Sistema de Gestão da Segurança da Informação (SGSI)

1. Política de Segurança da Informação

• Estabelecer diretrizes de proteção de dados, sistemas e ativos digitais.
• Aprovação e divulgação pela diretoria.
• Revisão anual ou em caso de mudanças críticas.

2. Escopo

Aplica-se a:
• Servidores em nuvem
• Sistema de backup automatizado
• Plataforma de Desktop Virtual
• Infraestrutura de rede, data center e suporte
• Todos os colaboradores, parceiros e fornecedores que tenham acesso aos ativos da empresa.

3. Gestão de Riscos

Metodologia baseada em ISO 27005:
1. Identificação de ativos críticos (servidores, bancos de dados, credenciais, clientes).
2. Identificação de ameaças (malware, ransomware, falhas humanas, ataques internos, falhas físicas).
3. Avaliação de vulnerabilidades.
4. Cálculo de impacto e probabilidade.
5. Plano de tratamento de riscos (aceitar, mitigar, transferir ou eliminar).

4. Controles de Segurança (ISO 27001 Anexo A)

• Controle de Acesso: autenticação multifator, segregação de funções, gestão de senhas.
• Segurança Física: acesso restrito ao data center, monitoramento por CFTV, alarmes.
• Segurança de Redes: firewall, IDS/IPS, VPN para acesso remoto.
• Gestão de Logs: auditoria e monitoramento contínuo.
• Treinamento e Conscientização: capacitação periódica contra phishing e engenharia social.
• Gestão de Backup: testes regulares de restauração, replicação geográfica.
• Gestão de Fornecedores: cláusulas contratuais de segurança e confidencialidade.

5. Plano de Continuidade e Recuperação de Desastres

• Integrado ao Plano de Continuidade de Negócios.
• RTO (tempo máximo de recuperação) definido para cada serviço.
• RPO (ponto de recuperação de dados) alinhado com necessidades de clientes.

6. Governança e Responsabilidades

• Diretoria: aprovar políticas e prover recursos.
• Gestor de Segurança (CISO): liderar implementação do SGSI.
• Equipe Técnica: aplicar controles e monitoramento.
• Colaboradores: cumprir normas de segurança.

7. Ciclo PDCA (Melhoria Contínua)

• Planejar (Plan): definir políticas e riscos.
• Executar (Do): aplicar controles.
• Checar (Check): auditorias internas, KPIs de segurança.
• Agir (Act): melhorias contínuas e correções.

8. Indicadores de Segurança (KPIs)

• % de incidentes resolvidos dentro do SLA.
• Taxa de sucesso em testes de backup e restauração.
• Número de tentativas de intrusão detectadas.
• % de colaboradores treinados em segurança.

9. Documentação do SGSI

• Política de Segurança
• Procedimentos de controle de acesso
• Plano de Resposta a Incidentes
• Relatórios de auditoria
• Plano de Continuidade e Recuperação

10. Conclusão

A implantação do SGSI assegura:

✅ Proteção dos ativos digitais
✅ Conformidade com normas internacionais (ISO 27001)
✅ Confiança dos clientes em soluções de servidores, backup e desktop virtual
✅ Resiliência contra ataques e falhas críticas