



CallNet Solutions

Objetivo

Esta Cartilha visa fornecer um guia rápido e essencial sobre as boas práticas de segurança da informação na CallNet Solutions. Nosso objetivo é capacitar cada colaborador a proteger nossos dados e sistemas, garantindo a confidencialidade, integridade e disponibilidade das informações, e contribuindo para um ambiente de trabalho seguro.

Penalidades

Leve: Advertência e treinamento.

Média: Suspensão de acessos.

Grave: Demissão por justa causa e/ou ações judiciais.

Princípios básicos

A segurança da informação na CallNet Solutions é fundamentada nos seguintes princípios, que todos devemos seguir:

- **Confidencialidade:** Assegurar que as informações sensíveis sejam acessíveis apenas por pessoas autorizadas.
- **Integridade:** Garantir que os dados sejam precisos, completos e protegidos contra modificações não autorizadas.
- **Disponibilidade:** Assegurar que os sistemas e informações críticas estejam acessíveis aos usuários autorizados sempre que necessário.
- **Conformidade:** Cumprir todas as leis, regulamentações e políticas internas.
- **Responsabilidade:** Todos são responsáveis por compreender e seguir as diretrizes de segurança.



Regras Gerais e Boas práticas

- Use senhas fortes, únicas e mude a cada 90 dias.
- Nunca compartilhe suas senhas; use gerenciador se precisar.
- Sempre acesse a rede via VPN, especialmente em redes públicas.
- Bloqueie o computador ao se afastar.
- Instale só softwares autorizados e cheque dispositivos externos com antivírus.
- Cuidado com e-mails suspeitos: não clique em links ou abra anexos duvidosos; reporte para TI.
- Mantenha antivírus ativo e atualizado, faça varreduras regulares.
- Proteja informações confidenciais, descarte documentos com triturador.
- Avise TI se notar algo estranho.

Incidentes de Segurança

- **Perda ou roubo de equipamentos:**

Comunique imediatamente a TI e registre BO (se necessário).

- **Vazamento de dados:**

Notifique a Gerência de TI e o Comitê de Segurança.

- **Vazamento de dados:**

Desconecte o dispositivo da rede e avise a TI.

- **Testes sem autorização:**

Proibido realizar testes de vulnerabilidade sem autorização.

Responsabilidades

- **Colaboradores:**

- Cumprir a PSI e relatar violações.
- Assinar o Termo de Ciência e Responsabilidade.

- **Equipe de TI:**

- Monitorar sistemas e bloquear acessos suspeitos.
- Garantir backups e atualizações de segurança.

- **Prestador de Serviço:**

- Seguir as mesmas regras dos colaboradores.
- Devolver os equipamentos ao término do contrato.

Contatos Importantes

Suporte TI:

- suporteti@callnet.com.br
- (31) 0000-0000

Comitê de Segurança:

comite.seguranca@callnet.com.br

