



Palestra Segurança da Informação

HUDSON BASTOS DE SOUZA

GERENTE DE SEGURANÇA DA INFORMAÇÃO

Segurança da Informação

- Hoje em dia a informação é o bem mais valioso de uma empresa/cliente.
- Quanto vale os dados da sua instituição?*



Segurança da Informação

“A segurança da informação é um conjunto de medidas que se constituem basicamente de **controles** e **política de segurança**, tendo como objetivo a proteção das informações dos clientes e da empresa (**ativos/bens**), controlando o **risco** de vazamento ou alteração por pessoas não autorizadas.”

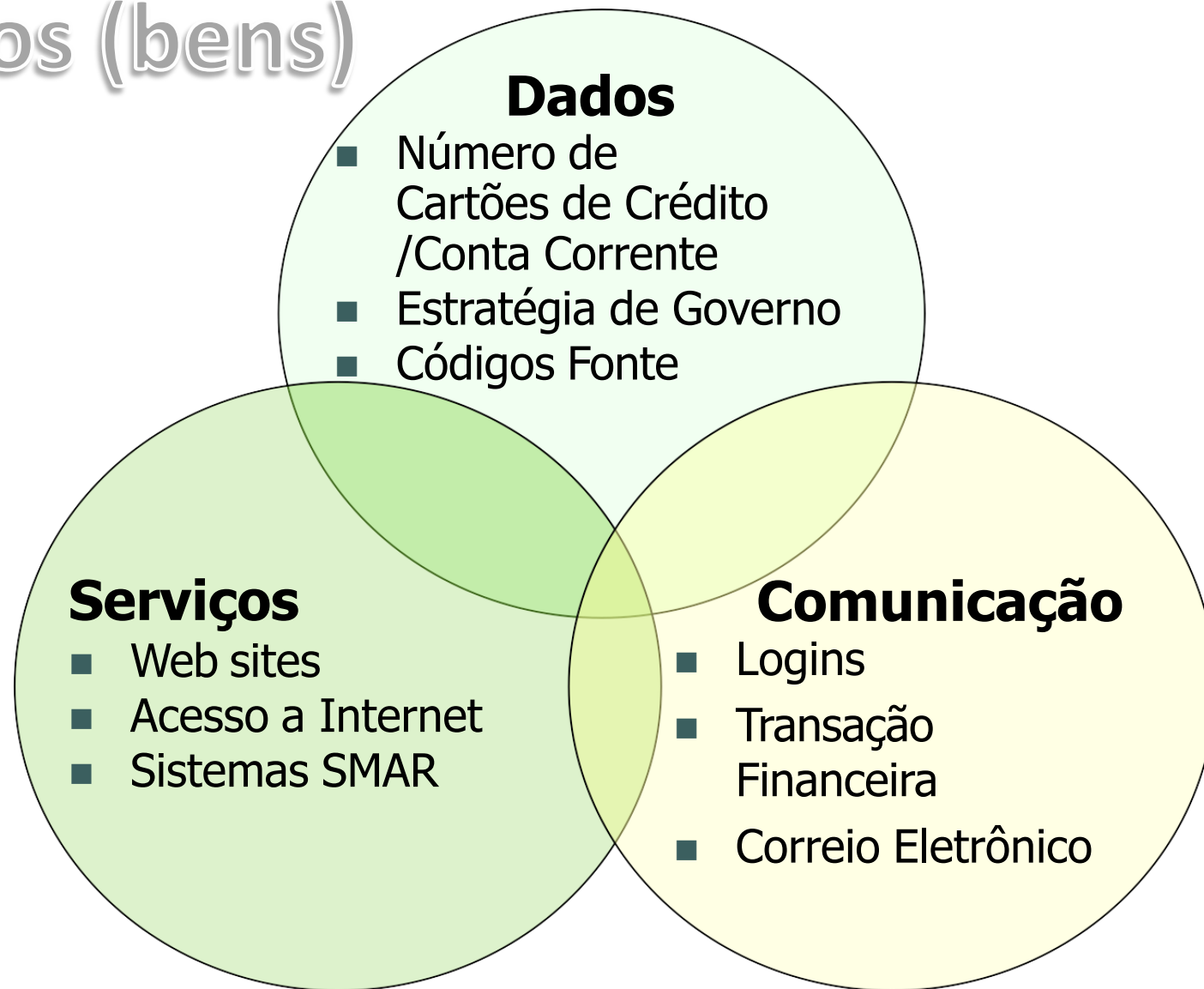


Políticas de Segurança da Informação

- Trata-se um conjunto de diretrizes (**normas**) que definem formalmente as regras e os direitos dos usuários, visando à proteção adequada dos **ativos** da informação.



Ativos (bens)



Definições

- **Ameaça**

- Evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um **recurso**;

- **Vulnerabilidade**

- Vulnerabilidade refere-se à "qualidade ou estado de ser exposto à possibilidade de ser atacado ou prejudicado, física ou digitalmente". Uma janela de vulnerabilidade é um período de tempo no qual as medidas defensivas são diminuídas, comprometidas ou ausentes;

Definições

- **Risco**
 - A **probabilidade** que uma ameaça explore uma determinada vulnerabilidade de um recurso

Princípios da Política de Segurança

Pilares da Segurança da Informação

DISPONIBILIDADE

INTEGRIDADE

CONFIDENCIALIDADE

Princípios da Política de Segurança

- Disponibilidade

- Possibilidade de **acesso à informação** por parte daqueles que a necessitam para o desenvolvimento de suas atividades

Integridade

- Condição na qual a informação ou os recursos da informação são **protegidos contra modificações não autorizadas**

- Confidencialidade

- Propriedade de certas informações que **não podem ser disponibilizadas ou divulgadas sem autorização prévia** do seu dono

Ameaças à Política de Segurança

- **Integridade**
 - Ameaças de ambiente (fogo, enchente...), erros humanos, fraudes, erro de processamento
- **Indisponibilidade**
 - ▮ Falhas de sistemas
- **Divulgação da informação**
 - Divulgação premeditada ou acidental de informação confidencial

História da Segurança da Informação

História da Segurança da Informação

- Referência
 - Os 10 Mandamentos de Deus

Moisés recebe informações sagradas de Deus

- Ref. Êxodo.34, Bíblia Sagrada*



História da Segurança da Informação

Referência

- Os 10 Mandamentos de Deus

Moisés disponibiliza informações sagradas de Deus a quem direito



História da Segurança da Informação

- **Evolução**
 - Melhorias de Segurança

Criação da Arca da aliança



História da Segurança da Informação

Evolução

- Melhorias de Segurança

Criação Tabernáculo

- Controles de acesso
- Políticas de segurança
- Dispositivos de segurança

Ameaças

- Tentativa invasão
- Roubo



Mecanismos de Segurança

- Controle físico
 - Barreiras que limitam o contato ou acesso direto à informação ou a estrutura que a suporta
 - ▮ Porta, paredes, trancas, blindagem, guardas ...
- Controle lógico
 - Barreiras que limita o acesso à informação em ambiente eletrônico
 - ▮ Mecanismos de criptografia
 - ▮ **Modificar a informação** de forma que seja impossível que pessoas não autorizadas a decodifiquem
 - ▮ Mecanismos de controle de acesso
 - ▮ Senhas, Firewall, Sistemas biométricos, duplo fator de autenticação;

Mecanismos de Segurança

- Geram
- Transtornos aos usuários

- Barreiras que limitam o contato ou acesso direto à informação ou a estrutura que a suporta
- Porta, paredes, trancas, blindagem, guardas ...

Malware

- Malware é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, celulares, ou a uma rede de computadores.
- Malware, portanto, é uma definição abrangente que serve para categorizar desde aplicativos espiões, os [spywares](#) usados para monitorar seu comportamento e roubar seus dados, a [ransomwares](#), que capturam o sistema, criptografam seus arquivos e exigem resgate para que você recupere acesso aos seus dados.

Tipos de Malwares

- São programas criados para causar danos ao computador:
 - Apagando dados
 - Capturando informações
 - Alterando o funcionamento normal da máquina
 - Sequestrar e Criptografar dados (pedir resgate)
- **Worm**: Tem o objetivo principal de se espalhar o máximo possível, não causando grandes danos

Tipos de Malwares

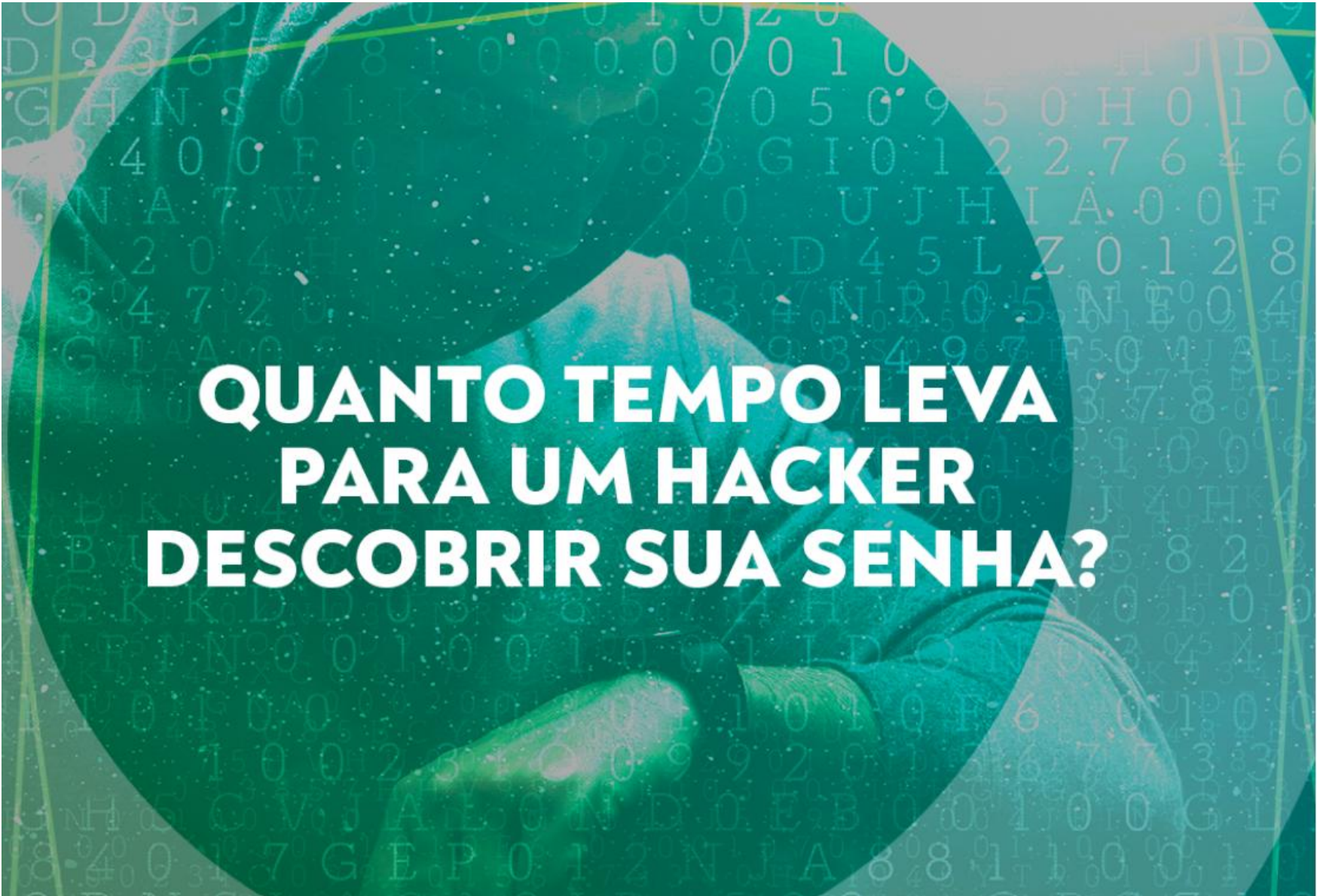
- **Spyware**
 - Utilizado para espionar a atividade do computador afetado e capturar informações
 - Geralmente são embutidos em programas freeware ou shareware
- **Keylogger**
 - Tem a função de capturar tudo que é digitado pelo usuário do computador atacado

Tipos de Malwares

Ransomware

É um malware que criptografa arquivos importantes no armazenamento local e de rede e exige um resgate para descriptografar os arquivos.

Os atacantes desenvolvem esse malware para ganhar dinheiro com extorsão digital.



QUANTO TEMPO LEVA PARA UM HACKER DESCOBRIR SUA SENHA?

Segundo levantamento da Hive Systems, empresa norte-americana de cibersegurança, o tempo de descoberta **dependerá diretamente do número de caracteres, uso de letras, números e símbolos.**

Número de Caracteres	Apenas Números	Letras Minúsculas	Minúsculas e Maiúsculas	Numéros, Letras Minúsculas e Maiúsculas	Numéros, Letras Minúsculas, Maiúsculas e Símbolos
4	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
5	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
6	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente	Instantaneamente
7	Instantaneamente	Instantaneamente	2 segundos	7 segundos	31 segundos
8	Instantaneamente	Instantaneamente	2 minutos	7 minutos	39 segundos
9	Instantaneamente	10 segundos	1 hora	7 horas	2 dias
10	Instantaneamente	4 minutos	3 dias	3 semanas	5 meses
11	Instantaneamente	2 horas	5 meses	3 anos	34 anos
12	2 segundos	2 dias	24 anos	200 anos	3 mil anos
13	19 segundos	2 meses	1 mil anos	12 mil anos	202 mil anos
14	3 minutos	4 anos	64 mil anos	750 mil anos	16 milhões de anos
15	32 minutos	100 anos	3 milhões de anos	46 milhões de anos	1 bilhão de anos
16	5 horas	3 mil anos	173 milhões de anos	3 bilhões de anos	92 bilhões de anos
17	2 dias	69 anos	9 milhões de anos	179 bilhões de anos	7 trilhões de anos
18	3 semanas	2 milhões de anos	467 bilhões de anos	11 trilhões de anos	438 trilhões de anos

Exemplos Recentes

Após queda do site

Prefeitura de Vitória registra ocorrência sobre possível ataque hacker

Site da administração municipal ficou fora do ar por quase uma semana. Um boletim de ocorrência foi registrado junto à Polícia Civil, que vai investigar o caso

Lais Magesky | Repórter

lmagesky@redegazeta.com.br

Vitória

Publicado em 03/11/2021 às 21h02



Não é a primeira vez

Há quase 3 anos, em 8 de novembro de 2020, o sistema de dados da PMV também foi alvo de invasão. O site ficou quatro dias fora do ar e voltou com os serviços gradativamente. O primeiro a voltar foi o Cerco Inteligente de Segurança. Dias antes, o Superior Tribunal de Justiça (STJ) também tinha sido invadido, o que impossibilitou julgamentos de processos.

Segurança no Ambiente PMC/IPC

- Equipe de Segurança da Informação
- Decretos/ normativas
- Leis
- Infraestrutura de Segurança de Rede /Data Center
- Dispositivos de segurança física e Lógica
- Investimentos

Equipe de Segurança da Informação

GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO



Hudson Bastos
Gerente de Segurança
da Informação



Eliakim Barros
Coordenador de
Segurança
Cibernética



**Luciano
Resende**
Coordenador de
Normas e Riscos



**Rodiney
Rezende**
Técnico MNM I -
Informática

Equipe de Segurança da Informação

Atribuições

- Fazer gestão de toda a segurança da informação do município
- Elaboração de políticas, normas e procedimentos de segurança da informação
- Monitoramento logs
- Suportar todos os ativos e softwares de segurança (150)
- Outras

Equipe de Segurança da Informação

Surface Web

A Surface Web existe desde a invenção do primeiro navegador à internet nos anos 1990, como parte da World Wide Web.

Deep Web – Definição

Em poucas palavras, a Deep web é a seção da web que não está indexada e não pode ser encontrada pelas ferramentas de buscas convencionais.

Dark Web

Diferentemente da Deep Web, além de suas páginas não serem indexadas em sites de busca, a Dark Web só pode ser acessada através de softwares específicos.



Equipe de Segurança da Informação

graylog Search Streams Alerts Dashboards Enterprise System 1 43 in 43 out  

>

i

+

🔊

X₁

SITES MAIS BLOQUEADOS 24h

web_site	client_user	count()
https://watson.telemetry.microsoft.com/	172.16.126.11	73016
	172.16.55.13	33072
	guilherme.ribeiro@cariacica.intra.corp	29876
	172.16.166.150	27902
	rosangela.siqueira@cariacica.intra.corp	27898
	172.16.179.143	23184
	alair.sales@cariacica.intra.corp	22436
	marcia.freitas@cariacica.intra.corp	21354
	jessica.santos@cariacica.intra.corp	21334
	carlos.caldeira@cariacica.intra.corp	20164
	172.16.154.184	19914
	172.16.123.11	19652
	rodrigo.santos@cariacica.intra.corp	19550

SITES MAIS ACESSADOS 24h

web_site	client_user	count()
https://www.google.com	ailton.ganho@cariacica.intra.corp	60818
	gabriel.ribeiro@cariacica.intra.corp	19934
	darsones.bernardino@cariacica.intra.corp	15068
	francisco.subtil@cariacica.intra.corp	13756
	virginia.ramos@cariacica.intra.corp	11686
	marcelly.moraes@cariacica.intra.corp	10048
	damarys.freitas@cariacica.intra.corp	9508
	larissa.valentim@cariacica.intra.corp	9104
	leticia.n.rodrigues@cariacica.intra.corp	9082
	rodrigo.santos@cariacica.intra.corp	8394
	saula.falqueto@cariacica.intra.corp	8220
	thalita.teixeira@cariacica.intra.corp	7836
	afonso.jesus@cariacica.intra.corp	6956

Equipe de Segurança da Informação

☰ Monitoramento Portas

dport	rule_action	count()
443	deny	9529408
	allow	9370178
-	deny	2082678
80	allow	1026572
123	allow	157912
	deny	26462
1250	deny	112580
	allow	30846
1251	deny	108200
	allow	29922
1252	deny	108176
	allow	29778
5222	allow	115512

Equipe de Segurança da Informação

← → ↻ 🔒 bttng.apura.com.br/wires/53619

 Cadastro Nacional...  Pessoa Física (Cidad...  Certidão eletrônica...  Certidões Criminais...  Modelo de efetiva...  Central de Servi



Prezados(as),

Encontramos 84 credenciais (login e senha) com URLs relacionadas com o domínio cariacica.es.gov.br

Screenshot:

cariacica.es.gov.br

 Pesquisar  Download

Filtros 1.428 resultados encontrados Ordenar por ▼

username: 213-7192-2764- password:  mostrar senha

application:  google chrome

url: https://conta.cariacica.es.gov.br/auth/realms/pmcariacica/login-actions...

08/05/2023, 10:25:35

Robots Intel  Logs de Malwares

username: 703404217870200 password:  mostrar senha

application:  google chrome

url: https://conta.cariacica.es.gov.br/auth/realms/pmcariacica/login-actions...

08/05/2023, 10:25:35

Robots Intel  Logs de Malwares

username: 23.793.494/0001-04 password:  mostrar senha

application:  google chrome

url: http://servicos.cariacica.es.gov.br:8080/tbw/loginSSContribuinte.jsp

07/05/2023, 13:47:36

Robots Intel  Logs de Malwares

username: 05555537794 password:  mostrar senha

application:  google chrome

url: https://sistemas.cariacica.es.gov.br/portalcidadao/

06/05/2023, 03:51:37

Robots Intel  Logs de Malwares

Decretos e Normativa

➤ Termo de Cooperação Técnica N° 028/2021

<https://transparencia.cariacica.es.gov.br/MostraArquivo.ashx?AnexoConveniold=1486>

➤ Decreto N° 157 de 2017 Institui as Políticas de Segurança da Informação no Âmbito da Administração Municipal

<https://www.ipccariacica.es.gov.br/uploads/filemanager/Decreto%20n%C2%BA%20157-2017.pdf>

➤ PSI – IPC

➤ Isso 27001 e 27002 – ISO/IEC 27001 e 27002 é um padrão para sistema de gestão da segurança da informação publicado em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commission.

Leis

➤ LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 (LGPD)

Lei Geral de Proteção de Dados

➤ LEI Nº 12.965, DE 23 DE ABRIL DE 2014

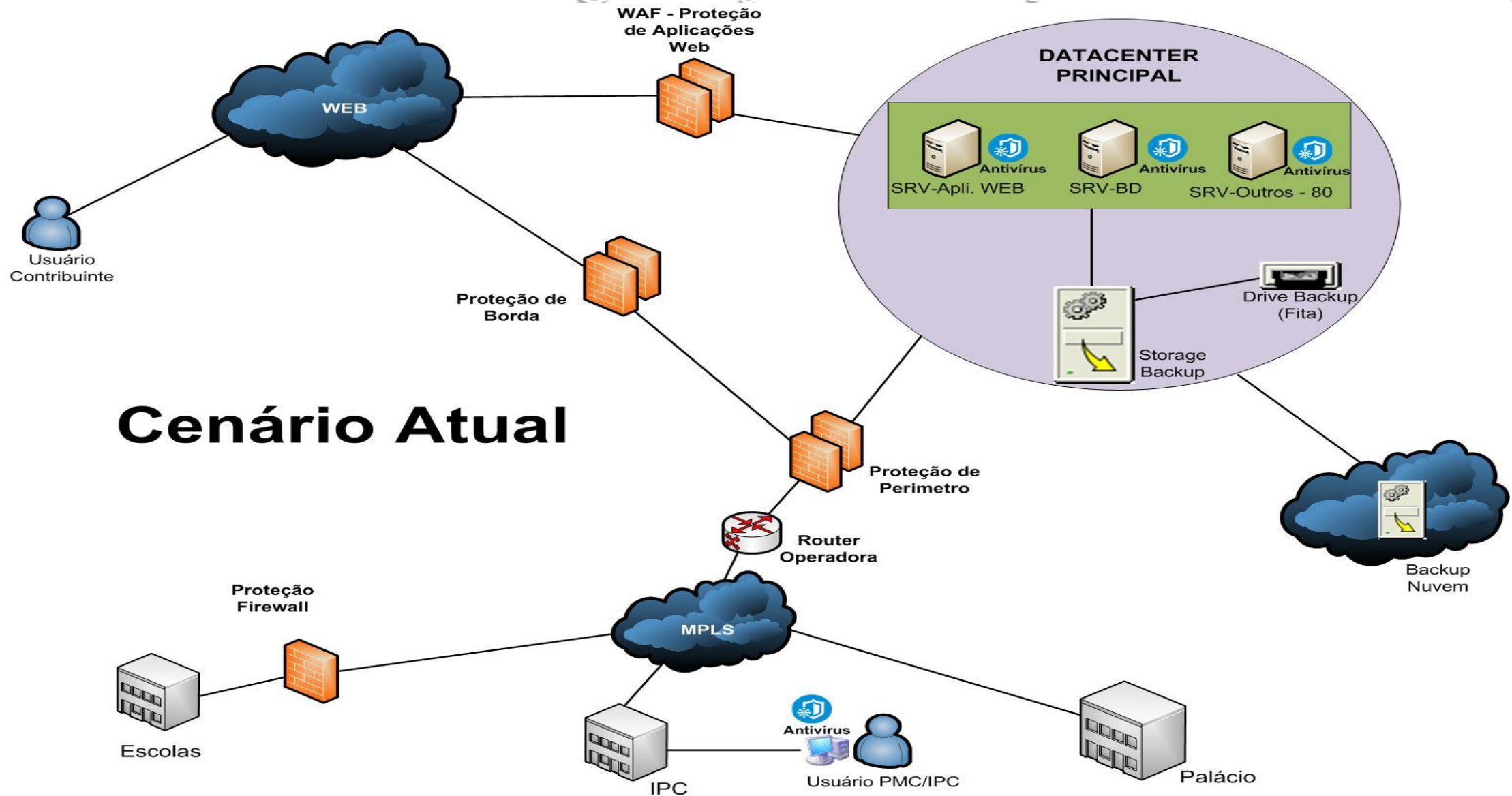
Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet)

➤ LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

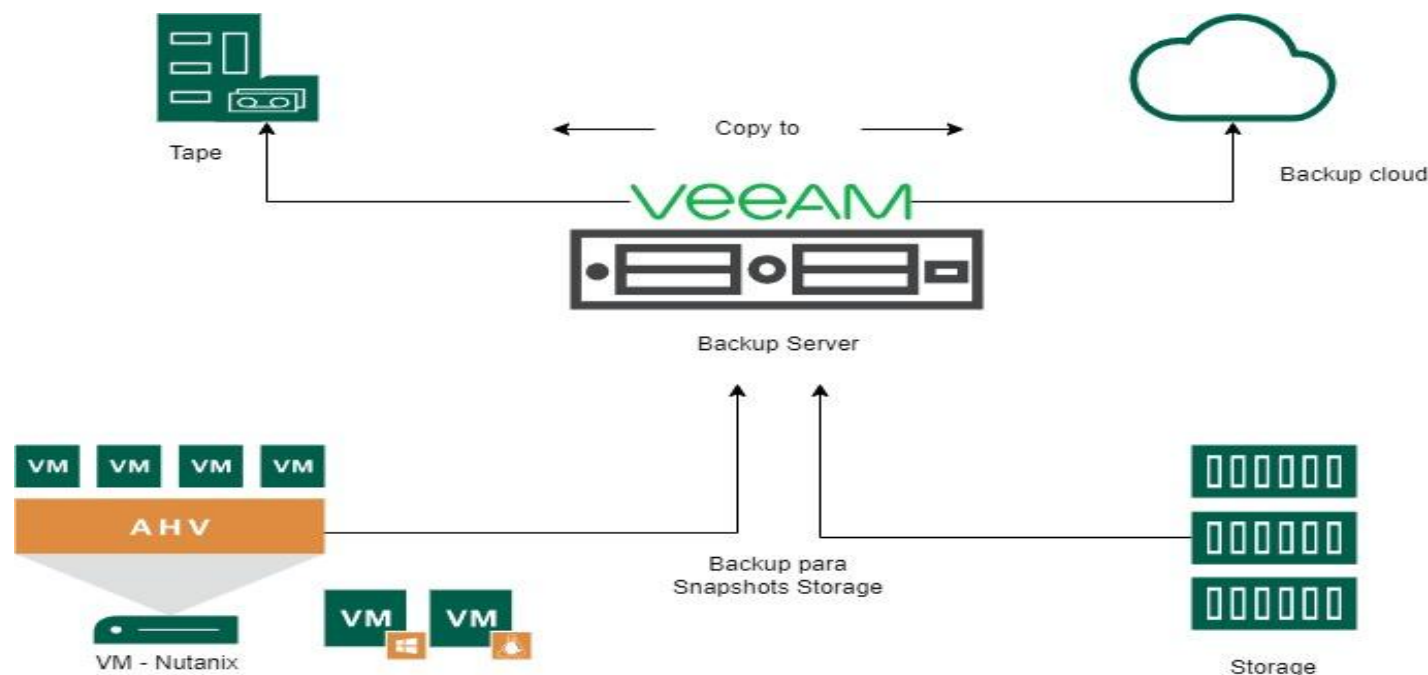
Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. (Lei Carolina Dieckmann).

➤ LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. (Lei de Acesso a Informação)

Infraestrutura de Segurança de Rede/Data Center



Investimentos em Segurança da Informação

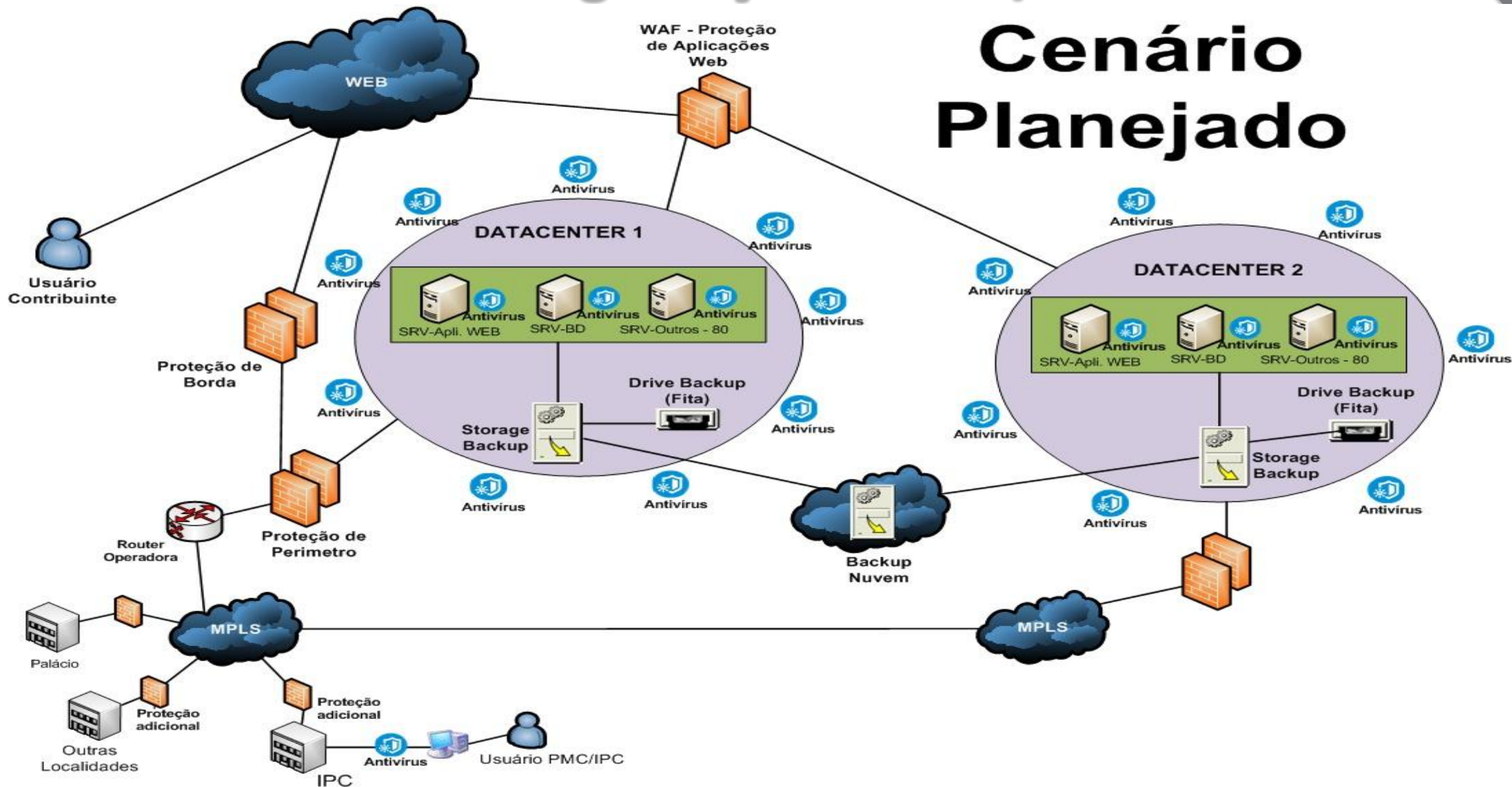


Estrutura de Backup PMC

Investimentos Previstos em Segurança da Informação

Infraestrutura de Segurança de Rede/Data Center

Cenário Planejado



Treinamentos e dicas de Segurança da Informação



Português - Brasil (pt_br) ▼

Você ainda não se identificou. (Acessar)



PREFEITURA DE
CARIACICA

Cursos disponíveis

Segurança da Informação - Cursos e Dicas



Página dedicada aos cursos, dicas e informativos referentes à Segurança da Informação, onde o usuário pode - e deve! - aprender a como proteger suas informações pessoais e profissionais de forma simples e objetiva.

Acesse: <https://capacitacao.cariacica.es.gov.br>



**PREFEITURA DE
CARIACICA**

PREFEITURA MUNICIPAL DE CARIACICA

AGRADECEMOS A SUA PARTICIPAÇÃO!

SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - 2023