VNC e SSH, por exemplo.



Medidas Técnicas e Organizacionais “TOMs”

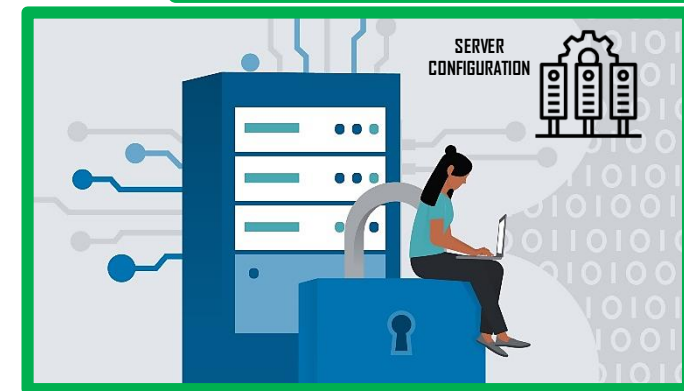
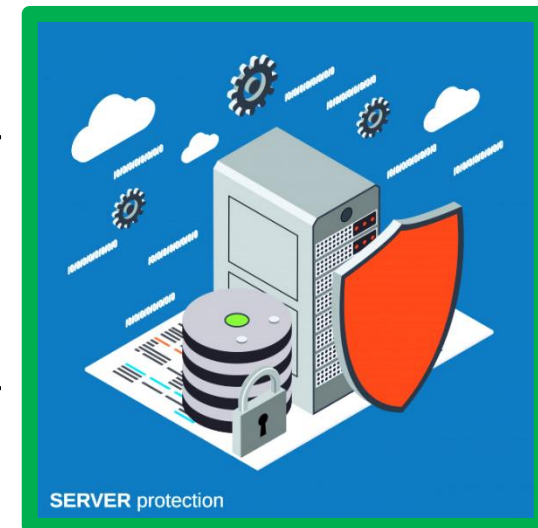
• Proteção de Servidores

Uma vez que os sistemas de servidor processam e armazenam os dados pessoais e essenciais (muitas vezes sensíveis) da empresa, os sistemas utilizados devem ser especialmente protegidos. A proteção do servidor é uma medida de segurança muito eficaz. Ele protege o sistema operacional, independentemente de ser um servidor físico, virtual ou baseado em nuvem.

Sistemas operacionais de servidor comuns, como Microsoft Windows Server ou vários sistemas Linux Server, não têm uma configuração de segurança muito restritiva por padrão e são potencialmente equipados com dispositivos e componentes diversos desnecessários. Muitas vezes, essas funcionalidades não utilizadas e não configuradas são usadas por invasores para comprometer o sistema operacional.

As principais ameaças para sistemas servidor não protegidos são:

- o Manipulação de dados pessoais e dados confidenciais da empresa
- o Perda de dados (por exemplo, sistemas de banco de dados inteiros)
- o Manipulação de aplicativos ou sistemas conectados
- o Manipulação, sabotagem ou espionagem dos processos de operação e produção
- o Furto de identidade (por exemplo, ataques a controladores de domínio)
- o Incorporação de malware de qualquer tipo e distribuir malware para outros sistemas
- o Abuso da capacidade do servidor para benefícios do invasor (por exemplo, criptografia de mineração)
- o Uso indevido de servidores para movimento lateral para atacar outros sistemas



A segurança de Servidores depende muito das configurações e dos Técnicos de TIC.

Medidas Técnicas e Organizacionais “TOMs”

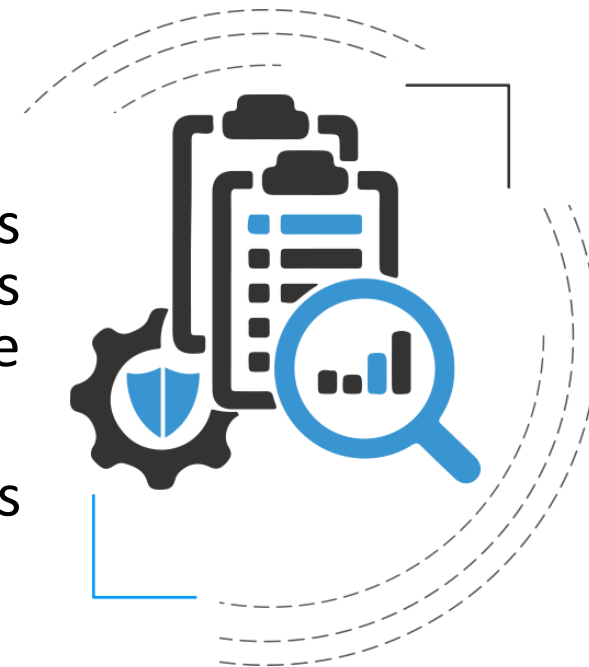
- **Proteção de Servidores (continuação)**

Para sistemas operacionais de servidor comuns, diretrizes de proteção mais detalhadas estão disponíveis publicamente:

- STIGs (Guias de Implementação Técnica de Segurança):
<https://iase.disa.mil/stigs>
- CIS Benchmarks ("Center for Internet Security, Inc."):
<https://www.cisecurity.org/cis-benchmarks>
- Orientação de segurança da Microsoft:
<https://blogs.technet.microsoft.com/secguide/>

A maioria das medidas de endurecimento pode ser realizada por ajustes técnicos. Essas configurações podem ser distribuídas para todos os sistemas de servidor da empresa automaticamente com um pacote de proteção (como scripts de proteção).

Novos sistemas de servidor devem ser protegidos imediatamente após a instalação com o respectivo pacote de configuração segura.



Medidas Técnicas e Organizacionais “TOMs”

• Proteção por Endpoint

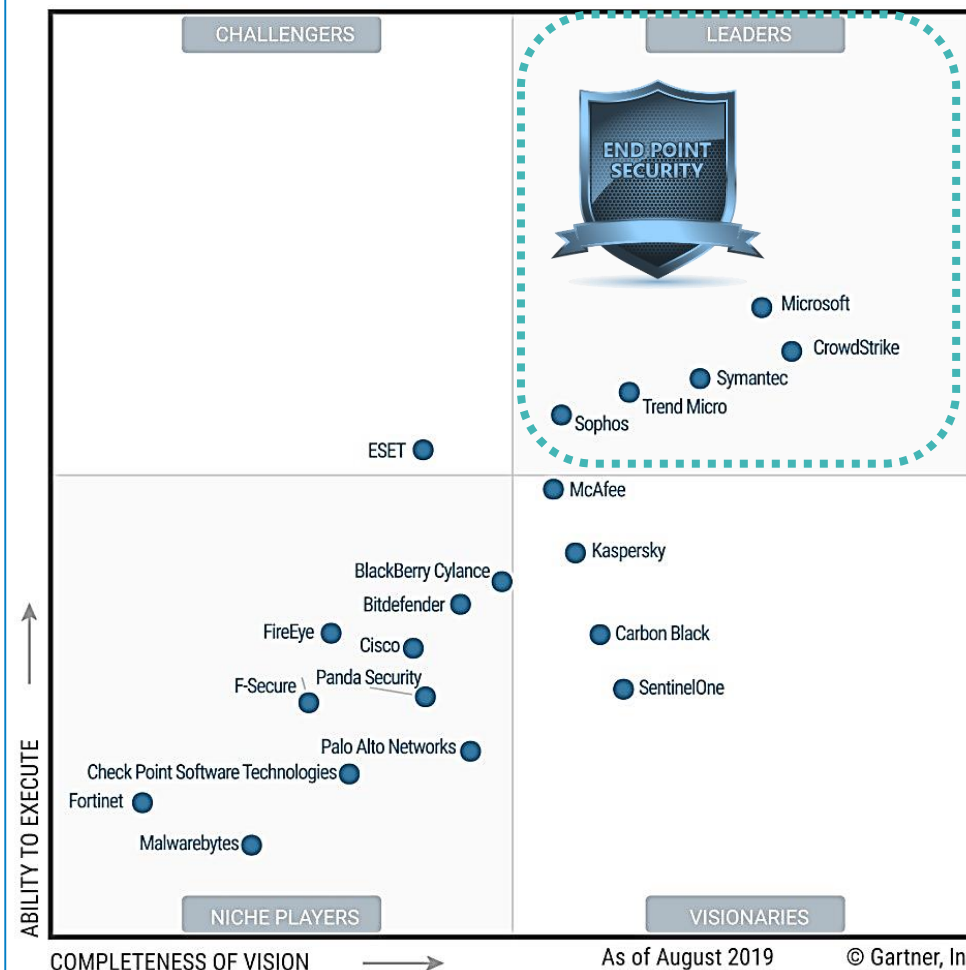
A proteção de dispositivos finais (por exemplo, PCs, laptops, smartphones ou tablets) agora requer muito mais do que apenas um programa antivírus. Soluções modernas (plataformas de detecção e resposta de endpoint, EDR) combinam as mais recentes tecnologias de proteção para impedir todos os tipos de ataques cibernéticos em sistemas cliente e servidor em sistemas operacionais e para identificar os originadores. Ao contrário das soluções convencionais, endpoints não requer conhecimentos adicionais dos técnicos:

Contra quais ameaças à segurança de TI a medida é usada?

- Malware
- Exploração
- Scripts maliciosos
- Atividades de hackers
- Abuso de ferramentas administrativas e ferramentas com intenção maliciosa

Soluções em hardware e software integrados.

Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (August 2019)

Medidas Técnicas e Organizacionais “TOMs”

• Proteção por Endpoint (Continuação)

A plataforma de proteção endpoint fornece um conjunto de utilitários de segurança para proteger Servidores, PCs e tablets. Fornecedores especializados competem pela qualidade de recursos de proteção e facilidade de administração.

Esta plataforma corporativa de proteção de endpoint normalmente é composta pelos seguintes itens:

- Anti-malware
- Anti-spyware
- Firewalls pessoais
- Host-based prevenção de intrusão
- Acesso e controle do dispositivo
- Criptografia de disco completa e arquivo, também conhecida como proteção de dados móveis
- Endpoint prevenção de perda de dados (DLP)
- Avaliação de vulnerabilidades
- Controles de aplicação
- Gerenciamento de dispositivos móveis (MDM)



Medidas Técnicas e Organizacionais “TOMs”

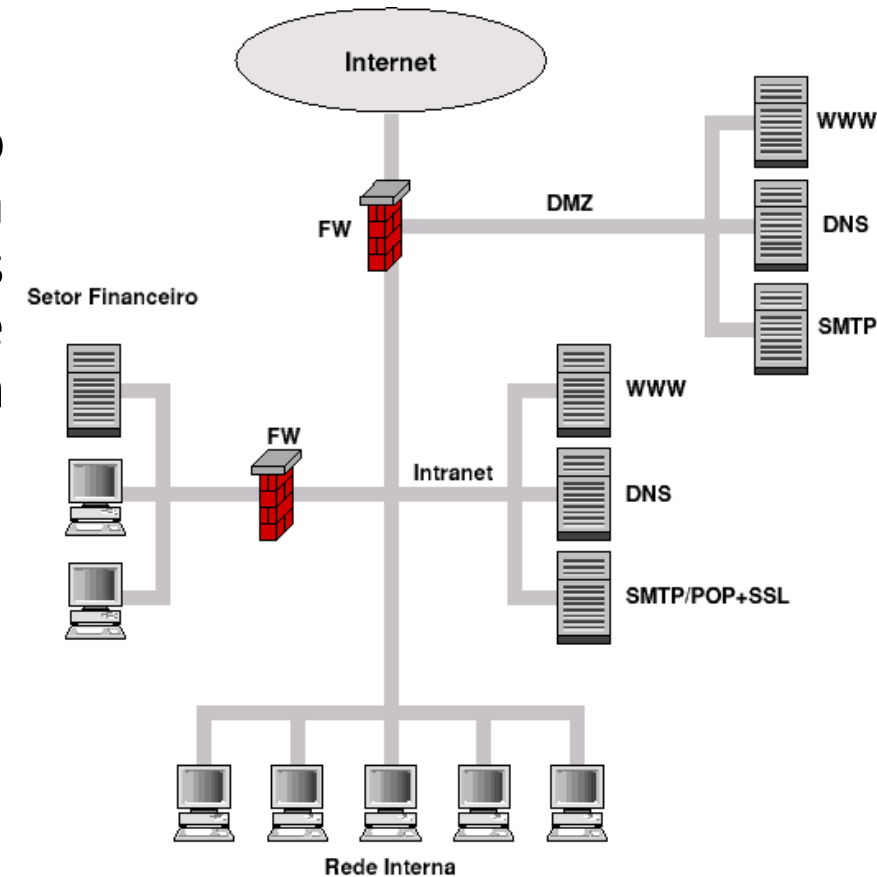
• Usando a Internet com isolamento WEB – DMZ

O isolamento da Web separa a área de trabalho do usuário das sessões do navegador e permite o uso seguro da Internet sem limitar o conteúdo ou funcionalidade. Ataques cibernéticos assistidos por navegador, fluxo / perda de dados e os restrições de produtividade e danos à imagem são evitados com eficácia.

Contra quais ameaças à segurança de TI a medida é usada?

Infecção da estação de trabalho ou computadores, por exemplo, por:

- Vulnerabilidades do navegador, downloads by-drive, sites infecciosos...
- Ransomware, APT, Trojans, Viruses, Worms, exploits de dia zero...
- links maliciosos em e-mails...



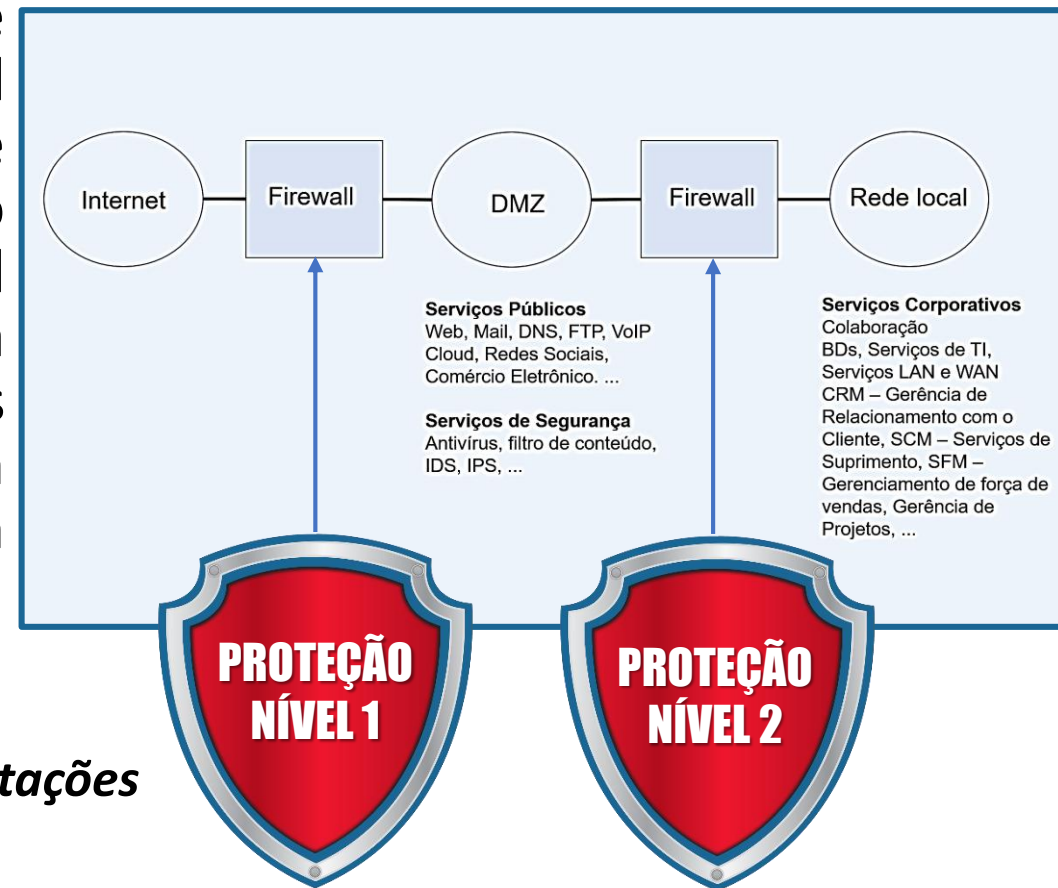
DMZ="Demilitarized Zone" ou zona aparentemente desprotegida.

FW=Firewall – usar especificamente um para isolar cada área crítica, como o financeiro.

Medidas Técnicas e Organizacionais “TOMs”

• Usando a Internet com isolamento WEB – DMZ (continuação)

A abordagem mais segura é usar dois firewalls de rede para criar uma DMZ. O primeiro firewall também chamado de “firewall de perímetro” é configurado para permitir o “tráfego destinado somente ao DMZ”. O segundo firewall ou “firewall interno” permite apenas o “tráfego da DMZ para a rede interna”. Este método é considerado mais seguro uma vez que teriam de serem comprometidos dois dispositivos, antes de um invasor acessar a rede interna.



Não confundir Firewall de Rede, como Firewall Pessoal das estações de trabalho, que é um terceiro nível de proteção.

INCIDENTES DE SEGURANÇA



A CHAVE É NOSSA

Na LGPD é obrigatória a transparência

LGPD, em seu art. 48, prevê a necessidade de comunicação pelo Controlador: tanto ao titular dos dados quanto à ANPD sobre a ocorrência de **incidentes de segurança** que possa trazer risco ou dano relevante aos titulares de dados pessoais.

Art. 48. (...)

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

- I - ampla divulgação do fato em meios de comunicação; e
- II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Ferramental para tratar IS – e IS-PII da LGPD

- sistemas IDS(Intrusion Detection System) e ou IPS (Intrusion Prevention System) (já citado),
- sistemas DLP (Data Loss Prevention – prevenção de vazamentos de dados),
- sistemas SIEM (Security Information and Event Management – correlação de eventos e Logs),
- sistemas **Honeypot** (para simulação de falhas e coleta de dados de invasores, fazendo-os pensar que estão alcançando o ataque real), ...
- TUDO PARA COMPOR UM **CSIRT** - CSIRT é um grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais. Pode ser um serviço prestado por uma empresa especializada ou uma unidade da própria empresa.
- Maiores detalhes em <https://www.cert.br/>

Strategic Security



CSO 
CHIEF SECURITY OFFICERS

Medidas Técnicas e Organizacionais “TOMs”

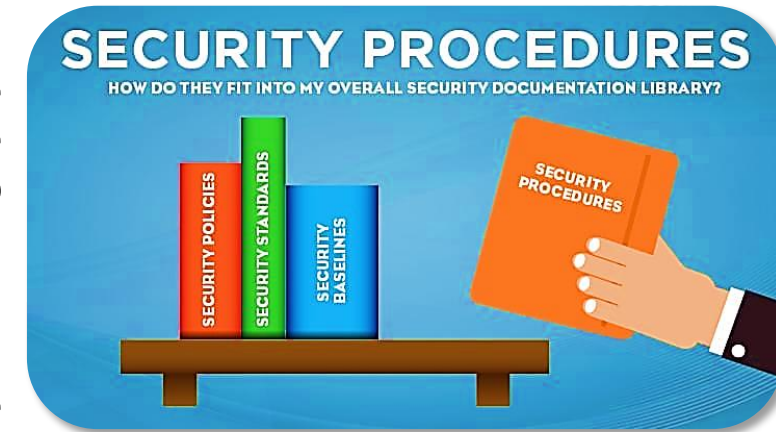
- **Medidas Organizacionais – é necessário AÇÃO!**

Os recursos computacionais de informação e comunicação nem sempre são projetados para a segurança como uma questão de princípio e a segurança técnica só é eficaz quando adequadamente acompanhada por processos organizacionais e medidas de impacto no âmbito pessoal.

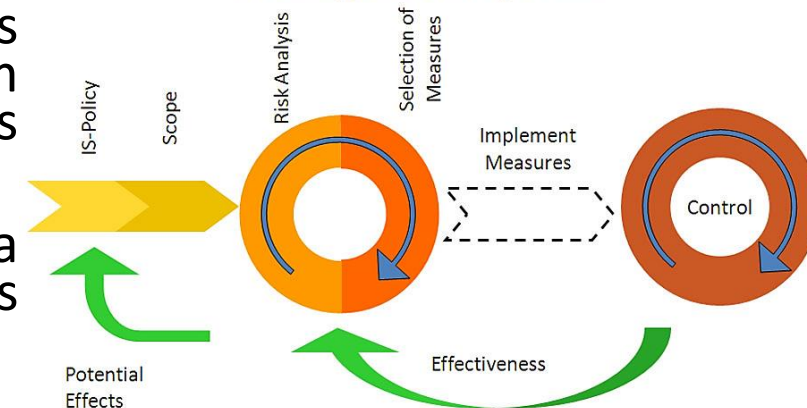
Cada organização precisa adotar sistemas e métodos, “Políticas, Processos e Procedimentos” - com regras para gerenciar a segurança da informação corporativa, ou em outras palavras, um Sistema de Gestão de Segurança da Informação (SGSI), de preferência, que tenha reconhecimento internacional.

Há uma série de padrões e normas internacionais que podem servir de base para a implementação de um ISMS. Ao contrário das medidas técnicas, as mudanças contínuas nas medidas organizacionais são um fenômeno de longo prazo, o que significa que a referência a padrões e normas é possível mesmo no contexto do "estado da arte".

A série ISO / IEC 27000 é usada aqui, como um ponto de referência para outras normas e padrões de segurança, a serem implementadas gradativamente.



ISO 27001 Information Security Management system

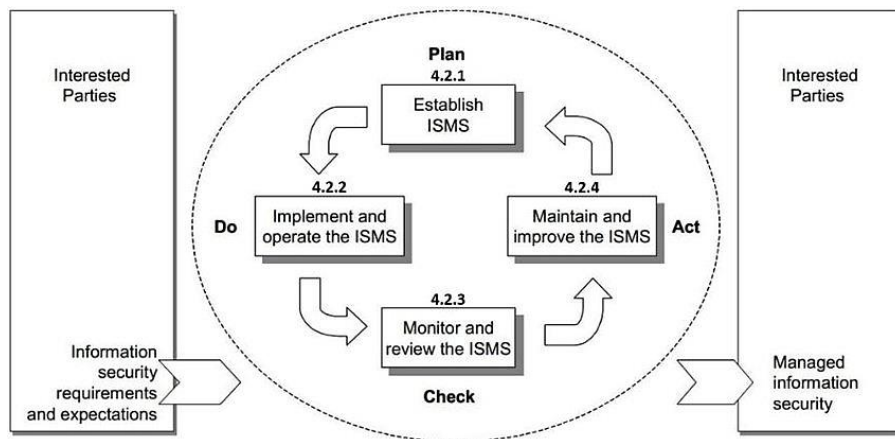


Medidas Técnicas e Organizacionais “TOMs”

Structure of ISO 27001



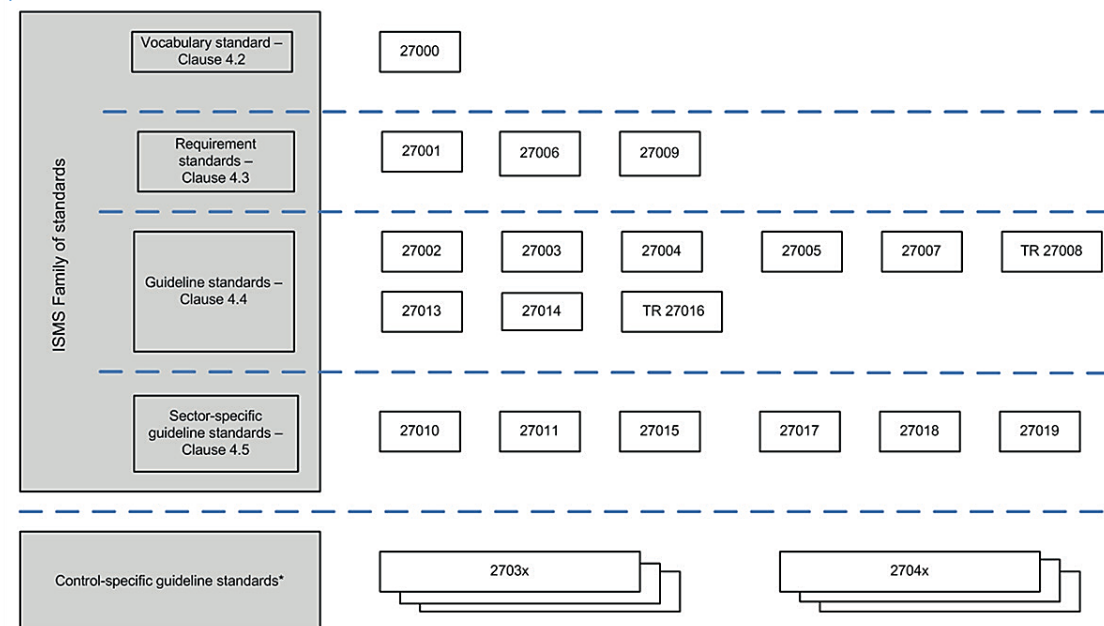
- 11 Information Security Control Areas
- 39 Information Security Control Objectives
- 134 Information Security Controls



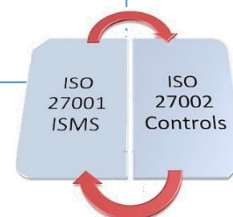
11 Control Areas:

1. Security Policy
2. Organization of Information Security
3. Asset Management
4. Human Resource Security
5. Physical & Environmental Security
6. Communication and Operation Management
7. Access Control
8. Information systems acquisition, development and maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

• Família de Normas ISO/IEC 27000



* out of the scope of this document



Medidas Técnicas e Organizacionais “TOMs”

• Padrões e Normas – definindo Políticas nas Empresas

Para uma organização definir uma Política ampla de SI (Segurança da Informação) é fundamental conhecer Normas e Padrões internacionais:

A série ISO / IEC 27000 inclui os seguintes itens principais, cada um dos quais funciona como um padrão e agrupados são uma série de padrões:

- ISO / IEC 27000 Termos e definições usados na série da norma ISO / IEC 27000
- ISO / IEC 27001 Requisitos para um ISMS (Information Security Management System)
- ISO / IEC 27002 Recomendações para mecanismos de controle de segurança da SI
- ISO / IEC 27003 Guia para implementação da ISO / IEC 27001
- ISO / IEC 27004 Avaliação da eficácia do ISMS
- ISO / IEC 27005 Desenvolvimento e operação gerenciamento de risco de SI
- ISO / IEC 27031 Guia conceitos ao suporte de TI para continuidade de negócios
- ISO / IEC 27034 Segurança de aplicativos
- ISO / IEC 27035 Gestão de Incidentes de Segurança da Informação

Na visão mais ampla também aplicamos o **SCF** (Security Control Framework) como padrão de Segurança e Privacidade **S|P**.



International
Organization for
Standardization



INTERNATIONAL
ELECTROTECHNICAL
COMMISSION



Health Insurance Portability
and Accountability Act



SECURE
CONTROLS
FRAMEWORK

O SCF é um framework integrado de todas as Normas e Padrões de maior importância para SI, PII e PHI (Protected Health information).

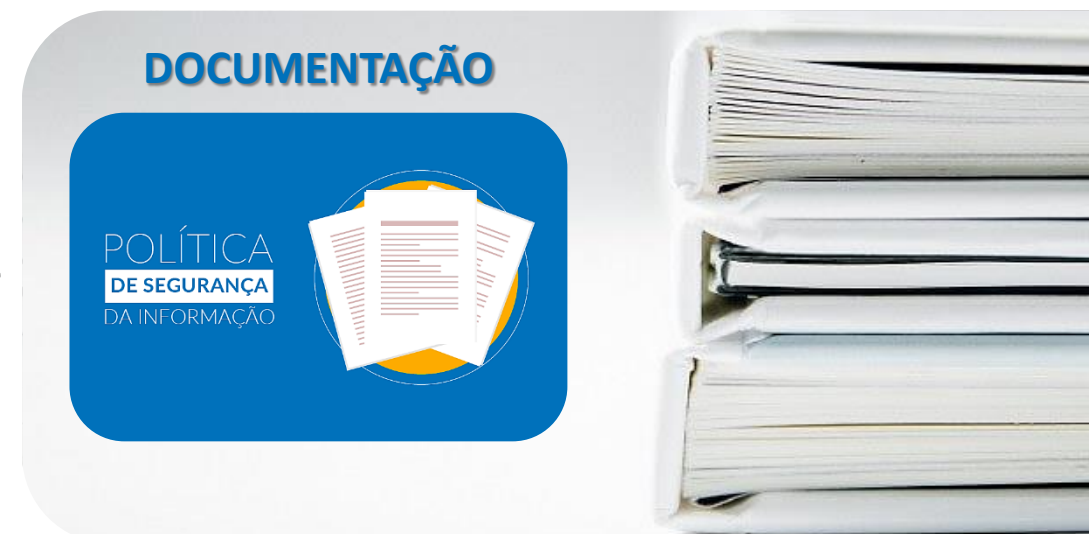


Medidas Técnicas e Organizacionais “TOMs”

• Políticas, Processos e Procedimentos

Para uma melhor compreensão, vamos a algumas definições:

- As **Políticas** estabelecem um conjunto de metas e afirmam “o que deve ser feito” em alinhamento com outros instrumentos estratégicos da organização. É um documento simples e objetivo de maior nível em uma empresa.
- Os **Processos** indicam as atividades, pessoas, ferramentas e regras necessárias para segurança na organização, ao cumprimento de uma determinada Política.
- Os **Procedimentos** descrevem em detalhes como exatamente executar os Processos estabelecidos para atender a uma Política. Nos Procedimentos devem estar descritos os controles, Técnicos e Administrativos, bem como, os indicadores de desempenho considerados na Gestão e Governança da Segurança da Informação conforme o **ISMS** e ou **PIMS** (Sistema de Gerenciamento de Informações de Privacidade).



Principais desafios da Gestão de Políticas de SI



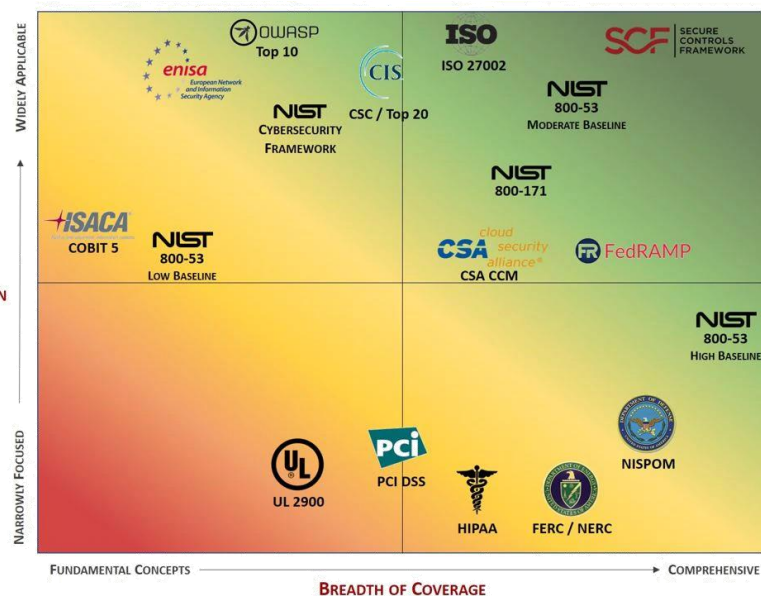
Medidas Técnicas e Organizacionais “TOMs”

• SCF – Security Control Framework

Para atender a necessidade de conhecimentos básicos sobre as melhores práticas para alcançar a segurança da informação, a segurança cibernética e as questões de Privacidade de dados pessoais, incluímos no nosso framework de solução LGPD PrivacidadeOK o Guia Controles e Defesa Cibernética com base SCF.

O Guia aborda a metodologia do framework SCF e entra em alguns detalhes importante.

Recomendamos a leitura atenta e a pesquisa de soluções alinhadas as recomendações.



Medidas Técnicas e Organizacionais “TOMs”

32 Princípios ou áreas de controle para garantir a SI Segurança da Informação, Privacidade de dados pessoais PII e a Cybersecurity

Security & Privacy by Design Principles (S|P)

- 1. Security & Privacy Governance**
Govern a documented, risk-based program that encompasses appropriate security and privacy principles to address all applicable statutory, regulatory and contractual obligations.
- 2. Asset Management**
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.
- 3. Business Continuity & Disaster Recovery**
Maintain the capability to sustain business-critical functions while successfully responding to and recovering from incidents through a well-documented and exercised process.
- 4. Capacity & Performance Planning**
Govern the current and future capacities and performance of technology assets.
- 5. Change Management**
Govern change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.
- 6. Cloud Security**
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal controls.
- 7. Compliance**
Oversee the execution of cybersecurity and privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations.
- 8. Configuration Management**
Govern the establishment and ongoing management of secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.
- 9. Continuous Monitoring**
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.
- 10. Cryptographic Protections**
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive data both at rest and in transit.
- 11. Data Classification & Handling**
Publish and enforce a data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.

The S|P establishes 32 common-sense principles to guide the development and oversight of a modern security and privacy program. The S|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF's comprehensive listing of over 850 cybersecurity and privacy controls is categorized into 32 domains that are mapped to over 130 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the S|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 32 S|P principles are listed below:

- 12. Embedded Technology**
Provide additional scrutiny to the risks associated with embedded technology, based on the potential damages posed when used maliciously.
- 13. Endpoint Security**
Harden endpoint devices to protect against reasonable threats to those devices and the data they store, transmit and process.
- 14. Human Resources Security**
Foster a security and privacy-minded workforce through sound hiring practices and ongoing personnel management.
- 15. Identification & Authentication**
Implement an Identity and Access Management (IAM) capability to ensure the concept of "least privilege" is consistently implemented across all systems, applications and services for individual, group and service accounts.
- 16. Incident Response**
Maintain a practiced incident response capability that trains all users on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with an Incident Response Plan (IRP).
- 17. Assurance**
Utilize an impartial assessment process to validate the existence and functionality of appropriate security and privacy controls, prior to a system, application or service being used in a production environment.
- 18. Maintenance**
Utilize secure practices to maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.
- 19. Mobile Device Management**
Govern mobile devices through a centralized or decentralized model to restrict logical and physical access to the devices, as well as the amount and type of data that can be stored, transmitted or processed.
- 20. Network Security**
Architect a defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.
- 21. Physical & Environmental Security**
Implement layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.
- 22. Privacy**
Implement a privacy program that ensures industry-recognized privacy practices are identified and operationalized throughout the lifecycle of systems, applications and services.



- 23. Project & Resource Management**
Utilize a risk-based approach to prioritize the planning and resourcing of all security and privacy aspects for projects and other initiatives to alleviate foreseeable governance, risk and compliance roadblocks.
- 24. Risk Management**
Govern a risk management capability that ensures risks are consistently identified, assessed, categorized and appropriately remediated.
- 25. Secure Engineering & Architecture**
Implement secure engineering and architecture processes to ensure industry-recognized secure practices are identified and operationalized throughout the lifecycle of systems, applications and services.
- 26. Security Operations**
Assign appropriately-qualified personnel to deliver security and privacy operations that provide reasonable protective, detective and responsive services.
- 27. Security Awareness & Training**
Develop a security and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.
- 28. Technology Development & Acquisition**
Govern the development process for any acquired or developed system, application or service to ensure secure engineering principles are operationalized and functional.
- 29. Third-Party Management**
Implement ongoing third-party risk management practices to actively oversee the supply chain so that only trustworthy third-parties are used.
- 30. Threat Management**
Identify, assess and remediate technology-related threats to assets and business processes, based on a thorough risk analysis to determine the potential risk posed from the threat.
- 31. Vulnerability & Patch Management**
Utilize a risk-based approach to vulnerability and patch management practices that minimizes the attack surface of systems, applications and services.
- 32. Web Security**
Govern all Internet-facing technologies to ensure those systems, applications and services are securely configured and monitored for anomalous activity.

Security & Privacy Capability Maturity Model (SP-CMM)

The SCF developed the Security & Privacy – Capability Maturity Model (SP-CMM) that is based on the maturity levels defined by the Secure Systems Engineering Capability Maturity Model (SSE-CMM). This allows organizations identify and assess against objective expectations for each control, based on the targeted maturity level.

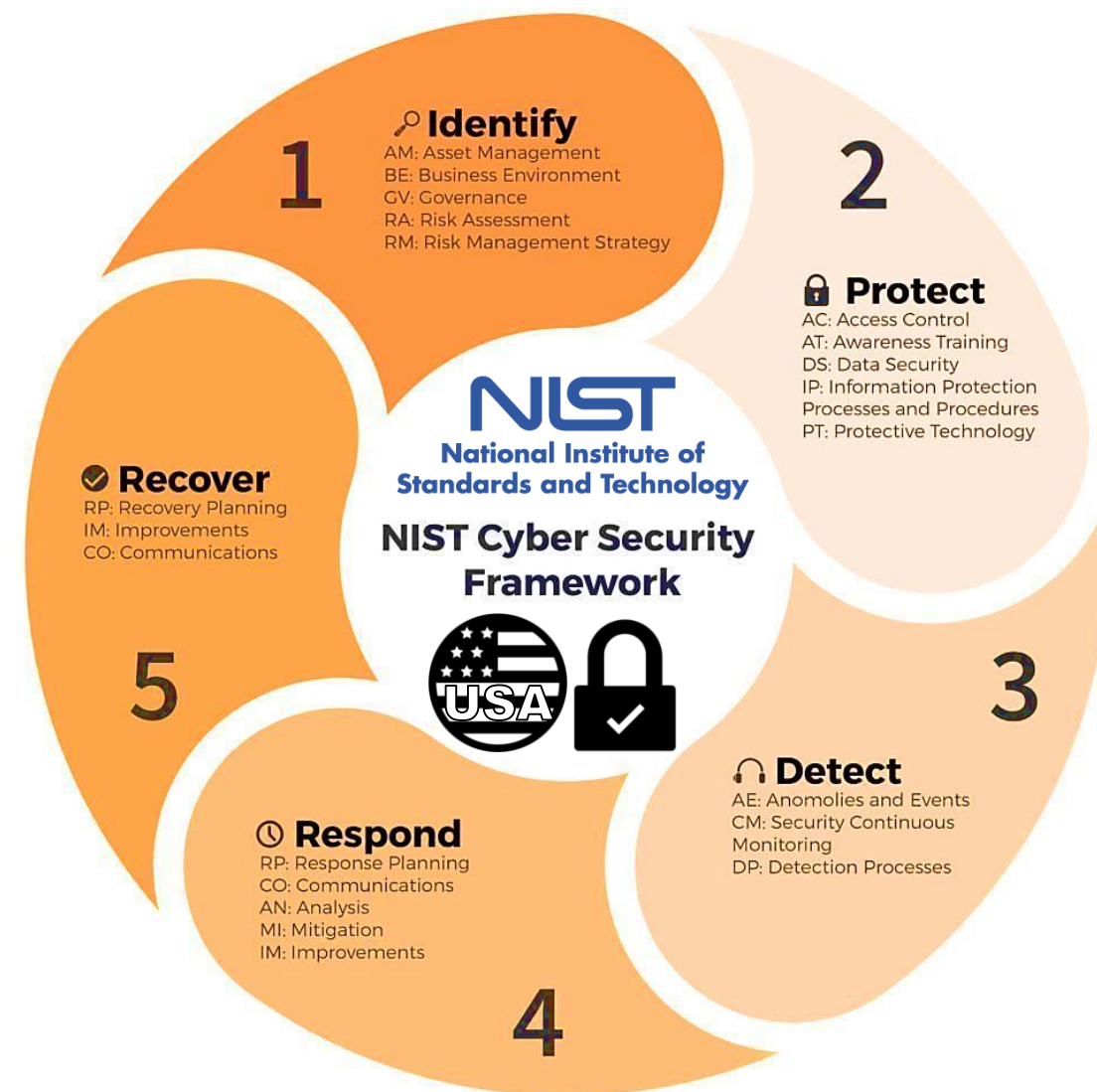
CMM 0 Not Performed NEGLIGENT PRACTICES	CMM 1 Performed Informally AD HOC PRACTICES	CMM 2 Planned & Tracked REQUIREMENTS-DRIVEN PRACTICES	CMM 3 Well Defined ENTERPRISE-WIDE STANDARDIZATION	CMM 4 Quantitatively Controlled METRICS-DRIVEN PRACTICES	CMM 5 Continuously Improving WORLD-CLASS PRACTICES
--	--	--	---	---	---

The objective maturity level definitions from the SSE-CMM allows the SCF's SP-CMM to both establish targets and assess against the maturity of a control that can span multiple statutory, regulatory or contractual requirements, since it is written to be objective and the maturity criteria is focused at the control level.

The SP-CMM is a free resource for businesses and is included as part of the SCE.

NIST Cybersecurity Framework – aderência mundial

- Estrutura bastante consolidada desde 2014 e em evolução.
- Farta documentação.
- Serve de base para outras organizações no mundo, inclusive para o SCF e TeleTrust.
- Possui uma oferta forte de aprendizado on-line indicada no link abaixo.
- Exige um pouco de conhecimento da língua inglesa pois, as figuras e tabelas não podem ser traduzidas automaticamente.



<https://www.nist.gov/cyberframework>

NIST - Privacy Framework

Discutido em 2019 e lançado em 2020.

Aplica todos os conceitos da GDPR.

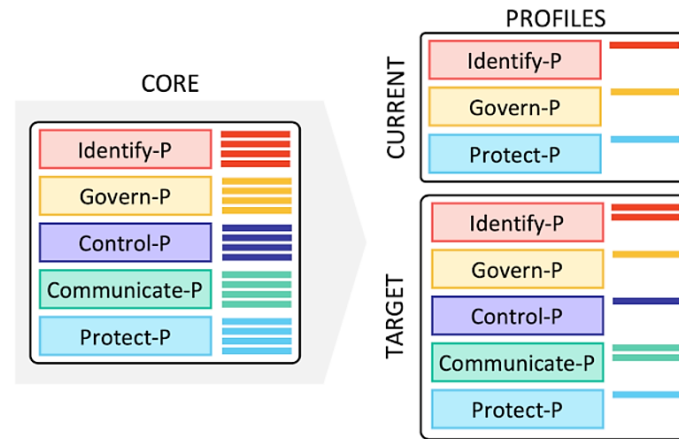


Table 2: Privacy Framework Core

Function	Category	Subcategory
IDENTIFY-P (ID)	Inventory and Mapping (ID.IM-P): Data processing and individuals' interactions with systems, products, or services are understood and inform the management of privacy risk.	ID.IM-P1: Systems/products/services that process data, or with which individuals are interacting, are inventoried.
		ID.IM-P2: The owners or operators of systems/products/services that process data, or with which individuals are interacting, are identified.
		ID.IM-P3: Data elements that systems/products/services are processing are inventoried.
		ID.IM-P4: Data actions are identified.
		ID.IM-P5: The data processing environment is identified (e.g., internal, cloud).
		ID.IM-P6: Data processing is mapped, illustrating the processing of data elements by system components and their owner/operators, and interactions of individuals and organizations with the systems/products/services.
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	ID.BE-P1: The organization's role in the supply chain is identified and communicated.
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.
		ID.BE-P3: Systems/products/services that process data, or with which individuals are interacting, are identified.
		ID.BE-P4: Data actions are identified.

<https://www.nist.gov/system/files/documents/2021/01/IST.Privacy.Framework.V1.Portuguese.Translation.pdf>

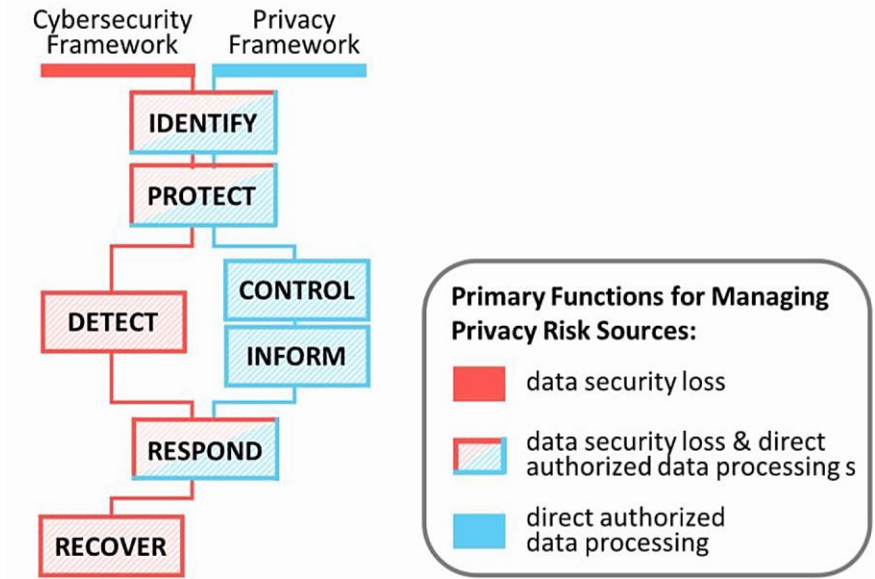


Figure 2: Cybersecurity Framework and Privacy Framework Functions Relationship



Figure 4: Notional Information and Decision Flows within an Organization

E o futuro? Como será 2022 e a frente?

- Leia o importante artigo de DAN LOHRMANN publicado em 20/12/2020.

Importante resumo de todas as melhores publicações de tendências em Cybersecurity para 2021 – com links para baixar mais de 30 relatórios das maiores empresas mundiais da área.



Direitos Autorais

Esta é uma publicação livre, com conteúdo obtido de fontes abertas, ofertada gratuitamente para os alunos dos cursos básicos de Segurança e Proteção de Dados Pessoais.

O Licenciamento desta compilação de dados é acadêmica e fundamentada no padrão **Creative Commons** - <https://br.creativecommons.net/licencas/>



BY



NC



SA

Atribuição - Não Comercial - Compartilha Igual

CC BY-NC-SA

Esta licença permite que outros remixem, adaptem e criem a partir do seu trabalho para fins não comerciais, desde que atribuam a você o devido crédito e que licenciem as novas criações sob termos idênticos.

CRÉDITOS AOS PROFISSIONAIS DO WEBSITE PRIVACIDADEOK.

Todas as figuras/imagens foram obtidas de fontes que alegam ser gratuitas inclusive para uso comercial – a maioria das figuras foram ajustadas e readequadas as necessidades de atendimento didático, sem uso comercial. Não houve preocupação com revisão ortográfica e edição profissional.

Concluimos este Curso Super Básico.



Agora vamos fazer uma avaliação de absorção de conhecimentos sobre os temas apresentados. A avaliação é individual e faz parte do processo de registro de evidências sobre as ações da organização, no atendimento as recomendações da Lei nacional nº 13709:2018 – Lei Geral de Proteção de Dados.

O arquivo enviado com as questões está em MS-Word, aberto, para a inclusão de respostas. Não esqueça de colocar o seu nome, nome da empresa e a data de realização do teste. Você tem 24 horas para retornar as respostas.

.

CONCLUSÃO



Avaliação de Reação
Queremos saber sua opinião.

