CERTIFIED CYBERSECURITY

Notas de estudo

DANIEL DONDA

https://danieldonda.com

SUMÁRIO

NOTAS DE ESTUDO CERTIFIED CYBERSECURITY

Uma excelente oportunidade para todos os profissionais de cibersegurança que buscam uma certificação de ponto de partida para iniciar a carreira obtendo uma certificação e aprendendo conceitos importantes para o mercado de trabalho.

Certified in Cybersecurity℠

A certificação em segurança cibernética é oferecida pela (ISC)² organização profissional líder em segurança cibernética do mundo, conhecida pela famosa certificação CISSP®. Esse é um compromisso de ajudar a fechar a lacuna da força de trabalho, uma iniciativa global chamada, **One Million Certified in Cybersecurity**,

Você não precisa de experiência – apenas a paixão e o desejo de entrar em uma área que abre oportunidades ilimitadas em todo o mundo.

Por isso a (ISC)² está oferecendo treinamento e exames on-line gratuitos para o primeiro milhão de pessoas.

Sobre o exame

O exame consiste em 100 questões de múltipla escolha. Você terá duas horas para concluir seu exame. Uma pontuação de aprovação é de 700 em 1000 pontos.

O exame é somente em inglês e dividido em 5 domínios.

- **Domínio 1 – Security Principles** – Conheça os conceitos de segurança da garantia da informação, o processo de gestão de riscos, os controles de segurança, o Código de Ética (ISC)² e os processos de governança. 26% do exame.
- **Domínio 2 – Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts** Mostre que você entende os três conceitos-chave. 10% do exame.
- **Domínio 3 – Access Controls Concepts** – Descubra o que você precisa saber sobre acesso físico e controles de acesso lógico. 22% do exame.

- **Domínio 4 – Network Security** – Mergulhe em redes de computadores, ameaças e ataques de rede e infraestrutura de segurança de rede. 24% do exame.
- **Domínio 5 – Security Operations –** Saiba tudo sobre segurança de dados, proteção do sistema, políticas de segurança de melhores práticas e treinamento de conscientização.18% do exame.

Existem treinamentos pagos online e com instrutores, porém é possível ter acesso ao treinamento gratuito oferecido pela (ISC)².

Como se cadastrar?

- Criar uma conta no portal da (ISC)2 (**https://my.isc2.org/s/login/SelfRegister**)
- **Preencher o formulário** para se tornar um candidato ISC elegível.
- **Inscrever-se no treinamento** gratuito
- **Copiar o código promocional** desta página
- Registrar-se no portal da **PearsonVue** e realizar a compra da prova de certificação utilizando o voucher

Referencia

- **https://blog.isc2.org/isc2_blog/2022/07/isc2-1-million-certified-in-cybersecurity.html**
- **https://www.isc2.org/Certifications/CC**

DOMÍNIO 1 – SECURITY PRINCIPLES

Confidentiality, Integrity and Availability (CIA)

CIA – A tríade **Confidentiality, Integrity and Availability (CIA)** é o fundamento básico de segurança da informação.

Confidencialidade – As informações só devem ser acessadas por pessoas autorizadas.

Integridade – A integridade dos dados é a garantia de que os dados não foram alterados de forma não autorizada.

Disponibilidade – O conceito central de disponibilidade é que os dados sejam acessíveis a usuários autorizados quando e onde forem necessários e na forma e formato exigidos. Isso não significa que os dados ou sistemas estejam disponíveis 100% do tempo.

Authentication

Existem basicamente três métodos comuns de autenticação:

- Algo que você sabe: senhas
- Algo que você tem: Tokens, cartões de memória, cartões inteligentes
- Algo que você é: Biometria

[IAAA]

- **Identificação**: O usuário deve ser identificado exclusivamente
- **Autenticação**: validação da declaração de identidade de uma entidade

- **Autorização**: Confirma se uma entidade autenticada possui os privilégios e permissões necessários.
- **Auditoria**: Qualquer atividade no aplicativo/sistema deve ser auditada

Non-repudiation – Não-repúdio é um termo legal e é definido como a proteção contra um indivíduo que nega falsamente ter realizado uma determinada ação. Um usuário não pode negar ter realizado uma determinada ação.

Least Privilege – Privilégio mínimo (acesso mínimo necessário) – Nem mais, nem menos

Need to know – Se você não precisa saber – Você não precisa acessar

Risk Management:

- Um ativo é algo que precisa de proteção;
- Uma vulnerabilidade é uma lacuna ou fraqueza;
- Uma ameaça é algo ou alguém que visa explorar uma vulnerabilidade.

Tratamentos de risco

- ***Avoidance*** – Evitar o risco é a decisão de tentar eliminar o risco completamente.
- ***Acceptance*** – Aceitar o risco é não tomar nenhuma ação
- ***Transfer*** – Transferência de risco é a prática de passar o risco para outra parte

A **mitigação de riscos** (***Mitigation***) inclui a tomada de ações para prevenir ou reduzir a possibilidade de um evento de risco ou seu impacto. A mitigação pode envolver medidas de remediação ou **controles**.

Security Controls

- ***Physical controls*** – Exemplo: Cães, cercas, guardas de segurança. Luzes
- ***Technical controls*** – Exemplo: Firewall, IPS, MFA, antivírus, IDS
- ***Administrative controls*** – Exemplo: Políticas de contratação e rescisão, separação de funções, classificação de dados.
    - *Os controles de segurança existem para reduzir ou mitigar o risco para esses ativos.*

Security Policies, Standards, Procedures, and Guidelines

- ***Security Policy***, a política de segurança é um documento obrigatório que define o escopo de segurança necessário para a organização.

- ***Standards*** – Padrões, requisitos obrigatórios – Hardware e Software (ISO,NIST,IETF,IEEE)
- ***Baseline*** – Linha de base – Requisito mínimo de segurança
- ***Guidelines*** – Diretrizes como os Padrões e Linhas de Base devem ser implementados
- ***Procedures*** – Procedimentos, documento passo a passo (conjunto de tarefas).
- ***Regulations*** – Regulamentações ou leis a serem seguidas (GDPR, LGPD)

Code of Ethics Canons

A estrita adesão a este Código é uma condição de certificação.

- **PROTECT SOCIETY** – **PROTEGER A SOCIEDADE**, o bem comum, a confiança e a confiança pública necessárias e a infraestrutura.
- **ACT HONORABLY** – **AGIR COM HONRA** honestidade, justiça, responsabilidade e legalidade.
- **PROVIDE DILIGENT** – **OFERECER** um serviço diligente e competente aos diretores.
- **ADVANCE AND PROTECT THE PROFESSION**. **AVANÇAR E PROTEGER A PROFISSÃO**.

Para lembrar na hora do exame as iniciais do código de ética iniciam com as letras ***P.A.P.A***

DOMÍNIO 2 – Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts

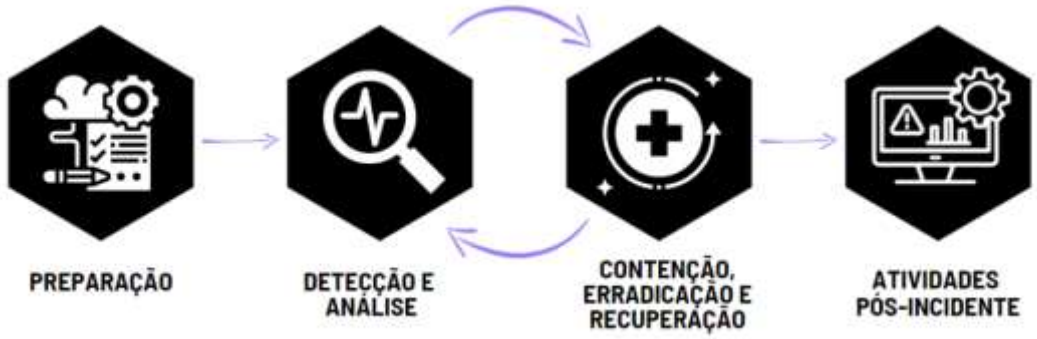
Terminologia de incidentes

- ***Breach*** – Uma violação**.** A perda de controle, comprometimento, divulgação não autorizada, aquisição não autorizada.
- ***Event*** – Um evento é qualquer ocorrência observável em uma rede ou sistema. NIST SP 800-61 Rev 2
- ***Exploit*** – Uma forma de "explorar" uma determinada vulnerabilidade através de um código seja um software ou um código.
- ***Incidente*** – Um evento que, real ou potencialmente, coloque em risco a confidencialidade, integridade ou disponibilidade
- ***Intrusion*** – Quando um intruso obtém, ou tenta obter, acesso a um sistema ou recurso do sistema sem autorização.
- ***Threat*** – Ameaça é qualquer condição que possa causar dano, perda, ou comprometimento de um ativo. Exemplo: Desastres naturais,ataques cibernéticos, violação da integridade dos dados, vazamento de dados confidenciais, Malware, Insiders.

- ***Vulnerability*** – Vulnerabilidade é qualquer falha no design do sistema, implementação, código de software ou falta de mecanismos preventivos Exemplo: Erros de software, software mal configurado, dispositivos de rede mal configurados, segurança física inadequada.
- **Zero Day** – Uma vulnerabilidade de sistema desconhecida com potencial de exploração.

Componentes do Plano de Resposta a Incidentes

Baseado no ***NIST Computer Security Incident Handling Lifecycle.*** NIST SP 800-61 Rev. 2



Equipe de resposta a incidentes

Essa equipe é conhecida como ***computer security incident response teams (CSIRTs)*** e deve saber:

- Dimensionar os danos causados pelo incidente;
- Identificar se houve vazamento de informações;
- Restaurar a segurança;
- Prevenir a recorrência do incidente.

BCP Business Continuity Plan (BCP)

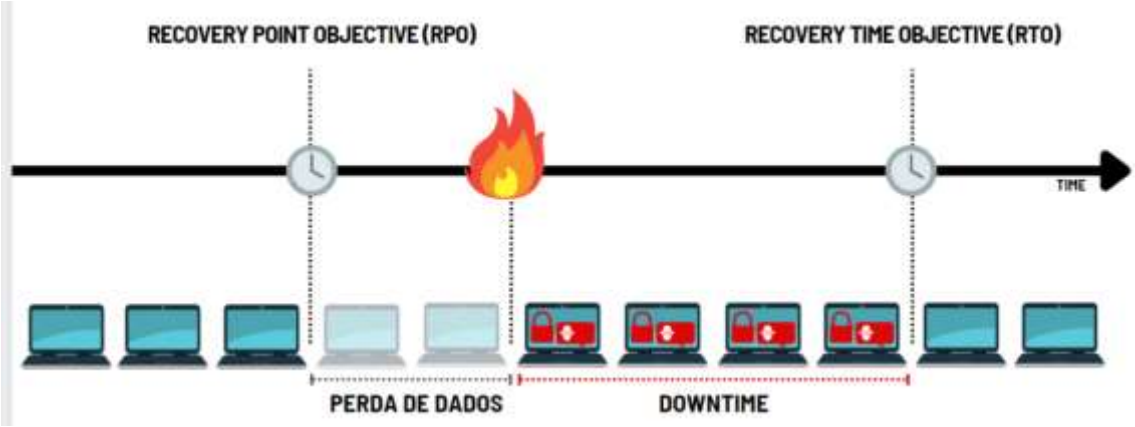
O **Business Continuity Plan (BCP)** realiza o **Business Impact Assessment (BIA)** e, em seguida, implementa **controles** para manter os negócios funcionando durante circunstâncias adversas.

Business Impact Assessment (BIA) – É processo para avaliar os efeitos de uma interrupção nas operações críticas de negócios.

O **BCP** deve ser testado sempre e principalmente quando houver mudanças no ambiente de negócio.

Disaster recovery plan (DRP)

- **RPO** – **Recovery Point Objective** (Máximo que você pode perder de dados)
- **RTO – Recovery Time Objective** (Tempo determinado de recuperação)
- **MTD – Maximum Tolerable Downtime** (Tempo máximo total que o processo pode ficar parado)



DOMÍNIO 3 – Access Controls Concepts

Um controle de segurança é uma **salvaguarda** ou **contramedida** usada para manter a **confidencialidade**, a **integridade** e a **disponibilidade**. Em controle de acesso procuramos limitar o acesso que ***subjects*** possuem em objetos (***objects***) através de regras (***rules***)

- **Subject** – *Ativo* – Exemplos: usuário. processo, programa, computador, etc.
- **Object** – *Passivo* – Exemplos: Computador, servidores, pasta, impressora, arquivos, etc.
- **Rules** – Permite acesso ou nega acesso a um objeto. Pode comparar uma lista de atributos, etc. Exemplo: Firewall, Permissões de pasta/arquivos.

Defense in Depth – O princípio de defesa em profundidade requer o uso de **controles** sobrepostos para atender ao mesmo objetivo.

Least privilege é um princípio de segurança que diz que os usuários devem ter o conjunto mínimo de permissões necessárias para desempenhar suas funções de trabalho.

Separation of duties (SoD), separação de tarefas exige que nenhum indivíduo tenha a capacidade de executar duas funções separadas que, quando combinadas, podem minar a segurança.

Two-person control, o controle de duas pessoas requer a presença de dois indivíduos para realizar uma única função sensível.

Physical Security Controls

- **Crime Prevention Through Environmental Design (CPTED)** -Uso do design do ambiente para prevenir crimes como luz natural, cercas baixas, caminho especifico de caminhada, obstáculos.
- **Monitoring** – Sistemas de câmeras e monitoramento.
- **Biometria** -A biometria usa características exclusivas do indivíduo para liberar acesso como a iris, digital (fingerprint), etc.
- **Controles de Entrada *turnstiles*** (catracas), ***mantraps*** (Sistema no qual a pessoa deve passar por duas portas com apenas uma aberta por vez).

mantraps https://www.ceia.net/security/product.aspx?a=14&lan=usa

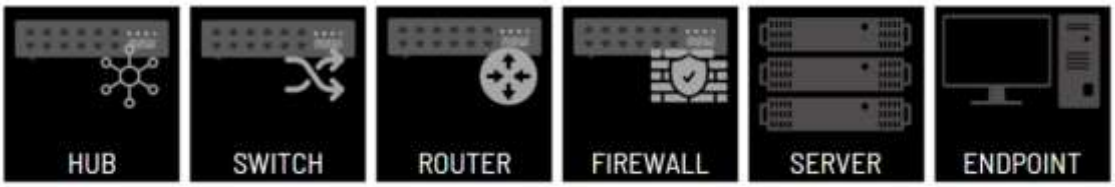
Logical Security Controls

- ***Discretionary Access Control (DAC)*** – Controle de acesso discricionário: O proprietário pode determinar quem deve ter direitos de acesso a um objeto e quais devem ser esses direitos. Exemplo: Pasta em servidor Windows ou Linux.
- ***Mandatory Access Control (MAC)*** – Controle de acesso obrigatório: Controle de acesso que exige que o próprio sistema gerencie os controles de acesso de acordo com as políticas de segurança da organização.Exemplo: Um sistema de segurança militar com um objeto de ultra-secreto
- ***Role-Based Access Control (RBAC)*** – Controle de acesso baseado em função configura permissões de usuário com base em funções.

DOMÍNIO 4 – Network Security

Local area network (LAN) – Rede Local, usada em único andar ou edifício e em redes domésticas.

Wide area network (WAN) – Rede usada para conexões de longa distância entre redes geograficamente remotas.



- **Hubs** – Hubs são dispositivos com fio e não são tão inteligentes quanto switches ou roteadores.
- **Switches** – Os switches são dispositivos com fio que conhecem os endereços dos dispositivos conectados a eles e roteiam o tráfego para essa porta/dispositivo em vez de retransmitir para todos os dispositivos. Os switches podem criar domínios de broadcast ao criar VLANs.
- **Routers** – Os roteadores determinam a "rota" mais eficiente para o tráfego na rede.
- **Servers** – Um servidor é um computador que fornece informações para outros computadores em uma rede.
- **Endpoints** – Um endpoint pode ser outro servidor, estação de trabalho desktop, laptop, tablet, celular ou qualquer outro dispositivo de usuário final.

Modelo OSI – Open Systems Interconnection

Layer	Layer Name	Descrição	Tipo	Protocols
7	**APPLICATION**	Corresponde às aplicações para usuários (programas) e acesso a serviços de rede.	Data	HTTPS, LDAP, DNS, SSH, IMAP, **SSH** **DHCP, SNMPm DHCP**
6	**PRESENTATION**	Formatação de dados a ser apresentado na camada de aplicação. Compressão e criptografia de dadis, ASCII, Unicode(UTF8)	Data	
5	**SESSION**	Estabelecimento de Sessão – Não é seguro	Data	Netbios, **RPC**, NFS, SOCKS, **PAP**, **PPTP**
4	**TRANSPORT**	Conexão de ponta a ponta, segmentação	Segment	TCP, UDP, **SSL/TLS**
3	**NETWORK**	Tratamento de erros de endereço lógico. Roteamento, Subnet, mapeamento de endereço lógico / físico.	Packets	ICMP, IGMP, ISAKMP **IPSEC**, IKE IPv6, OSPF, **IP**
2	**DATA LINK**	Logical Link Control Midia Access Control	Frames	**ARP**, **LLC**, PPTP, PAP. CHAP, EAP, PPP

		(**MAC**) Data framming,		
1	**PHYSICAL**	Topologia, Codificação e Sinalização – Transmissão e controle de colisões	Bits	Ethernet, 802.11

MAC Media Access Control – **MAC Address** Cada dispositivo de rede possui um endereço de controle de acesso de mídia (MAC). Um exemplo é 00-13-02-1F-58-F5.

ARP – Protocolo de Resolução de Endereço IP para MAC Address

Endereço IP (Internet Protocol) Os hosts IP associam esse endereço MAC a um endereço lógico (IP) exclusivo. Exemplos são 192.168.1.1 e 2001:db8::ffff:0:1.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Application	Define os protocolos para a camada de transporte. (Aplicação, apresentação e sessão)
Transport	Permite que os dados se movam entre dispositivos (Transporte)
Internet	Cria/insere pacotes. (Internet)
Network	Como os dados se movem pela rede. (Data link, e Física)

IPv4

Nós usamos a notação decimal para representar um endereço de IP. Exemplo: 192.168.2.200
Recomendo baixar o PDF Guia_do_TCP-IP

Guia_do_TCP-IPBaixar

Endereços de rede privados

- **Classe A** 10.0.0.0 até 10.255.255.255
- **Classe B** 172.16.0.0 até 172.31.255.255
- **Classe C** 192.168.0.0 até 192.168.255.255

IPv6

- ::1 é o endereço de loopback local, usado da mesma forma que 127.0.0.1 no IPv4.

- O intervalo de 2001:db8:: a 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff é reservado
- fc00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff são endereços reservados para uso interno da rede e não são roteáveis na internet.

Secure Ports

- Well-known ports (0–1023)
- Registered ports (1024–49151):
- Dynamic or private ports (49152–65535)

Porta	Protocolo	Porta Segura alternativa	Protocolo
21	File Transfer Protocol	22* – SFTP	Secure File Transfer Protocol
23	Telnet	22* – SSH	Secure Shell
25	Simple Mail Transfer Protocol	587	SMTP with TLS
37	Time Protocol	123	NTP Network Time Protocol
53	DNS	853	DNS over TLS (DOT)
80	HTTP	443	HTTPS – (SSL/TLS)
143	IMAP	993	IMAP – (SSL/TLS)
161/162	SNMP	161/162	SNMPV3
445	SMB	2049	NFS
386	LDAP	636	LDAPS

Three-way handshake

```
+----+                +----+
|    | --------SYN-------> |    |
|    | <------SYN/ACK----- |    |
|    | --------ACK-------> |    |
+----+                +----+
10.0.0.1/21           10.0.0.3:21
```

Ameaças

- **Spoofing** – Falsificação de um endereços IP, MAC, nomes de usuários, SSIDs de wifi, endereços de e-mail
- **Phishing** – E-mail falso com redirecionamento para sites maliciosos, URL e anexos infectados.
- **DoS/DDoS** – Denial-of-service (DoS) ou distributed denial-of-service (DDoS) term como objetgivo parar a rede ou serviços .
- **Vírus** – Software malicioso que se espalha geralmente quando um usuário clicar em um link ou abrir um arquivo.
- **Worm** – Similar ao vírus porém eles se propagam sem exigir qualquer intervenção humana.

- **Trojan** – Programa de software que parece inofensivo , mas carrega um payload malicioso
- **On-Path Attack** é o mesmo que **man-in-the-middle (MITM)** um método de interceptar e/ou manipular os dandos entre duas ou mais vítimas.
- **Side-channel** – Ataque que faz uso de monitoramento de energia, pulsos eletromagnéticos e alguns ataques a criptografia. É um ataque passivo.
- **Advanced Persistent Threat (APT)** – Um ataque sofisticado geralmente conduzidos por grupos altamente organizados de invasores.
- **Insider Threat** – Ameaça interna, por exemplo, funcionários descontentes ou funcionários envolvidos em espionagem.
- **Malware** – Software malicioso
- **Ransomware** – Ataque que geralmente usa criptografia para "bloquear" arquivos e exigir o pagamento de resgate. (*Ransomware com dupla extorsão além da criptografia pede resgate para não publicar dados vazados*)

Ferramentas de proteção

Ferramenta	Descrição	Identifica Ameaça	Previne Ameaças
Intrusion Detection System (IDS)	Uma forma de monitoramento para detectar atividade anormal; ele detecta tentativas de intrusão e falhas do sistema.	X	
Host-basaed DS (HIDS)	Monitora a atividade em um único computador.	X	
Network-based DS (NIDS)	Monitora e avalia a atividade da rede para detectar ataques ou anomalias de eventos.	X	
SIEM	Reúne dados de log de fontes em uma empresa para entender as preocupações de segurança e distribuir recursos.	X	
Anti-malware/Antivirus	Procura identificar softwares ou processos maliciosos.	X	X
Scans	Avalia a eficácia dos controles de segurança.	X	
Firewall	Filtra o tráfego de rede – gerencia e controla o tráfego de rede e protege a rede.	X	X
Intrusion Protection System (IPS-NIPS/HIPS)	Um IDS ativo que automaticamente tenta detectar e bloquear ataques antes que eles atinjam os sistemas de destino.	X	X

Firewalls podem gerenciar o tráfego nas camadas 2 (endereços MAC), 3 (interfaces de IP) e 7 (interface de programação de aplicativos (API) e firewalls de aplicativos).

Infraestrutura de rede segura.

Acordos de uso de recursos em caso de emergência (redundância). Esses acordos muitas vezes incluem até concorrentes: Exemplo, um hospital que precise usar os recursos tecnológicos de outro hospital.

- *joint operating agreements (JOA)*
- *memoranda of understanding (MOU)*
- *memoranda of agreement (MOA)*

Service-Level Agreement (SLA) – Contrato com os níveis mínimos de serviço e soluções.

Managed service provider (MSP) – é uma empresa prestadora de serviço que gerencia ativos de tecnologia da informação para outra empresa.

Cloud e On-Premises

On-Premises – Ambiente físico. As organizações podem terceirizar o data center ou possuir o data center.

Cloud ou Cloud computing – Serviços de computação de um datacenter vendidos por um provedor de serviços em nuvem (CSP) com muitas vantagens:

- Segurança;
- Redundância;
- Disponibilidade;
- Serviços modernos e mensuráveis;
- Elasticidade (capacidade de suportar o aumento de recursos automaticamente) ;
- On-Demand Self-service.

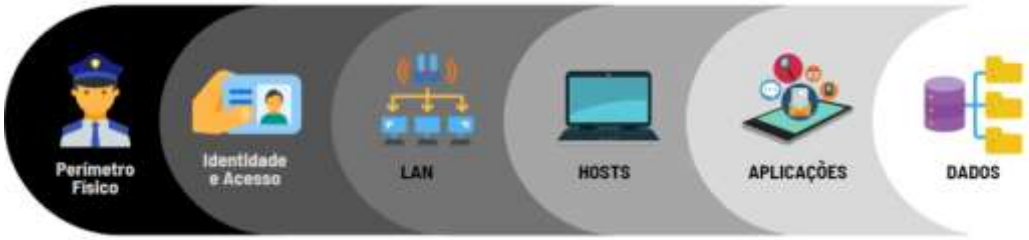
Cloud pode ser: **publica**, **privada** ou **hibrida**.

Os modelos de serviços oferecidos na cloud são:

- **Software as a Service (SaaS**) – Aplicativos de software, como e-mail ou ferramentas de produtividade.
- **Platform as a Service – (PaaS)** – Plataforma com ambiente para os clientes construir e operar seu próprio software.
- **Infraestructure as a Service – (IaaS)** – Recursos básicos de computação, isso inclui servidores, armazenamento e, em alguns casos, recursos de rede.

Defense in Depth – Defesa em profundidade.

O princípio de defesa em profundidade requer o uso de **controles** sobrepostos para atender ao mesmo objetivo.



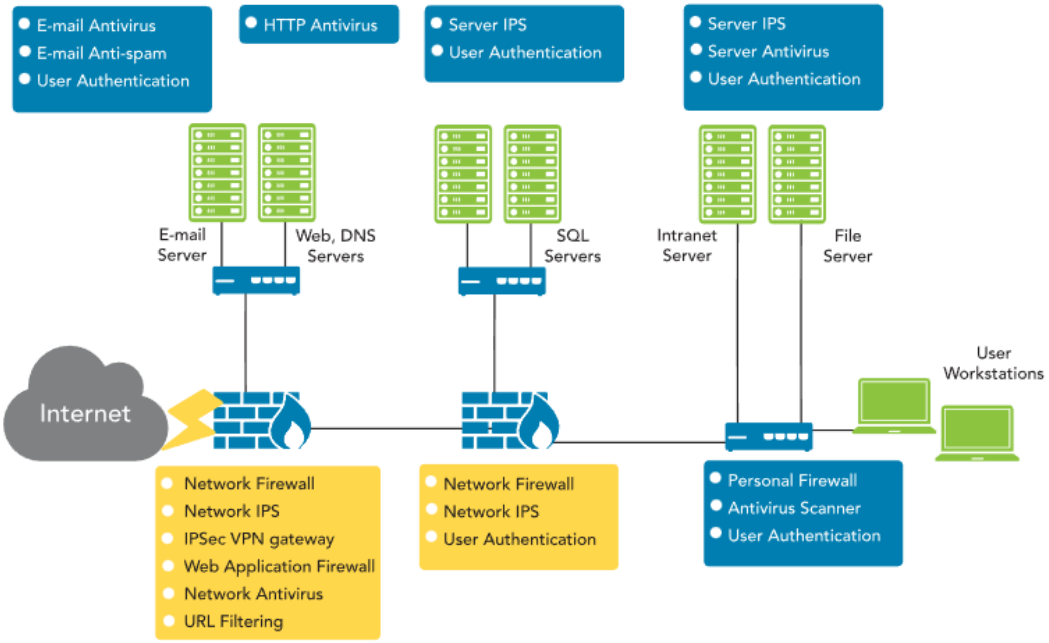
Zero Trust – Em network é o conceito que usa a microsegmentation para proteger os segmentos de rede.

VLAN – Uma rede local virtual definida em switches.

VPN – túnel de comunicação que fornece transmissão ponto a ponto de autenticação e tráfego de dados em uma rede não confiável

Network Access Control (NAC) – Controla o acesso a rede através de políticas aumentar a segurança e reduzir riscos.

DMZ (demilitarized zone) é um segmento virtual geralmente definido por um firewall que contém dispositivos menos confiáveis entre a rede corporativa e a internet.



DOMÍNIO 5 – Security Operations

Ciclo de vida dos dados "Criar – Armazenar – Usar – Compartilhar – Arquivar – Destruir"

Classificação – Classificar dados com base no seu valor para o negócio – objetivo da classificação de dados é aplicar Controles de Segurança (lembre-se da LGPD e os dados sensíveis). Os dados classificados recebem uma marcação (***Labelling***). Exemplo:

- *Top Secret*
- *Secret*
- *Confidential*
- *Unclassified*

Classificação de Ativos *deve corresponder à classificação dos dados. Se um computador estiver processando dados* ***ultrassecretos****, o computador também deve ser classificado como um ativo* ***ultrassecreto***.

Criptografia

Informações e dados devem ser mantidos (***Retention***) enquanto for necessário, nem mais nem menos.

- **Data at Rest** – Dados em repouso podemos usar criptografia ***AES 256, TPM, Bitlocker, EFS***
- **Data in Transit** – Dados em trânsito temos ***IPSec, SSL/TLS***
- **Data in Use** – Dados em uso – bloqueio do computador, protetor de tela

A criptografia fornece confidencialidade, HASH garante a integridade.

Plaintext – Texto simples são os dados ou mensagens não criptografados.

Encryption – Processo de converter um "texto simples" em texto criptografado (***ciphertext***)

Hash Function – A função hash gera um valor numérico unico para um arquivo ou mensagem (dados em geral). **Entendendo o HASH (MD5 e SHA1)** – As senhas são geralmente transformadas em hash e então criptografadas.

Digital signatures – Assinaturas digitais fornece integridade ao verificar se uma mensagem não foi alterada por malícia ou erro.

LOGs – Armazenamento de eventos gerados nos sistemas e nas comunicações e permite monitorar ações, comportamentos, saúde dos sistemas e ajudam a identificar possíveis riscos.

- ***Ingress monitoring*** – Eventos de entrada e tentativas de acesso (Firewalls, IDS/IPS, Gateways)
- ***Egress monitoring*** – Eventos de saída (Email, File Transfer Protocol (FTP), websites, DLP)

Destruição de dados – Destruir dados confidenciais

- **Erasing (Delete)** – Apenas exclui
- **Clearing (Override)** – Limpar a mídia para reutilização – não use para SSDs
- **Purging (Intense Overrride)** – substituição intensa para um ambiente com menos segurança
- **Degaussing (Magnetic field)** A desmagnetização do HD destroi os dados. Não serve para CD, DVD, SSD
- **Crypto-shredding** – Consiste em destruir as chaves que permitem que os dados sejam descriptografados, tornando os dados indecifráveis.
- **Destruction** – Destruir é o método de higienização mais seguro

O melhor método de higienização do SSD é a destruição.

Configuration management

Inventário – Identificação, catalogo ou registro de de ativos.

Você não pode proteger o que não sabe que tem.

Baseline – Uma linha de base de segurança é um nível mínimo de proteção que pode ser usado como ponto de referência

Hardening – Uma referência ao processo de aplicação de configurações seguras (para reduzir a superfície de ataque)

Change Management – Um processo de revisão e aprovação para todas as alterações. Isso inclui atualizações e patches, Inclui os seguintes componentes.

Patch Management – O gerenciamento de patches se aplica principalmente a dispositivos de software e hardware. Um patch é uma atualização, upgrade ou modificação de um sistema ou componente.

- Request for change (RFC)
- Approval
- Rollback

Security Awareness Training – Eficiente principalmente sobre Engenharia Social

- Education (Educação)
- Training (Treinamento)
- Awareness (Conscientização)

Ataques de Engenharia Social

Phishing – Técnica de engenharia social usada para enganar usuários de modo que possam clicar ou acessar algo malicioso a fim de executar um malware ou coletar informações sensíveis.

Spear phishing – Mesmo método do phishing porém com um alvo específico

Whaling – Ataques de phishing que tentam enganar funcionários de alto escalão

vishing – Uso de um sistema de resposta de voz interativa (IVR) não autorizado para recriar uma cópia legítima de um sistema IVR de um banco ou outra instituição.

Pretexting – O equivalente "humano" de phishing, onde alguém se faz passar por uma figura de autoridade ou um indivíduo confiável.

Quid pro quo – Solicitar dadosm informações, senhas ou credenciais de login em troca de alguma compensação.

Tailgating – A prática de seguir um usuário autorizado em uma área ou sistema restrito. (Se aproveitar de uma passagem aberta)

Password Protection – Conscientização para que o usuário saiba que não deve:

- Reutilizar senhas em vários sistemas
- Anotar senhas e deixá-las em áreas não seguras.
- Compartilhar uma senha com o suporte técnico ou um colega de trabalho.