Cartilha de Boas Práticas para você

Para garantir a segurança da informação na nossa cooperativa bancária, todos os colaboradores devem estar cientes das melhores práticas de segurança de acesso. Esta cartilha visa orientá-los sobre como proteger nossas informações e sistemas, mantendo um ambiente seguro para todos

ATENÇÃO!

Senhas Seguras

Criação de Senhas

- Senhas com, no mínimo, 8 caracteres.
- Combine letras maiúsculas e minúsculas, números e caracteres especiais.
- Evite usar informações pessoais, como datas de nascimento ou nomes.
- Não reutilize senhas antigas.

Manutenção de Senhas

- Altere suas senhas regularmente, pelo menos a cada 90 dias.
- Não compartilhe suas senhas com ninguém, nem mesmo com colegas de trabalho.
- Nunca escreva suas senhas em locais visíveis ou de fácil acesso.

Computadores e Laptops

- Bloqueie a tela do seu computador quando estiver ausente, mesmo que por pouco tempo.
- Utilize apenas dispositivos autorizados e fornecidos pela CredUai.
- Mantenha seu sistema operacional e todos os softwares atualizados.

Dispositivos Móveis

- Utilize senhas ou métodos de autenticação biométrica para desbloquear dispositivos móveis.
- Evite conectar dispositivos móveis a redes Wi-Fi públicas ou não confiáveis.
- Em caso de perda ou roubo do dispositivo, informe imediatamente departamento de TI.

Acesso ao Sistemas

Autenticação Multifator

- Ative e utilize a autenticação multifator (MFA) para acessar sistemas críticos.

Sessões de Trabalho

- Sempre faça logout de sistemas e aplicações ao final do expediente ou quando não estiver utilizando-os.
- Não permita que outras pessoas utilizem suas credenciais de acesso.

Armazenamento de Dados

- Armazene dados sensíveis apenas em locais seguros e autorizados.
- Utilize criptografia para proteger informações confidenciais.

Transferência de Dados

- Use métodos seguros para transferir dados, como redes privadas ou serviços de transferência criptografados.
- Evite enviar informações sensíveis por e-mail ou outros meios não seguros.

Sites Confiáveis

- Acesse apenas sites confiáveis e necessários para o trabalho.
- Verifique se o site usa HTTPS antes de inserir informações confidenciais.
- Utilize a VPN da CredUai ao acessar a internet em redes Wi-Fi públicas ou domésticas.
- Mantenha o software da VPN sempre atualizado para garantir máxima proteção.

Downloads e Instalações

- Não baixe ou instale softwares sem a autorização do departamento de TI.
- Evite clicar em links suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.

E-mails Suspeitos

- Desconfie de e-mails inesperados ou de remetentes desconhecidos, especialmente se contiverem links ou anexos.
- Verifique o endereço de e-mail do remetente e busque por sinais de phishing, como erros gramaticais ou solicitações de informações confidenciais.

Boas Práticas

- Não envie informações sensíveis por e-mail sem a devida proteção, como criptografia.
- Utilize a assinatura de e-mail padrão da CredUai para todas as comunicações oficiais.

Treinamentos

- Participe de todos os treinamentos sobre segurança da informação oferecidos pela CredUai.
- Mantenha-se atualizado sobre as melhores práticas de segurança.

Relato de Incidentes

- Relate imediatamente qualquer incidente de segurança ou atividade suspeita ao Comitê de Segurança da Informação (CSI).
- Utilize os canais de comunicação estabelecidos para reportar incidentes.

Responsabilidades do Colaborador

- Siga todas as diretrizes e práticas desta cartilha.
- Seja vigilante e proativo na proteção das informações e sistemas da CredUai.
- Contribua para um ambiente seguro, reportando qualquer situação que comprometa a segurança da informação.

Em um ambiente bancário, a segurança da informação é fundamental. Proteja dados confidenciais e evite compartilhá-los sem autorização para garantir a integridade e a confiança dos nossos clientes.

CredUai
COOPERATIVA BANCÁRIA
(31) 3456-7890
Cede: Rua Alegre, 123 - Cidade Barbacena

Diretrizes Gerais

Confidencialidade

- ***Controle de Acesso:*** O acesso às informações deve ser restrito apenas aos indivíduos autorizados, com base nas suas funções e responsabilidades. Todos os acessos dos colaboradores devem ser identificáveis e únicos, garantindo assim a qualificação de cada um como responsável pelas atividades realizadas.

- ***Classificação da Informação:*** As informações devem ser classificadas de acordo com seu grau de sensibilidade e importância, e tratadas conforme as normas estabelecidas para cada categoria.

***1.* PRIVADOS:** *Documentos que forem relacionados aos clientes, bem como informações confidenciais, serão classificados como PRIVADOS, onde somente pessoal autorizado terá acesso e não deverá ser divulgado publicamente.*

2. RESTRITOS: Documentos relacionados a informações críticas, estratégicas e financeiras, documentos de compliance e auditoria, planos de segurança da informação e recuperação de desastres, detalhes sobre novos produtos e serviços antes do lançamento, informações sobre a infraestrutura de T.I e segurança, serão classificados como RESTRITOS, onde somente executivos de alto nível e membros do conselho e funcionários de departamentos específicos e de auditoria.

***3.* PÚBLICOS:** *Documentos de cunho informativo, bem como esta Política da Segurança da Informação, serão classificados como PÚBLICOS e todos terão acesso.*

Integridade

- **Controle de Alterações:** Qualquer modificação nas informações deve ser registrada e auditável para garantir a rastreabilidade.
- **Proteção contra Malware:** Todos os sistemas e dispositivos devem estar protegidos contra vírus, malware e outras ameaças que possam comprometer a integridade das informações.

Disponibilidade

- **Plano de Continuidade de Negócios:** Deve ser mantido um plano de continuidade de negócios para garantir que as operações possam ser retomadas rapidamente em caso de interrupção.

- **Backup:** As informações críticas devem ser regularmente copiadas e armazenadas em locais seguros para garantir a recuperação em caso de perda de dados.

Conformidade

- Cumprir todas as leis, regulamentos e normas aplicáveis relacionadas à segurança da informação e à Lei Geral de Proteção de Dados (LGPD).

CredUai
COOPERATIVA BANCÁRIA
(31) 3456-7890
Cede: Rua Alegre, 123 - Cidade Barbacena