Política de Resposta a Incidentes de Segurança

C Controle - CLOSMAQ INFORMATICA LTDA
Site: https://www.ccontrole.com.br
Versão: 1.0
Última atualização: 17 de julho de 2026

1. Objetivo

Esta política estabelece as diretrizes do C Controle para identificação, avaliação, tratamento, comunicação e registro de incidentes de segurança da informação.

O objetivo é garantir que incidentes físicos, técnicos, operacionais ou relacionados a dados sejam tratados de forma organizada, com responsabilidades definidas e canais adequados de comunicação.

2. Escopo

Esta política se aplica aos sistemas do C Controle, servidores, bancos de dados, backups, infraestrutura de rede, ambientes administrativos, integrações, colaboradores autorizados e dados tratados pela empresa.

3. Definição de Incidente

Para fins desta política, considera-se incidente qualquer evento confirmado ou suspeito que possa comprometer a confidencialidade, integridade ou disponibilidade dos sistemas, dados ou infraestrutura do C Controle.

Exemplos de incidentes incluem:

- Acesso não autorizado a sistemas, servidores ou dados.
- Suspeita de vazamento, perda ou exposição de dados.
- Indisponibilidade relevante de sistemas.
- Falha física em servidor, rede, energia ou ambiente.
- Infecção por malware ou atividade suspeita.
- Comprometimento de credenciais.
- Alteração indevida de dados.
- Falha em backup ou recuperação.
- Evento que possa afetar a segurança ou continuidade dos serviços.

4. Responsáveis e Funções

O C Controle define responsáveis internos para condução das ações de resposta a incidentes.

Responsável por incidentes de segurança:
David Prado
Telefone: (32) 9 8852-516

Responsabilidades do responsável por incidentes

- Receber, registrar e avaliar comunicações de incidentes.
- Identificar a natureza, impacto e urgência do incidente.
- Restringir acessos quando necessário.
- Acionar colaboradores autorizados para suporte técnico.
- Preservar evidências quando aplicável.
- Validar backups e recursos de recuperação.
- Coordenar ações de contenção, correção e restauração.
- Comunicar clientes afetados quando houver confirmação de impacto relevante.
- Registrar ações tomadas e lições aprendidas.

Responsabilidades dos colaboradores autorizados

- Comunicar imediatamente suspeitas de incidentes.
- Proteger credenciais e equipamentos.
- Apoiar ações de contenção e recuperação.
- Não divulgar informações sobre incidentes sem autorização.
- Seguir orientações do responsável por incidentes.

5. Canal de Comunicação

Comunicações relacionadas a incidentes de segurança podem ser realizadas pelo seguinte canal:

Responsável: David Prado
Telefone: (32) 9 8852-516

Quando disponível, clientes também podem utilizar os canais oficiais de suporte do C Controle já utilizados no relacionamento comercial.

6. Quando o Atendimento de Incidente é Acionado

O processo de resposta a incidentes é acionado somente quando houver:

- Identificação interna de incidente real ou suspeito.
- Falha física, técnica ou operacional relevante.
- Indício de acesso não autorizado.
- Indício de exposição, perda ou alteração indevida de dados.
- Solicitação formal de cliente salvo/ativo que identifique suspeita de incidente relacionada ao uso dos serviços do C Controle.

Solicitações de clientes serão avaliadas conforme vínculo ativo, contexto técnico, registros disponíveis e relação com os serviços prestados pelo C Controle.

7. Etapas de Resposta a Incidentes

O C Controle adota as seguintes etapas gerais para resposta a incidentes:

7.1 Identificação

Coleta inicial de informações, verificação de alertas, registros, relatos de clientes, indisponibilidade, comportamento anormal ou falha técnica.

7.2 Avaliação

Análise da natureza do incidente, sistemas afetados, possíveis dados envolvidos, impacto operacional, urgência e necessidade de comunicação.

7.3 Contenção

Adoção de medidas para limitar o impacto do incidente, como restrição de acessos, alteração de credenciais, isolamento de sistemas, bloqueios de rede ou ativação de ambiente de réplica.

7.4 Correção

Tratamento da causa identificada, aplicação de ajustes técnicos, restauração de configurações, atualização de sistemas ou correção de falhas.

7.5 Recuperação

Validação de backups, restauração de serviços, ativação de servidor de réplica quando necessário e monitoramento do ambiente após retorno operacional.

7.6 Registro e Melhoria

Registro das ações realizadas, evidências disponíveis, causa identificada, medidas corretivas e oportunidades de melhoria.

8. Comunicação a Clientes

A comunicação a clientes será realizada quando houver confirmação de impacto relevante aos serviços, dados ou operação do cliente.

Quando aplicável, o C Controle poderá solicitar informações adicionais ao cliente para avaliar a ocorrência, confirmar vínculo, validar registros e direcionar as medidas necessárias.

A comunicação será feita por canais oficiais de atendimento, telefone do responsável ou outro meio adequado conforme a situação.

9. Preservação de Evidências

Quando aplicável, o C Controle preservará registros, logs, prints, backups, horários, relatos e demais evidências necessárias para análise do incidente, suporte técnico, comprovação de ações e melhoria dos controles.

10. Continuidade e Recuperação

Em caso de incidente físico ou falha que afete o servidor de produção, o C Controle poderá acionar o servidor de réplica e validar backups disponíveis para apoiar a continuidade dos serviços.

A empresa mantém backups diários e infraestrutura de contingência para apoiar a recuperação operacional.

11. Limitações

O atendimento de incidentes é direcionado a ocorrências relacionadas aos sistemas, serviços e infraestrutura do C Controle.

Solicitações que não estejam relacionadas aos serviços prestados, que não permitam validação mínima, ou que não sejam feitas por cliente ativo/salvo poderão exigir análise adicional antes de qualquer ação técnica.

12. Revisão

Esta política é revisada periodicamente e pode ser atualizada sempre que houver mudanças nos sistemas, infraestrutura, processos internos, canais de atendimento, requisitos legais ou controles de segurança.