

## re\_s28\_A1\_SL08\_redes\_segurança

### Entrega no AVA

Nome: \_\_\_\_\_ Turma: \_\_\_\_\_

## **Atividade 1 : Fortalecendo a segurança das contas on-line**

### **Objetivos**

Como parte dos esforços contínuos para fortalecer a segurança da nossa empresa, vamos realizar uma atividade prática para destacar a importância de senhas fortes na proteção das contas on-line.

### **Lista de materiais**

- Computador com internet;
- Caderno para anotações;
- Uma caneta.

Como parte do treinamento de segurança da informação, é importante que todos os colaboradores compreendam a importância de ter senhas fortes para proteger suas contas on-line. Senhas fracas podem resultar em violações de segurança e comprometer a integridade dos nossos dados.

Cada colaborador será solicitado a criar senhas fortes para suas contas on-line. Eles devem seguir as diretrizes fornecidas pela equipe de segurança da informação, incluindo o uso de pelo menos 12 caracteres, uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais, e evitar o uso de informações pessoais óbvias.

Deverá testar a sua senha em <https://testedesenha.com.br/> e registrar a cópia da tela mostrando que a senha é confiável.

Após testar a senha, faça o registro no AVA sobre quantas tentativas você precisou realizar até obter uma senha que contemplasse todas as diretrizes necessárias de segurança e qual foi a sua maior dificuldade durante esse processo.

**\*Tire um print ou foto da tela para enviar pelo AVA**

## **Atividade 2: Configurando a Autenticação Multifator (MFA)**

### **Objetivos**

Configurar a autenticação multifator (MFA) com o Google Authenticator.

**Tempo estimado:** 25 minutos.

### **Lista de materiais**

- Computador com internet;
- Caderno para anotações;
- Uma caneta.

#### **Passo 1: Acesse as Configurações de Segurança do Google:**

1. Faça log in na sua conta do Google.
2. Clique na sua foto de perfil no canto superior direito e selecione “Gerenciar sua Conta Google”.
3. No painel lateral esquerdo, clique em “Segurança”.

#### **Passo 2: Ative a verificação em duas etapas:**

1. Em “Verificação em duas etapas”, clique em “Configurar”.
2. Siga as instruções na tela para confirmar sua identidade, geralmente fornecendo sua senha novamente.
3. Escolha o método de verificação “Aplicativo Authenticator” e clique em “Próximo”.

#### **Passo 3: Configure o Google Authenticator:**

1. Abra o Google Authenticator no seu dispositivo móvel.
2. Toque em “+”, geralmente localizado no canto superior direito, e selecione “Ler código de barras”.

3. Use a câmera do seu dispositivo para escanear o código QR exibido na tela do seu computador.
4. Se preferir, você também pode inserir manualmente o código de 16 dígitos exibido abaixo do código QR.

#### **Passo 4: Verifique sua configuração:**

1. Após escanear o código QR ou inserir manualmente o código, o Google Authenticator começará a gerar códigos de verificação de seis dígitos.
2. Insira um código de verificação gerado pelo Google Authenticator para verificar que a configuração está funcionando corretamente.
3. Clique em “Salvar” ou “Concluir” para confirmar a configuração.

#### **Passo 5: Guarde códigos de backup (opcional):**

1. O Google fornecerá códigos de backup que você pode usar para acessar sua conta se não puder acessar seu dispositivo móvel.
2. Anote esses códigos e guarde-os em um local seguro. Eles são únicos e só podem ser usados uma vez cada.

#### **Passo 6: Conclua a configuração:**

1. Após configurar com sucesso a autenticação em duas etapas com o Google Authenticator, clique em “Concluído” ou “Ativar” para finalizar o processo.
2. Você pode optar por receber alertas de segurança adicionais por e-mail ou SMS, se desejar.

Agora, sempre que você fizer log in na sua conta do Google, será solicitado a fornecer seu nome de usuário e senha padrão, seguidos de um código de verificação gerado pelo Google Authenticator no seu dispositivo móvel. Essa camada adicional de segurança ajudará a proteger sua conta contra acesso não autorizado.

**\*Tire um print ou foto da tela para enviar pelo AVA**