Documento de Políticas de Gestão Operacional

Grupo Syscamp

Área de Atuação: Segurança Eletrônica

1. Política de Risco Operacional

1.1. Objetivo

Garantir a identificação, avaliação e mitigação de riscos operacionais associados à prestação de serviços de segurança eletrônica.

1.2. Escopo

Aplicável a todos os colaboradores, parceiros e fornecedores envolvidos na prestação de serviços de segurança eletrônica, abrangendo monitoramento, instalação e manutenção de sistemas de segurança.

1.3. Diretrizes

- Identificação de Riscos: Mapear possíveis falhas operacionais que possam comprometer a entrega de serviços de segurança.
- Controles e Mitigação: Implementar medidas para minimizar riscos relacionados a sistemas de vigilância, alarmes e monitoramento.
- Monitoramento Contínuo: Revisar e monitorar regularmente os controles para garantir sua eficácia.

1.4. Responsabilidades

- Gestores de Risco: Responsáveis por garantir que os riscos sejam monitorados e mitigados.
- Colaboradores e Parceiros: Devem cumprir as orientações e reportar quaisquer falhas ou riscos identificados.

2. Plano de Continuidade Operacional (PCO)

2.1. Objetivo

Assegurar que a operação dos sistemas de segurança eletrônica permaneça ativa em situações de interrupção ou falha.

2.2. Escopo

Aplicável aos serviços críticos de segurança, como monitoramento de câmeras, sistemas de alarme e resposta a emergências.

2.3. Componentes do PCO

- Análise de Impacto nos Negócios (BIA): Avaliar como a interrupção de serviços de segurança afeta clientes e operações.
- Planos de Contingência: Incluir backups de dados de monitoramento e redundâncias nos sistemas de alarme e resposta.
- Ações de Emergência: Procedimentos claros para a manutenção de serviços em caso de falhas de energia, ataques cibernéticos ou desastres naturais.

2.4. Testes e Manutenção

- Realizar simulações periódicas para testar a eficácia dos sistemas de backup e de resposta emergencial.

3. Política de Gestão de Incidentes

3.1. Objetivo

Estabelecer um processo eficaz para identificar, gerenciar e resolver incidentes que possam comprometer a segurança eletrônica dos clientes.

3.2. Escopo

Aplica-se a incidentes que afetem o funcionamento de sistemas de monitoramento, alarmes, controle de acesso e outros serviços de segurança eletrônica.

3.3. Processo de Gestão de Incidentes

- Relato e Registro de Incidentes: Qualquer problema nos sistemas deve ser reportado imediatamente através de nosso canal de suporte.
- Classificação e Priorização: Incidentes são classificados como críticos, altos, médios ou baixos, de acordo com o impacto sobre a segurança do cliente.
- Investigação e Resolução: A equipe de suporte técnico inicia a resolução assim que o incidente é identificado, garantindo a rápida restauração do sistema.

3.4. Documentação e Revisão

- Todos os incidentes são documentados e analisados para melhorar os serviços e evitar recorrências.

4. Política de Gestão de Crises

4.1. Objetivo

Fornecer um plano claro para gerenciar crises que possam afetar a prestação de serviços de segurança eletrônica, protegendo os clientes e seus ativos.

4.2. Escopo

Aplica-se a crises que comprometam a infraestrutura de segurança eletrônica, como falhas generalizadas de sistema, ataques cibernéticos ou eventos de grande impacto.

4.3. Plano de Gestão de Crises

- Ativação do Comitê de Crise: Uma equipe de resposta é ativada imediatamente para avaliar e mitigar a situação.
- Ações Imediatas: Manutenção de backups, restauração de sistemas comprometidos e comunicação contínua com os clientes.
- Plano de Comunicação: Informar rapidamente os clientes sobre a natureza da crise e as medidas sendo tomadas para restabelecer a normalidade.

4.4. Encerramento e Lições Aprendidas

Após a crise, realizamos uma revisão completa para aprimorar nossos processos e garantir a segurança contínua dos clientes.