

Boas Práticas de Segurança da Informação



Unidade 4 - Boas práticas da segurança da informação

- 4.1-Políticas de senha
- 4.2-Treinamento dos usuários
- 4.3-Mecanismos de proteção
- 4.4-Controle de acessos
- 4.5-Política de utilização de antivírus e antimalwares
- 4.6-Backups
- 4.7-Criptografia e Certificado Digital

Boas Práticas de Segurança da Informação

- Segurança da informação é um tema que ganhou corpo nos últimos anos, obtendo espaço nas mídias e tornando-se “commodity”, em empresas dos mais variados portes e segmentos.
- Em contrapartida é importante frisar que a popularização do termo **SI** (Segurança da Informação) foi motivada pela elevação no número de incidentes de segurança, ocorridos em âmbito mundial.
- Os transtornos gerados por estes incidentes são variados gerando, desde danos à imagem do negócio, vazamento de informações críticas, podendo acarretar em perdas financeiras substanciais.



Boas Práticas de Segurança da Informação

- O aumento do número de ocorrências influencia na percepção de valor sobre investimentos em Segurança da Informação, e fazem com que empresas busquem a estruturação de processos para garantir que seus negócios estejam protegidos contra os mais variados tipos de ameaças virtuais.



4.1-Políticas de Senha

- A **política de senha** é um conjunto de regras destinadas a aumentar a segurança da informação nos computadores, através do incentivo para os usuários utilizarem senhas fortes e usá-las corretamente.
- A política de senha faz muitas vezes parte dos regulamentos oficiais da organização e pode ser ensinada como parte do treino de conscientização de segurança.
- A política de senhas pode ter tanto um carácter de precaução ou ser imposta por meios técnicos.



4.1-Políticas de Senha

- **Tamanho mínimo da senha e Complexidade da senha:** A exigência de um tamanho mínimo e a de complexidade (i.e. a presença de letras, números, símbolos e maiúsculas/minúsculas, número de caracteres) são a principal defesa contra ataques de força bruta ou dicionário.
- As duas juntas garantem um nível de variação – ou entropia - mínimo para tornar um ataque de força bruta demasiado caro ou mesmo inviável.



4.1-Políticas de Senha

- A configuração de complexidade default do Active Directory exige que a senha tenha pelo menos três símbolos de quatro categorias (maiúsculas, minúsculas, algarismos e caracteres não-alfanuméricos) e não contenha nem o primeiro nem o último nome do usuário. Isso deve ser suficiente para a maioria das organizações - pode ser implementado no entanto um critério particular.



4.1-Políticas de Senha

- Mas como balancear a complexidade da senha com a necessidade dela ser facilmente lembrada pelos usuários?
- Orientando o uso de frases secretas ao invés de senhas curtas mais ininteligíveis. Por exemplo, a senha *Eu adoro pão* tem mais entropia do que *egp** (a primeira é muito mais fácil de ser lembrada). Não aceite a velha desculpa de que os usuários não vão conseguir lembrar as senhas e, por isso, não dá para forçar senhas complexas - a experiência no mundo real prova o contrário.



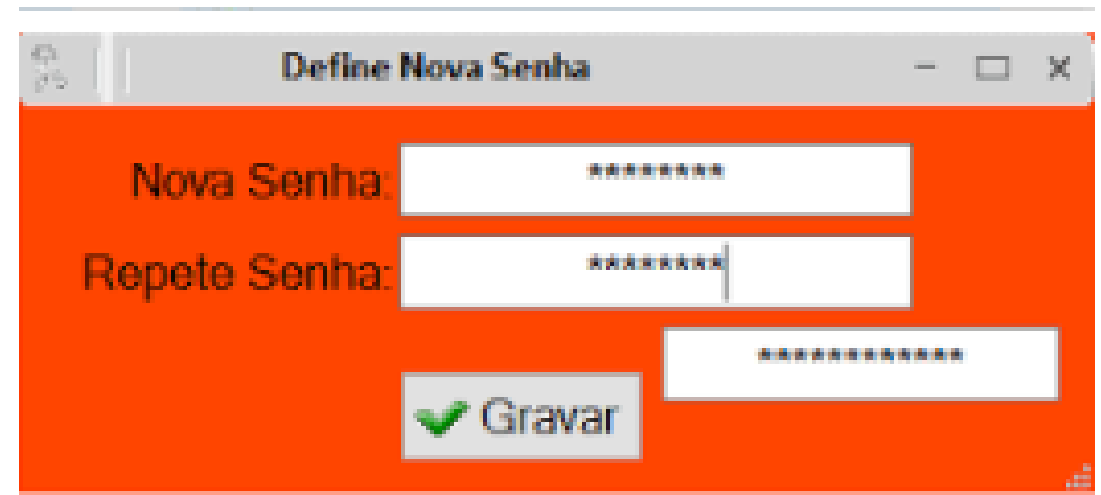
4.1-Políticas de Senha

- **Troca periódica da senha:** Trocar a senha periodicamente acrescenta muito pouco em termos de segurança.
- A origem da troca periódica de senha está no tempo em que o poder computacional para fazer o ataque de força bruta contra uma senha era limitado, e fazia sentido trocar a senha em um prazo menor do que o tempo que em tese seria gasto fazendo o ataque.
- Nos dias de hoje com o poder computacional esse cálculo não faz mais muito sentido, e forçar uma troca periódica muito frequente cria mais chamadas no Help Desk do que proteção adicional.



4.1-Políticas de Senha

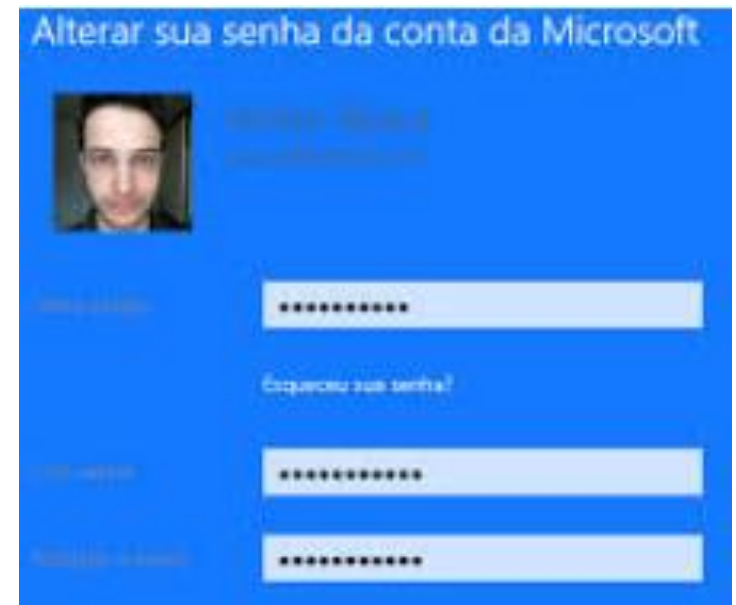
- **Troca periódica da senha:**
- Trocas periódicas de senha têm no entanto um benefício - elas são ótimas para você encontrar contas de usuário que não são mais utilizadas (*stale accounts* – *conta antiga*) e deveriam ter sido desabilitadas ou removidas.
- Recomenda-se colocar a troca periódica na política de senhas, mas em um prazo maior, talvez a cada três ou quatro meses.



The image shows a screenshot of a web application window titled "Define Nova Senha". The window has a red background. It contains three input fields for passwords, each with a white border and a small "x" icon on the right. The first field is labeled "Nova Senha:" and contains seven asterisks. The second field is labeled "Repete Senha:" and contains seven asterisks. The third field is empty and contains eight asterisks. Below the input fields is a green button with a white checkmark icon and the text "Gravar".

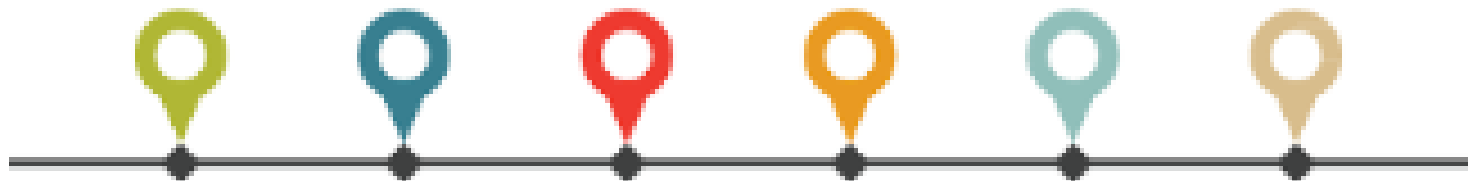
4.1-Políticas de Senha

- **Não repetição das últimas senhas:** Usado para impedir que o usuário "troque" a senha e continue com a mesma.
- Não há contra indicações em definir um limite alto para esta - o default no Windows são as últimas 24 e parece adequado, mas fica a critério de cada administrador de rede e suas políticas.



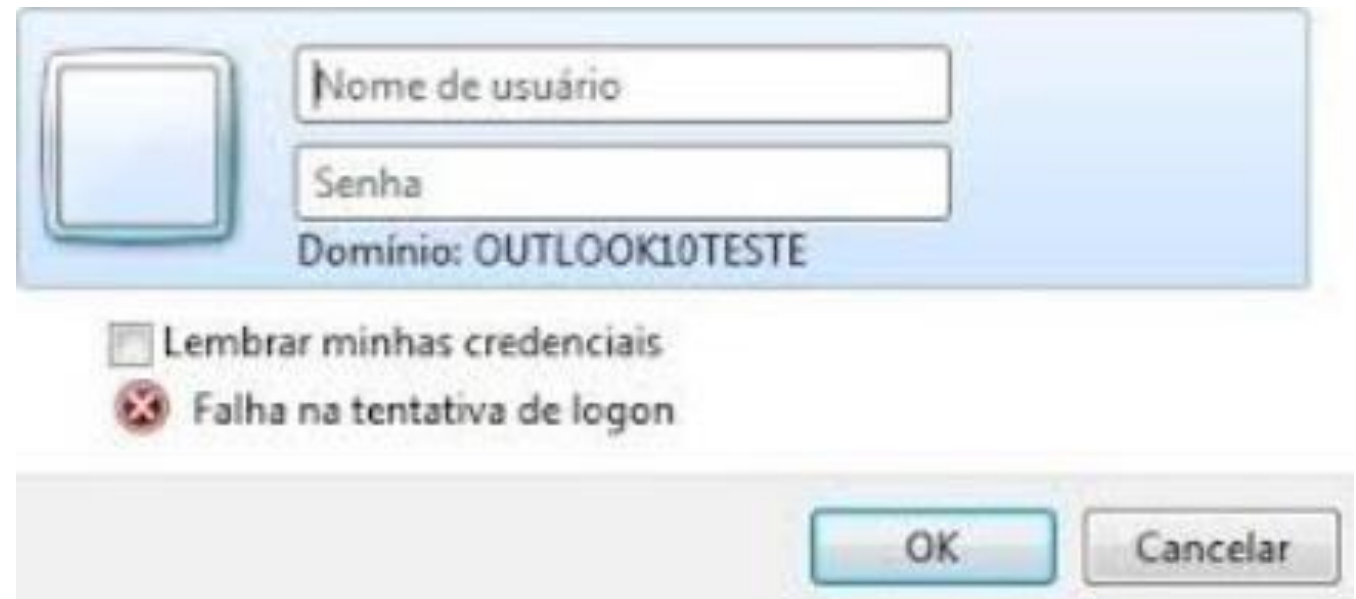
4.1-Políticas de Senha

- **Prazo mínimo de troca de senhas:** Serve em tese para impedir que o usuário troque a senha seguidas vezes, ultrapassando o limite estabelecido para não repetir as últimas senhas, e voltando para a senha anterior.
- Tem no entanto um efeito colateral: se o usuário trocou a senha e ele não se sentiu confortável (ou mesmo foi vista por uma outra pessoa), ele terá que esperar o prazo mínimo ou chamar o Help Desk para poder fazer uma nova troca (“ressetar” a senha).



4.1-Políticas de Senha

- **Prazo mínimo de troca de senhas/bloqueio**
- **Bloqueio de contas:** Bloquear o acesso do usuário após um determinado número de tentativas de autenticação incorretas é uma das melhores formas de se proteger contra ataques.



The image shows a Windows login dialog box with a light blue header and a white body. On the left is a square icon placeholder. To its right are two text input fields: the top one is labeled 'Nome de usuário' and the bottom one is labeled 'Senha'. Below the password field, the text 'Domínio: OUTLOOK10TESTE' is displayed. Underneath the input fields is a checkbox labeled 'Lembrar minhas credenciais'. Below the checkbox is a red 'X' icon followed by the text 'Falha na tentativa de logon'. At the bottom right of the dialog are two buttons: 'OK' and 'Cancelar'.

4.2 - Treinamento dos Usuários

- O universo da Segurança da Informação vem passando por um momento de mudanças graduais, constantes e significativas devido ao avanço tecnológico e ao **crescimento do cibercrime**.
- Atualmente, a introdução de tecnologias como IoT, por exemplo, apesar de terem trazido mais velocidade e eficiência para os negócios, também ampliaram a superfície de ataque, aumentando, consequentemente, o êxito dos ataques cibernéticos.



4.2 - Treinamento dos Usuários

- Atualmente, muitas empresas estão sendo invadidas por ataques simples e nada sofisticados.
- Os cibercriminosos tem utilizado técnicas de engenharia social, por exemplo, para persuadir as pessoas e conseguirem acesso às redes ou às informações.
- Ataques que poderiam ser totalmente evitados caso os usuários tivessem sido conscientizados.



4.2 - Treinamento dos Usuários

- A conscientização em Segurança da Informação é capaz de **gerar mudança no comportamento** de todos e por isso é vista como uma ferramenta com grande potencial para beneficiar as organizações.



4.2 - Treinamento dos Usuários

- Funcionários conscientes do quão importante são os dados e informações, com os quais trabalham, e de seu papel na proteção desses ativos, redobram seus níveis de atenção e proteção.
- Isso faz com que seja diminuído o sucesso dos ataques que poderiam vazar dados da empresa, dos colaboradores e até mesmo dos clientes, debilitando a imagem da empresa.



4.2 - Treinamento dos Usuários

- Portanto, os membros da organização ficarão mais atentos a ataques e dispostos a participar de treinamentos à medida que forem se conscientizando da importância do papel que desempenham dentro da empresa. Podendo, inclusive, propor novas medidas de segurança, deixando de ser apenas um **usuário conscientizado**, e passando a ser um **usuário participativo**.



4.2 - Treinamento dos Usuários

- Somente a criação de uma Política de Segurança da Informação não garante a segurança da empresa.
- Os colaboradores devem cumprir com a política estabelecida e é aqui que as campanhas de conscientização entram como recurso, garantindo que toda a empresa seja treinada, educada e conscientizada de acordo com as políticas e procedimentos da organização.



4.2 - Treinamento dos Usuários

Boas Práticas:

- Bloquear o computador ao se ausentar do posto de trabalho a fim de que ninguém tenha acesso aos seus dados.
- Nunca disponibilizar logins e senhas, mesmo que para colegas de trabalho.
- Ter atenção ao falar sobre a empresa, clientes ou negócios em táxis, elevadores e metros, por exemplo.
- Utilizar as redes sociais com segurança, não disponibilizando informações sigilosas ou fazendo contato com desconhecidos.
- Verificar atentamente os e-mails.
- Nunca fotografar o ambiente de trabalho, principalmente telas de computador e documentos.
- Reportar à equipe de segurança de sua empresa qualquer problema ou desconfiança em relação às atitudes suspeitas na internet.
- Seguir as políticas e práticas de segurança da empresa, a fim de que exista uma gestão funcional de segurança.

4.2 - Treinamento dos Usuários

- Os Treinamento visam não só educar e conscientizar o colaborador, mas procura informá-lo sobre as reais ameaças as quais ele está exposto, ensinando como identificar e reagir aos diferentes ataques online.
- Estar consciente não significa saber tudo sobre todos as possíveis formas de ataque às quais você pode ser submetido, mas sim, entender o grau de importância das informações com as quais você está lidando e redobrar sua atenção e cuidado a fim de proteger os dados mais sensíveis e os ativos essenciais da sua empresa.



4.3 - Mecanismos de Proteção

- O suporte para as recomendações de segurança pode ser encontrado em:
 - Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.
- Existem mecanismos de segurança que apoiam os controles físicos:
 - Portas / sensores / dispositivos digitais de acesso / blindagem / guardas / etc.



4.3 - Mecanismos de Proteção

- Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.
- Existem mecanismos de segurança que apoiam os controles lógicos:
 - *Mecanismos de criptografia.* Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.



4.3 - Mecanismos de Proteção

- Controles lógicos (Continuação):
 - *Assinatura digital*. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.
 - *Mecanismos de controle de acesso*. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
 - *Mecanismos de certificação*. Atesta a validade de um documento.



4.3 - Mecanismos de Proteção

- Controles lógicos (Continuação):
 - *Honeypot*: É o nome dado a um software, cuja função é detectar ou impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.



4.4 - Controle de Acessos

- Em segurança, especialmente segurança física, o termo **controle de acesso** é uma referência à prática de permitir o acesso a uma propriedade, prédio, ou sala, apenas para pessoas autorizadas.
- O controle físico de acesso pode ser obtido através de pessoas (um guarda, segurança ou recepcionista); através de meios mecânicos como fechaduras e chaves; ou através de outros meios tecnológicos, como sistemas baseados em cartões de acesso.



4.4 - Controle de Acessos

- O **controle de acesso** é composto dos processos de Autenticação, Autorização e Auditoria (*accounting*).
- Neste contexto:
- O controle de acesso pode ser como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo).
- A autenticação identifica quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer.
- E a auditoria diz o que o usuário fez.



4.4 - Controle de Acessos

- **A identificação e autenticação** fazem parte de um processo de dois passos que determina quem pode acessar determinado sistema.
- Durante a identificação o usuário diz ao sistema quem ele é (normalmente através de um nome de usuário).
- Durante a autenticação a identidade é verificada através de uma credencial (uma senha, por exemplo) fornecida pelo usuário.



4.4 - Controle de Acessos

- **A identificação e autenticação (Continuação)...**
- Atualmente, com a popularização tecnológica, reconhecimento por impressão digital, smartcard, RFID estão substituindo, por exemplo, o método de credencial (nome e senha).
- Dispositivos com sensores que fazem a leitura, a verificação e a identificação de características físicas únicas de um indivíduo aplicam a biometria e fazem agora a maior parte dos reconhecimentos.
- A identificação biométrica por impressão digital é a mais conhecida e utilizada atualmente por sua fiabilidade alta e baixo custo.



4.4 - Controle de Acessos

- **A autorização** define quais direitos e permissões tem o usuário do sistema.
- Após o usuário ser autenticado, o processo de autorização determina o que ele pode fazer no sistema.



4.4 - Controle de Acessos

- **A auditoria (*accounting*)** é uma referência à coleta da informação relacionada à utilização, pelos usuários, dos recursos de um sistema.
- Esta informação pode ser utilizada para gerenciamento, planejamento, cobrança e etc.
- A auditoria em tempo real ocorre quando as informações relativas aos usuários são trafegadas no momento do consumo dos recursos.
- Na auditoria em batch as informações são gravadas e enviadas posteriormente.
- As informações que são tipicamente relacionadas com este processo são a identidade do usuário, a natureza do serviço entregue, o momento em que o serviço se inicia e o momento do seu término.



4.5 - Política de Utilização de Antivírus e Antimalwares

- **Antivirus:** Todo computador/notebook da instituição deve possuir instalado a solução de antivírus corporativo.
- Todo e qualquer dispositivo conectado ao equipamento que possui o antivírus instalado será scanado para verificar se o mesmo está ou não infectado.
- Semanalmente, o antivírus fará uma varredura em todos os computadores da instituição procurando por pragas virtuais. Esta varredura se faz de forma diferencial, ou seja, apenas nos arquivos modificados desde a última varredura.
- A equipe responsável pela manutenção da ferramenta tem autonomia para, caso julguem necessário, tomar medidas pró-ativas para combater ou prevenir uma disseminação de pragas virtuais.
- Outras políticas podem e devem ser implementadas.



4.5 - Política de Utilização de Antivírus e Antimalwares

- **Antimalwares:**
- Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador.
- Políticas de antimalware incluem informações sobre o agendamento de verificação, os tipos de arquivos e pastas para exame e as ações a serem tomadas quando um malware é detectado.
- Quando você habilita Proteção de ponto de extremidade, uma política de antimalware padrão é aplicada a computadores cliente. Você também pode usar modelos de diretiva adicionais que são fornecidos ou criar suas próprias políticas de antimalware personalizadas para atender às necessidades específicas do seu ambiente.



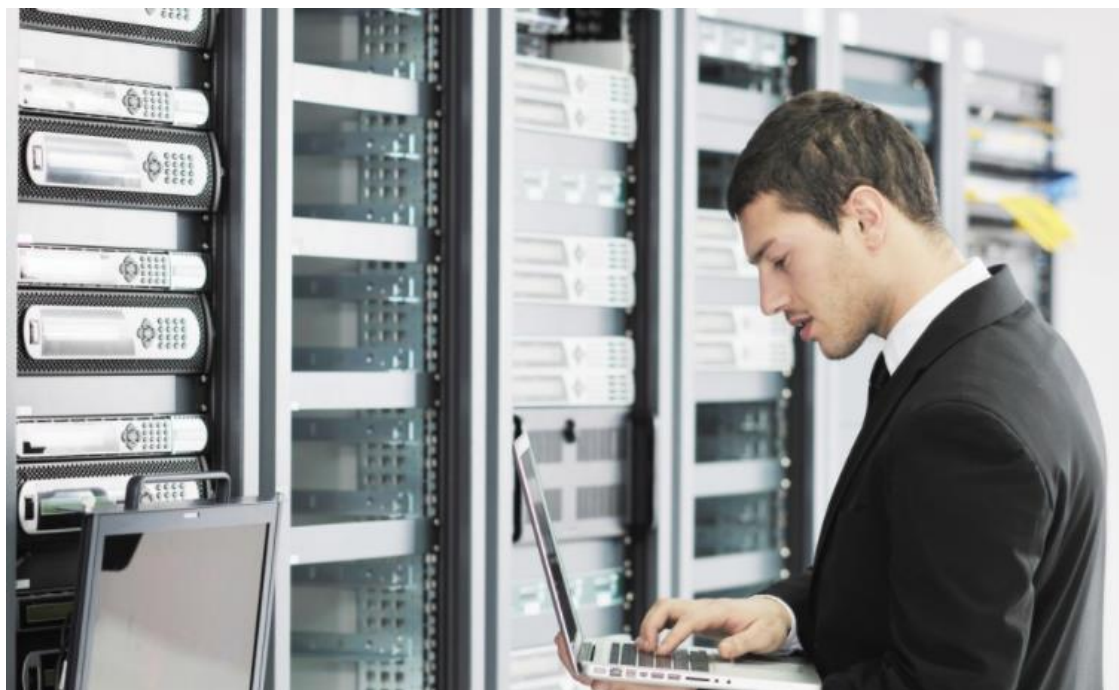
4.6 - Backups

- O que acontece com os dados de sua empresa quando existem falhas no sistema de gestão, quando informações são acidental ou intencionalmente excluídas ou quando os servidores param?
- A política de backup exerce a função de garantir que sua equipe de TI esteja preparada para reagir caso os dados sejam afetados por qualquer tipo de incidente.



4.6 - Backups

- A política de backup precisa ser definida exatamente na estratégia de diminuição de riscos.
- Afinal, sua função é garantir a disponibilidade de cópias de segurança quando elas forem necessárias.



4.6 - Backups

Os 5 questionamentos para a definição de uma boa política de backup:

- 1. Quais dados precisam ser copiados?
 - Avalie junto aos diversos setores da empresa quais são os documentos, qual é a importância deles e o tempo de retenção que cada um deve ter. Analise a frequência com que surgem novos arquivos daquela categoria e mapeie quais serão os impactos de perdê-los.
- 2. Onde podem ser copiados?
 - Na nuvem, em fita, em disco ou em um servidor de redundância?
- 3. Qual é a rotina de backup?
 - A rotina deve ser estabelecida com base no volume de arquivos importantes utilizados por seus colaboradores na execução de seus trabalhos.



4.6 - Backups

Continuando.....Os 5 questionamentos para a definição de uma boa política de backup:

- 4. Quem executa o backup e as restaurações?
 - A equipe de TI pode executar a rotina completa ou usar um software para automatizar o backup, ficando responsável apenas pelas restaurações. Outra opção é contratar um serviço terceirizado para gerenciar esse processo.
- 5. Quais são os custos?
 - A última parte do plano é dimensionar o tamanho dos arquivos a serem copiados, a taxa prevista de crescimento em Terabytes para as cópias de documentos e os dispositivos necessários para suportar o backup. Depois disso, aponte os custos financeiros da estratégia.



4.6 - Backups

- Definir uma política de backup deve ser uma das primeiras tarefas da governança de TI.
- Afinal, as cópias de segurança são recursos que apoiam outras estratégias, como a de Disaster Recovery.
- Colocar essa estratégia em ação será muito mais simples e eficaz após a área de TI ou um parceiro ter documentado quais dados, onde, como e quem executa o backup de sua empresa.



4.7-Criptografia e Certificado Digital

- A criptografia (do grego kriptós que significa escondido mais grápho que significa grafia, escrita) é a ciência de escrever em códigos, de forma que apenas o destinatário consiga compreender a mensagem.
- A Criptografia transforma um texto compreensível em um texto incompreensível, chamado de texto cifrado.



4.7-Criptografia e Certificado Digital

- Cada vez mais comum, o certificado digital oferece uma série de vantagens em relação à economia de tempo e dinheiro e permite reduzir a burocracia.
- A Certificação Digital trata uma identidade virtual que utiliza criptografia e permite saber, de forma segura e inequívoca, quem foi o autor de uma determinada mensagem ou de uma transação feita em meios eletrônicos.



4.7-Criptografia e Certificado Digital

- Por trás das ferramentas que agilizam processos pela internet e faz com que transações fiquem mais seguras e baratas está a **criptografia** .
- "O certificado digital é gerado e assinado por uma Autoridade Certificadora, que segue regras estabelecidas pelo Comitê Gestor da ICP-Brasil [Infraestrutura de Chaves Públicas Brasileira] e associa cada titula a um par de chaves criptográficas”.



4.7-Criptografia e Certificado Digital

- **Como o certificado digital utiliza a criptografia?**
- Ao utilizar este tipo de segurança, o emissor envia um texto cifrado que terá de ser reprocessado novamente para que o receptor consiga acessar a informação.
- Esse segundo processamento ocorre somente se o destinatário tiver a chave correta para decodificar a mensagem.
- "Na prática, assinatura digital, por meio da criptografia, garante a integridade e a comprovação da autoria do documento.



4.7-Criptografia e Certificado Digital

- **Qual o principal benefício da assinatura digital?**
- "Todo mundo quer ganhar mais eficiência, fazer comunicação remota, reduzir custos.
- A contrapartida, porém, é que quanto menor o investimento em segurança, maior a probabilidade do surgimento de vulnerabilidades que exigem a identificação dos cliente e dos funcionários.
- A identificação segura e com validade jurídica, conferida pela certificação digital, protege os dados pessoais e estimula a transformação digital nos mais diferentes setores da economia, contribuindo para a transparência, eficiência, além de permitir menos burocracia.

4.7-Criptografia e Certificado Digital

- **Em que setores a certificação digital é mais usada atualmente?**
- A certificação já é amplamente adotada por aplicações do setor público e também no judiciário, rendendo a eles uma série de avanços.
- Os benefícios da transformação digital, com suporte jurídico, já estão sendo identificados também por outros setores importantes da economia, entre eles, o setor de saúde, financeiro e de serviços.



4.7-Criptografia e Certificado Digital

- **Que tipo de informações um certificado digital pode carregar?**
- As principais informações que um certificado carrega são chave do titular, nome e endereço de e-mail, período de validade do certificado, nome da Autoridade Certificadora que emitiu o documento, além do número de série e da assinatura digital da empresa responsável pelo certificado.



4.7-Criptografia e Certificado Digital

- **O que são tokens e smart cards?**
- Tokens e smart cards são dispositivos portáteis que servem como mídias armazenadoras de chaves.
- O proprietário de uma certificação pode consultar suas chaves por meio do que está salvo nos chips dos equipamentos.
- O acesso às informações é feito por meio de uma senha pessoal, determinada pelo titular.
- O **smart card** é uma espécie de cartão magnético e depende de um aparelho leitor para funcionar.
- **Já o token** funciona como um pen drive que pode ser inserido diretamente na entrada USB do dispositivo do usuário.



4.7-Criptografia e Certificado Digital

- **Que cuidados devo tomar ao utilizar um certificado digital?**
- "Primeiramente, lembre-se que o certificado digital representa a sua 'identidade' no mundo virtual".
- Por isso, se você não seguir recomendações simples, como não compartilhar a senha, poderá permitir que outra pessoa utilize essa identificação para fechar negócios ou realizar transações bancárias, por exemplo, sem a sua autorização.

