TREINAMENTO DE SEGURANÇA DA INFORMAÇÃO

Pelo Parceiro e Substabelecido
da CREDLEVE

Sumário

Objetivo

- A informação é um ativo crítico e precisa ser protegida contra ameaças e vulnerabilidades, garantindo segurança, integridade, confidencialidade, disponibilidade e autenticidade.

- Base Normativa: Este documento é baseado na norma internacional ABNT NBR ISO/IEC 27002:2022.

- Objetivo Principal: Disciplinar o uso da tecnologia da informação, orientando todos os colaboradores sobre condutas e procedimentos seguros dentro da CREDFRANCO

Abrangência

- Abrangência: Aplica-se a qualquer colaborador, parceiro ou substabelecido que tenha acesso às informações da empresa.

- Propriedade: Toda informação produzida ou recebida na atividade profissional pertence exclusivamente à CREDLEVE.

- Ciência de Monitoramento: Todos ficam cientes de que sistemas, computadores e redes poderão ser monitorados (com prévia informação).

- Implicações Legais: Divulgar informações estratégicas ou confidenciais sem autorização configura crime previsto nas leis de propriedade intelectual e industrial.

RESPONSABILIDADES DOS USUÁRIOS

Assinar o Termo de Compromisso, Sigilo e Confidencialidade e o Termo de Responsabilidade

Responder pela guarda, proteção e uso exclusivo/intransferível de suas senhas de acesso.
Garantir cuidados de segurança ao trabalhar
Relatar prontamente à TI qualquer fato, ameaça, vírus ou quebra de segurança identificada.

Responsabilidades
E PAPÉIS DA ÁREA DE TI

Revisão de Credenciais: Efetua a revisão periódica das credenciais de acesso a cada 90 dias, barrando usuários duplicados.

- Backups e Auditorias: Administra e testa cópias de segurança de dados e gera trilhas de auditoria detalhadas para rastrear falhas ou fraudes.

- Monitoramento Ativo: Implementa sistemas para monitorar estações de trabalho, e-mails, acessos à internet e uploads/downloads.

- Bloqueio Imediato: Garante a exclusão e o bloqueio de acessos do usuário assim que solicitado o desligamento do colaborador.

REGRAS CRIAÇÃO DE SENHAS:

1

Troca Obrigatória: A alteração de senha é exigida mensalmente (a cada mês) para quem utiliza computadores.

Bloqueio Automático: A credencial é bloqueada após 3 tentativas sem sucesso, exigindo contato com a TI para o desbloqueio

Regras de Criação: Mínimo de 8 caracteres, misturando maiúsculas, minúsculas, números e caracteres especiais.

O que Evitar: É proibido usar informações pessoais óbvias, nomes próprios, repetições de dígitos ou palavras de dicionário.

Contas Genéricas: São totalmente proibidas no ambiente corporativo (salvo contas de serviço previamente documentadas).

2

Telas, mesas limpas e descarte de dados

Computador Monitorado: O papel de parede e proteção de tela devem seguir o padrão corporativo, e as máquinas devem ser bloqueadas ao se ausentar.

Stand-by Efêmero: Se o computador ficar ocioso por mais de 1 minuto, a sessão é finalizada e exigirá login novamente.

Eliminação de Dados: Dados pessoais e contratos são eliminados definitivamente dos servidores por meio de um sistema automatizado executado em todos os primeiros sábados de cada mês, às 08:00.

Sigilo e Confidencialidade

Classificação de Dados: As informações internas são classificadas pelos gestores como Públicas, Confidenciais ou Internas.

Uso Restrito: Toda informação compartilhada no trabalho é considerada confidencial por padrão e de propriedade da empresa.

Vigência: O dever de sigilo e as obrigações de confidencialidade continuam válidos mesmo após o desligamento do colaborador.

Cópia Proibida: É vedada a criação de backups pessoais de dados confidenciais ou o armazenamento em nuvens não corporativas (como OneDrive pessoal ou Dropbox).

Regras de e-mail e mensagens

Foco Profissional: O e-mail (@credleve.com.br) e aplicativos de mensagens são de uso exclusivamente profissional.

Proibições no E-mail: É proibido enviar correntes, pirâmides, spam, malas diretas ou usar o e-mail em cadastros de redes sociais e sites de compras.

Aplicativos (WhatsApp/Telegram): Devem ser usados para fins corporativos apenas quando necessário. Assuntos relevantes, sigilosos ou confidenciais não podem ser tratados por esses apps.

Preferência Corporativa: A empresa estabelece o uso do Google Chat para interações internas diárias

Uso da Internet, Softwares e Penalidades

Internet: O uso pessoal é permitido, desde que feito com parcimônia e sem prejudicar as atividades de trabalho.

Jogos e Pirataria: Jogos eletrônicos de qualquer tipo e a instalação de softwares piratas/não homologados são terminantemente proibidos.

Consequências Disciplinares: Práticas que ameacem a segurança cibernética geram penalidades que variam desde advertência verbal até a rescisão por justa causa (nos termos do art. 482 da CLT), sem prejuízo de processos civis e criminais.