**Universidade São Judas Tadeu - Mooca**

**Aplicações na área de Sistemas computacionais e segurança**

**Henrique Rosa da Silva - RA: 82518188**  
  
**Gabriel Luiz Vicente Soares - RA: 825150671**  
  
**Vítor de Souza Devicari - RA: 825139110**  
  
**Vitor Bernardes - RA: 825138944**  
  
**Felipe Honorio de Sousa – RA: 825134274**

**São Paulo**

**2025**

**Criptografia para empresas**

 Importância da criptografia no ambiente profissional.

O que é a criptografia? É um processo de proteção de dados transformando-os em um código secreto, só podendo ser decodificado com uma chave digital.

 Amplamente utilizada em diversas áreas, incluindo:

  Comunicações Seguras: Proteção de e-mails, mensagens e chamadas de voz;

  Transações Financeiras: Garantindo a segurança de pagamentos online e dados bancários;

 Armazenamento de Dados: Proteção de informações sensíveis em bancos de dados e dispositivo;

 Autenticação: Utilizada em sistemas de autenticação para verificar a identidade de usuários.

 Tipos de criptografia: Simétrica (Mesma chave utilizada para codificar e decodificar a informação, chave compartilhada por pessoas autorizadas tornando-as privadas) assimétrica (Duas chaves sendo uma pública e outra privada, sendo a privada conhecida apenas por quem a criou).

**Autenticação Multifator (MFA)**

A Autenticação Multifator (MFA) é um método de segurança utilizado para proteger acessos a sistemas, redes e dispositivos. Ela exige que o usuário forneça mais de um fator de autenticação, garantindo uma camada extra de proteção contra acessos não autorizados. Essa tecnologia é amplamente usada em bancos, redes corporativas e serviços online para dificultar ataques baseados em roubo de credenciais.

A verificação em duas etapas é um recurso opcional oferecido por diversos serviços de Internet, como webmail, redes sociais, Internet Banking e de armazenamento em nuvem. Ao habilitá-la você estará aumentando a segurança de sua conta e, caso não deseje mais utilizá-la, basta que você a desabilite.

O tipo de verificação usado pode variar de acordo com o serviço acessado mas, por facilidade, a maioria costuma utilizar-se de algo que apenas você sabe ou possui.

Existem diferentes tipos de autenticação multifator, alguns dos mais comuns são:

* Código de verificação: é um código gerado para aplicativos que não suportam a verificação em duas etapas;
* Token gerador de senhas: é um tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade;
* Cartão de segurança: é um cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta;
* Lista de códigos reserva/backup: é uma lista de códigos que devem ser usados de forma sequencial e uma única vez;
* Chave de recuperação: é um número gerado pelo serviço quando você ativa a verificação em duas etapas. Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis;
* Dispositivo confiável (ou de confiança): é um computador ou dispositivo móvel que você frequentemente usa para acessar suas contas.
* Biometria: A autenticação biométrica utiliza características físicas do usuário, como impressão digital, reconhecimento facial ou leitura da íris, para garantir um acesso seguro. Esse método é amplamente usado em smartphones e bancos, pois a biometria é única para cada indivíduo e dificilmente pode ser falsificada.

**Backup de Dados**

Os backups são indispensáveis para assegurar a integridade e a recuperação das informações em virtude de falhas, ataques cibernéticos ou desastres, e para tal, devem ser adotadas estratégias que assegurem a disponibilidade dos dados.

Os principais tipos de backup são o total (cópia total dos dados), incremental (salva somente as alterações a partir do último backup) e diferencial (copia as alterações a partir do último backup total). A regra 3-2-1 é de extrema importância: mantenha três cópias dos dados, armazenadas em dois suportes de mídia diferentes e uma delas deve estar externamente, tal como a nuvem.

A segurança dos backups deve ser assegurada, implementando criptografia, controle de acesso e isolamento de cópias para evitar perdas por ransomwares. O tempo da realização dos backups deve ser definido em função da criticidade da informação, sendo realizada na frequência de diária, semanal e mensal.

Além disso, automatizar backups e realizar testes periódicos de recuperação se fazem essenciais para a garantia de que os dados possam ser recuperados de modo correto no caso da necessidade. Seguir essas práticas conservará a continuidade dos negócios e a proteção contra a perda irrecuperável.

**Ataques Cibernético**

Os ataques cibernéticos são tentativas de invadir dispositivos ou redes conectadas para roubar, prejudicar ou expor dados. Os tipos mais comuns de ataques cibernéticos são:

Phishing: Enganar pessoas para que compartilhem senhas ou dados financeiros, geralmente via e-mails falsos.

Malware: Programas maliciosos como vírus, worms e trojans, usados para roubar ou danificar dados.

Engenharia Social: Manipulação psicológica para obter informações confidenciais.

DDoS: Ataques que sobrecarregam servidores, tornando serviços indisponíveis.

Biometria

A Biometria, é um tipo fator de segurança usado em diversos aspectos, desde a segurança do desbloqueio do seu celular, até a segurança ao seu banco, existem muitos tipos de biometria, um deles é a

Biometria Facial: A biometria por reconhecimento facial identifica os traços físicos da pessoa, mapeando a sua estrutura facial em 3D ou 2D. Ao longo dos anos, ou após procedimentos estéticos e intervenções cirúrgicas, a fisionomia do indivíduo pode mudar, o que atrapalha o funcionamento do sistema. Além disso, também há um risco de segurança considerando a semelhança entre algumas pessoas, como acontece com irmãos gêmeos.

Íris: O reconhecimento de íris é um dos métodos de biometria mais seguros e um dos mais caros do mercado. Esse sistema consiste na leitura da íris da pessoa a parte colorida do olho humano, por onde a luz, que é única para cada indivíduo e não se modifica com o passar dos anos.

Impressão Digital: Atualmente, a leitura de impressão digital é o sistema de biometria mais utilizado. Ele tem um baixo custo de implementação um dos menores dessa lista e é altamente confiável, uma vez que as digitais de cada pessoa são únicas e não se alteram ao longo da vida. A única possibilidade de erro é caso o indivíduo perca a digital por algum motivo. Esse sistema é muito utilizado para desbloquear smartphones, permitir acesso a escolas e faculdades, e durante o processo eleitoral no Brasil.

Também é encontrado em bancos, além de permitir a validação em assinaturas e certificados.

Além dessas, existem diversos outros tipos de biometria, mas essas, sendo as principais.