Escopo Proposto – Programa Cybersecurity

1. Desenvolvimento de políticas e procedimentos de segurança
   - O que é: Criação de normas internas (acesso, backup, uso de e-mail, classificação de dados, etc.).
   - Valor: Estabelece regras claras de segurança alinhadas ao negócio.
   - Resultado: Conjunto de documentos normativos aprovados pela direção.
2. Mapeamento e gestão de riscos de segurança da informação
   - O que é: Identificação contínua, análise e tratamento dos riscos relacionados à informação.
   - Valor: Ajuda a manter o SGSI em conformidade com a ISO 27001.
   - Resultado: Registro atualizado de riscos, controles aplicados e responsáveis.
3. Implementação de governança (Baseado em ISO 27001, NIST, COBIT, etc.)
   - O que é: Estruturação de controles e processos de acordo com frameworks reconhecidos.
   - Valor: Maior confiança do mercado, compliance e resiliência.
   - Resultado: Programa de segurança alinhado às normas, pronto para auditoria.
4. Gestão de identidade e acesso (IAM)
   - O que é: Implementação de políticas e soluções de autenticação, autorização e provisionamento de usuários.
   - Valor: Reduz riscos de acessos indevidos.
   - Resultado: Controle centralizado de identidades, logs de auditoria e menor exposição a ataques internos.
5. Implementação de firewalls, antivírus e soluções de EDR/XDR
   - O que é: Implantação e configuração de ferramentas de defesa perimetral e de endpoints.
   - Valor: Aumenta a capacidade de detecção e resposta a ataques.
   - Resultado: Camada de proteção ativa contra ameaças conhecidas e avançadas.
6. Soluções de DLP (Data Loss Prevention)
   - O que é: Monitoramento e bloqueio de movimentações não autorizadas de dados sensíveis.
   - Valor: Protege contra vazamento de informações críticas.
   - Resultado: Relatórios de tentativas de exfiltração e controles preventivos aplicados.
7. Segmentação de rede e proteção de endpoints
   - O que é: Divisão lógica da rede e aplicação de controles de segurança em dispositivos.
   - Valor: Minimiza superfícies de ataque e dificulta movimentação lateral do invasor.
   - Resultado: Arquitetura de rede mais segura e endpoints protegidos.
8. Treinamentos de segurança da informação para usuários
   - O que é: Capacitação contínua sobre boas práticas de segurança.
   - Valor: Reduz falhas humanas, que são a principal causa de incidentes.
   - Resultado: Colaboradores mais conscientes e preparados.
9. Simulações de phishing e campanhas de conscientização
   - O que é: Testes práticos de engenharia social e campanhas educativas.
   - Valor: Mede o nível de vulnerabilidade dos usuários e aumenta a resiliência contra golpes.
   - Resultado: Relatórios de taxa de cliques e melhorias após treinamentos.

Escopo Proposto – Gestão de TI (ITSM) & Helpdesk

1. Atendimento ao Usuário (Helpdesk & Suporte Técnico)
   - Central de atendimento multicanal (telefone, e-mail, Whatsapp).
   - Atendimento VIP com prioridade a executivos e áreas críticas.
   - Horários diferenciados / plantão estendido (opcional 24x7), se necessário.
   - Suporte remoto e presencial conforme criticidade.

- Atendimento a incidentes, requisições e dúvidas operacionais.
- SLA definido por criticidade (ex.: resposta em até 15 min para criticidade alta).

2. Gestão Ativa de TI (ITSM)
   - Adoção de ITIL/ITSM como boas práticas de gestão.
   - Gestão de incidentes, problemas, requisições e mudanças.
   - Abertura, acompanhamento e resolução via ferramenta de chamados (ticketing).
   - Registro de base de conhecimento (FAQs, how-to, KB, soluções).
   - Gestão de acessos: provisionamento/desprovisionamento de usuários, desligamentos, revisões periódicas de permissões.
3. Gestão de Ativos e Licenciamento
   - Inventário de hardware e software atualizado.
   - Controle de licenciamento de softwares (Microsoft, antivírus, etc).
   - Planejamento de renovação e aquisições de software.
4. Gestão de Fornecedores de TI
   - Gestão de contratos de outsourcing (impressoras, links de internet, data centers, cloud, etc).
   - Monitoramento de SLA de terceiros (tempo de reparo, disponibilidade de link).
   - Mediação entre cliente e fornecedores em caso de incidentes.
5. Governança e Políticas de TI
   - Criação e revisão de políticas de segurança da informação (senhas, backup, uso de e-mail, etc).
   - Definição de normas para acesso remoto e BYOD (Bring Your Own Device).
   - Revisão periódica das políticas de backup, disaster recovery e PCN (plano de continuidade de negócios).
6. Manutenções Preventivas e Monitoramento
   - Verificação periódica de computadores, rede, no-breaks, servidores.
   - Atualizações de sistemas operacionais e aplicações críticas.
   - Monitoramento proativo de disponibilidade e performance de rede/servidores.
   - Testes regulares de restore de backup.
   - Inspeções físicas e lógicas de infraestrutura.