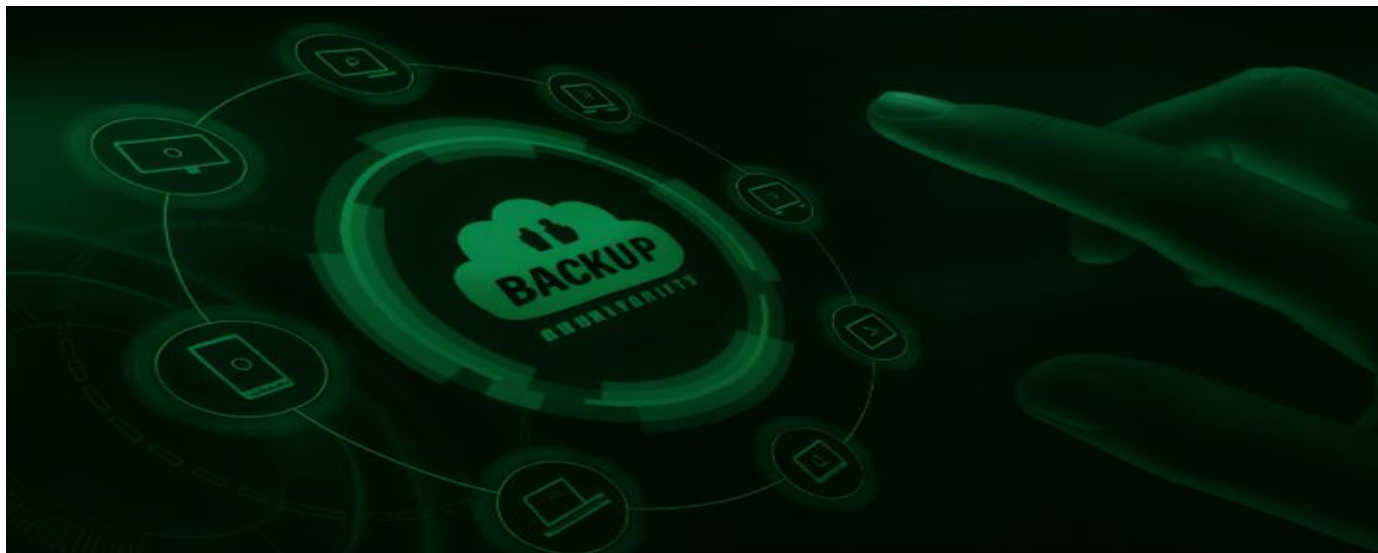


CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



NESTA EDIÇÃO

RECUPERAÇÃO DE DADOS

- Por que é importante?
- Boas Práticas

RECUPERAÇÃO DE DADOS

- O que é ?
- Ameaças comuns
- Sinais de Alertas
- O que fazer?
- Boas Práticas

CONCLUSÃO

Você sabia que falhas de armazenamento e exclusões acidentais são as principais portas de entrada para ataques cibernéticos?

Neste volume, vamos mostrar como proteger sua empresa adotando boas práticas de recuperação de dados.

Recuperação de Dados

A recuperação de dados é um pilar fundamental da segurança digital, tanto para usuários quanto para empresas. Esses ambientes são alvos frequentes de cibercriminosos, que empregam técnicas como phishing, malware e sites falsos para roubar informações sensíveis ou comprometer sistemas.

Por que é importante?

- 🔒 Garantia de continuidade dos negócios após falhas ou ataques
- 📁 Recuperação de arquivos excluídos acidentalmente ou corrompidos
- 📋 Conformidade com normas de proteção e retenção de dados
- 💰 Redução de impactos financeiros e operacionais em caso de perda de dados

Boas Práticas:

- ✓ Tenha uma política clara de backup e recuperação;
- ✓ Teste periodicamente os backups;
- ✓ Armazene dados críticos em locais seguros;
- ✓ Eduque os usuários sobre boas práticas de armazenamento.

Recuperação de Dados

O que é ?

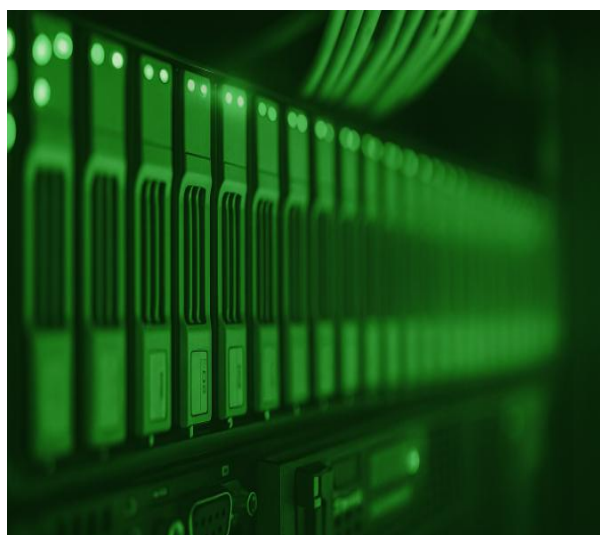
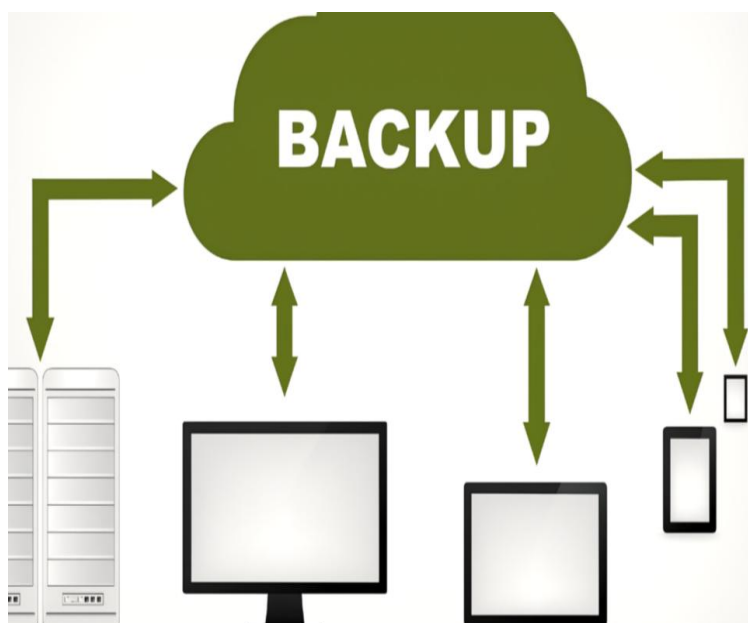
Recuperação de Dados é um conjunto de práticas e tecnologias voltadas à proteção e restauração de informações armazenadas em sistemas e bancos de dados. Seu principal objetivo é garantir a continuidade dos negócios e a integridade dos dados, mesmo diante de falhas, ataques cibernéticos ou desastres.

⚠ Ameaças comuns:

- 🔌 Falhas de hardware ou software;
- 🔗 Links de phishing em mensagens e redes sociais;
- 🌐 Erros humanos como exclusão acidental;
- 🗑️ Corrupção de arquivos.

🔍 Sinais de alerta:

- 🗂️ Arquivos ou pastas desaparecendo repentinamente;
- 🌐 Mensagens de erro ao acessar arquivos;
- 🛑 Sistema travando ou reiniciando sem motivo;
- 📁 Perda de acesso a dados importantes.



📌 O que fazer:

- 🔌 Pare de usar o dispositivo imediatamente;
- 📞 Comunique o time de TI ou suporte técnico;
- 📝 Anote o que aconteceu e quando.

✅ Boas Práticas:

- 🔒 Mantenha backups atualizados regularmente;
- 🛠️ Utilize ferramentas de recuperação confiáveis;
- 🌐 Evite sobrescrever dados perdidos;
- 👤 Considere serviços profissionais de recuperação de dados.

Conclusão

Manter os sistemas atualizados e seguir boas práticas de segurança não é apenas uma recomendação — é uma necessidade. Em um cenário onde as ameaças digitais evoluem constantemente, a prevenção se torna a melhor defesa. Cada colaborador tem um papel fundamental na proteção dos dados da empresa. Ao adotar atitudes proativas, como atualizar softwares, realizar backups e reportar comportamentos suspeitos, contribuímos para um ambiente digital mais seguro e resiliente. Lembre-se: em caso de dúvida, procure sempre o time de TI ou Segurança da Informação. Fiquem atentos aos próximos boletins para mais dicas!