**GERENCIAMENTO DE RESPOSTA A INCIDENTES**

**GRI #1**

**RANSOMWARE**

Diretrizes para Lidar e Responder

a uma Infecção por Ransomware



**RESUMO**

GRI Autor: William Lima

Empresa: Suricatoos

E-mail: [william.lima@suricatoos.com](mailto:william.lima@suricatoos.com)

GitHub: https://github.com/williamsouzadelima

### **METODOLOGIA DE RESPOSTA A INCIDENTES**

Este **Playbook de Resposta a Incidentes** é um **guia de referência** dedicado a profissionais responsáveis por investigar e mitigar incidentes de segurança específicos.

## **📌 QUEM DEVE USAR ESTE PLAYBOOK?**

🔹 **Analistas de Segurança** 🛡️

🔹 **Analistas de SOC (Centro de Operações de Segurança)** 👨‍💻

🔹 **CISOs, Gerentes e Coordenadores de Segurança** 📊

🔹 **Equipes CERTs (Computer Emergency Response Teams)** 🚨

🔹 **Blue Team** 🎯

## **📢 ORIENTAÇÕES IMPORTANTES DURANTE UM INCIDENTE**

✔️ **Siga o PLANO DE RESPOSTA A INCIDENTES** detalhado para minimizar impactos financeiros e a imagem da EMPRESA.

✔️ **Documente cada ação tomada** – isso ajudará na análise pós-incidente e na melhoria contínua.  
✔️ **Mantenha a calma e siga os procedimentos** – evite tomar decisões precipitadas.  
✔️ **Entre em contato com a equipe de Resposta a Incidentes** ou com o **CERT da sua organização** sempre que necessário.

📌 **Contato do GRI CERT Suricatoos:**

🔗 GitHub: [GRI CERT Suricatoos](https://github.com/williamsouzadelima)

📩 E-mail: **contato@suricatoos.com**

🚀 **Uma resposta estruturada a incidentes protege sua empresa de maiores danos e reduz o tempo de recuperação!**

**ETAPAS DE RESPOSTA A INCIDENTES**

A resposta eficaz a incidentes de segurança segue **6 etapas essenciais**, conforme definido pelo **Guia de Tratamento de Incidentes de Segurança de Computadores do NIST**.

## **PREPARAÇÃO** 🛠️

**📌 Objetivo:** Garantir que a organização esteja pronta para responder rapidamente a incidentes de segurança.

✅ Desenvolver e documentar **políticas de resposta a incidentes (PRI)**.

✅ Definir **funções e responsabilidades** da equipe de resposta.

✅ Implementar **ferramentas de detecção e monitoramento** (SIEM, EDR/XDR).

✅ **Treinar e conscientizar** funcionários sobre ameaças cibernéticas.

✅ Criar um **plano de comunicação interna e externa** para resposta a incidentes.

## **IDENTIFICAÇÃO** 🔍

**📌 Objetivo:** Detectar e confirmar a ocorrência de um incidente.

✅ Monitorar **logs e alertas** de segurança em tempo real.

✅ Identificar **indicadores de comprometimento (IoCs)** e atividades anômalas.

✅ Confirmar a natureza do ataque (ransomware, phishing, malware, vazamento de dados).

✅ Determinar **quais sistemas e dados foram afetados**.

✅ Ativar **o plano de resposta a incidentes** e envolver as partes apropriadas.

## **CONTENÇÃO** 🚧

**📌 Objetivo:** Limitar o impacto do incidente e evitar sua propagação.

✅ **Isolar sistemas comprometidos** (desconectar da rede, segmentação de VLANs).

✅ Bloquear **tráfego suspeito** e conexões C2 (Command & Control).

✅ Desativar **contas comprometidas** e redefinir credenciais afetadas.

✅ Aplicar **bloqueios em firewalls, EDR/XDR** para mitigar novos acessos maliciosos.

✅ Coletar **evidências forenses** para análise pós-incidente.

## **REMEDIAÇÃO** 🔄

**📌 Objetivo:** Eliminar a ameaça e restaurar a integridade dos sistemas.

✅ **Remover malware** e fechar brechas exploradas.

✅ Verificar e restaurar **backups limpos**.

✅ Aplicar **patches de segurança** e reforçar configurações.

✅ Reinstalar sistemas comprometidos, se necessário.

✅ Revisar permissões e políticas de acesso.

## **RECUPERAÇÃO** 🔧

**📌 Objetivo:** Retomar operações normais de forma segura.

✅ Validar que **os sistemas foram completamente limpos** e estão seguros.

✅ Restaurar **operações críticas** de maneira controlada.

✅ Monitorar **atividade pós-ataque** para detectar possíveis reinfecções.

✅ Aplicar **melhorias de segurança** baseadas na análise do incidente.

## **LIÇÕES APRENDIDAS** 📖

**📌 Objetivo:** Aprimorar continuamente a resposta a incidentes.

✅ Elaborar um **relatório detalhado** do incidente.

✅ Revisar **o que funcionou e o que falhou** na resposta.

✅ Melhorar **planos de segurança e defesa** com base na experiência adquirida.

✅ Ajustar **políticas, ferramentas e processos** para evitar ataques futuros.

✅ **Treinar equipes** para lidar melhor com incidentes similares no futuro.

**PREPARAÇÃO**

**🎯 OBJETIVO:** Estabelecer contatos, definir procedimentos e coletar informações essenciais para economizar tempo durante um incidente de ransomware.

## **Conhecimento e Infraestrutura de Segurança**

Para uma resposta eficaz, é essencial ter um **bom entendimento das políticas de segurança** e da **arquitetura da rede**.

### ESTRATÉGIA DO BACKUP 3-2-1

### **Estratégia de Backup 3-2-1: O Padrão Ouro para Proteção de Dados**

A estratégia 3-2-1 de backup é um dos métodos mais eficazes para garantir a recuperação de dados em caso de falhas, ataques cibernéticos (como ransomware) ou desastres naturais. Essa abordagem é amplamente recomendada por especialistas em segurança da informação e continuidade de negócios.

## **📌 O que é a Estratégia 3-2-1?**

A metodologia consiste em manter três cópias dos dados armazenadas em dois tipos diferentes de mídia, sendo uma cópia externa (offsite).

🔹 3 cópias dos dados

* Uma cópia primária em produção (dados ativos).
* Duas cópias adicionais para recuperação em caso de falha.

🔹 2 tipos diferentes de mídia de armazenamento

* Exemplo: Um disco rígido local + um armazenamento na nuvem.
* Isso reduz o risco de perda devido a falhas em um único tipo de mídia.

🔹 1 cópia offsite (fora do local principal)

* Deve ser armazenada em um local seguro e geograficamente distante (exemplo: cloud backup).
* Protege contra incidentes físicos como incêndios, inundações ou ataques cibernéticos.

## **🔄 Como Implementar a Estratégia 3-2-1?**

### **1️⃣ Backup Primário (Cópia de Trabalho)**

* Armazene os dados principais no sistema de produção.
* Pode estar em um servidor local, NAS ou ambiente de armazenamento corporativo.

### **2️⃣ Backup Secundário (Tipo Diferente de Mídia)**

* Armazene uma cópia dos dados em outro dispositivo, como:
  + HD externo ou SSD.
  + Servidor dedicado para backup (NAS, SAN).
  + Fita magnética (para grandes volumes de dados).

### **3️⃣ Backup Offsite (Cópia Remota)**

* Armazene uma cópia fora da empresa para proteção contra desastres e ataques.
* Opções recomendadas:
  + Backup na nuvem (Google Drive, AWS S3, Azure, Backblaze, Wasabi).
  + Replicação para um Data Center secundário.
  + Armazenamento em fita enviado para local seguro.

## **🛡️ Vantagens da Estratégia 3-2-1**

✅ Proteção contra ransomware – Ransomware pode criptografar arquivos locais, mas uma cópia offsite impede perda total.  
✅ Recuperação rápida – Com múltiplas cópias, é possível restaurar sistemas rapidamente.  
✅ Redundância confiável – Se um backup falhar, há outras alternativas para restauração.  
✅ Conformidade e governança – Atende requisitos de segurança (LGPD, ISO 27001, NIST).

## **⚠️ Melhores Práticas para Backup Seguro**

✔️ Automatize backups – Agende processos diários/semanalmente para evitar falhas humanas.  
✔️ Teste a recuperação – Verifique periodicamente se os backups podem ser restaurados corretamente.  
✔️ Use criptografia – Proteja os dados contra acessos não autorizados.  
✔️ Aplique retenção inteligente – Mantenha versões históricas para recuperação em longo prazo.  
✔️ Utilize backup imutável – Para evitar exclusão/modificação em ataques (ex.: Object Lock em S3).

✅ **Conhecimento das Políticas de Segurança**

* Estar familiarizado com **as configurações de segurança padrão** dos sistemas operacionais.
* Definir **políticas rigorosas de perfis de usuários** e privilégios mínimos.

✅ **Arquitetura e Segmentação de Rede**

* Documentar a **segmentação de VLANs e interconexões**.
* Ter capacidade para **isolar rapidamente** entidades, regiões, parceiros e conexões com a Internet.

✅ **Atualização dos Produtos de Segurança**

* Manter **EDR/XDR, firewall, gateways de e-mail e proxies sempre atualizados**.
* Aplicar **regras de bloqueio para IoCs** conhecidos associados a ransomware.

## **Implantação de Soluções de Detecção e Resposta**

🔹 **2.1 Implementação de EDR/XDR**

✅ O **EDR/XDR se tornou essencial** para resposta a incidentes de ransomware e grandes compromissos.

✅ **Definir políticas de prevenção** para bloquear ameaças antes da execução.

✅ **Realizar hunting proativo** com regras explícitas baseadas em **IoCs conhecidos**.

🔹 **2.2 Detecção Avançada e Coleta de Logs**

✅ **Implantar SIEM** para coleta centralizada de logs e correlação de eventos.

✅ Ter capacidade para rodar **YARA e DFIR-ORC** para investigações forenses.

✅ Configurar **retenção adequada de logs**, garantindo armazenamento suficiente para análise pós-incidente.

## **Fortalecimento da Postura de Segurança**

🔹 **3.1 Conscientização e Treinamento**

✅ Capacitar a equipe de suporte de TI e **treinar usuários finais** sobre sinais de ransomware.

✅ Criar **procedimentos claros** para resposta rápida caso suspeitas sejam identificadas.

🔹 **3.2 Estratégia de Comunicação**

✅ **Definir um plano de comunicação interna e externa**, incluindo porta-vozes e mensagens padrão.

✅ Garantir alinhamento entre **segurança da informação, TI, jurídico e alta gestão**.

🔹 **3.3 Ações em Caso de Detecção de Ransomware**

✅ Se um dispositivo for **infectado**, **desconectá-lo imediatamente da rede**, **mas mantê-lo ligado** para análise forense de memória.

**IDENTIFICAÇÃO**

**🎯 OBJETIVO:** Identificar um incidente de ransomware, determinar seu escopo e envolver as equipes apropriadas para resposta.

## **Sinais Gerais de Presença de Ransomware**

A detecção precoce de um ataque de ransomware pode minimizar danos. Algumas evidências que indicam comprometimento incluem:

🔹 **1.1 Monitoramento de Indicadores de Comprometimento (IoCs)**

✅ SOC (Security Operations Center) monitorando **indicadores de ransomware** em tempo real.

✅ Alertas de **EDR/XDR** detectando **comportamentos suspeitos** nos endpoints.

🔹 **1.2 Análise de Comportamento e Atividades Suspeitas**

✅ Recebimento de **e-mails maliciosos** disfarçados de faturas com **anexos suspeitos**.

✅ Exibição de **mensagens de resgate** na área de trabalho do usuário informando sobre arquivos criptografados.

✅ Relatos de **arquivos inacessíveis ou corrompidos** com **extensões incomuns** (.abc, .xyz, .aaa).

✅ Alta modificação de arquivos em **curto período de tempo** nos compartilhamentos de rede.

✅ Publicação de **dados roubados** nos sites de vazamento de operadores de ransomware.

🔹 **1.3 Movimento Lateral e Atividade na Rede**

✅ Verificação de **autenticações anômalas** no Active Directory (AD) e servidores de arquivos.

✅ Detecção de **conexões suspeitas** com redes Tor (I2P, tor2web) e **sites de pagamento em Bitcoin**.

✅ Identificação de **conexões raras ou em horários incomuns** por contas privilegiadas.

## **Determinação do Escopo do Incidente**

🔹 **2.1 Ferramentas para Análise Forense e Hunting**

✅ Uso de **EDR/XDR**, **YARA**, **DFIR-ORC** e outras ferramentas para identificar **máquinas comprometidas**.

✅ Mapeamento do impacto **para definir a estratégia de contenção e erradicação**.

🔹 **2.2 Identificação do Vetor de Ataque Inicial**

✅ Identificar **como o ransomware entrou na rede** (phishing, RDP exposto, credenciais vazadas).

✅ Determinar se há **outros sistemas comprometidos** e **possíveis pivôs usados pelos atacantes**.

**CONTENÇÃO**

**🎯 OBJETIVO:** Minimizar o impacto do ataque no ambiente, interromper a propagação e proteger os sistemas ainda não comprometidos.

## **Ações de Contenção Imediatas**

🔹 **1.1 Comunicação e Postura Estratégica**

✅ **Emitir uma declaração pública** o mais rápido possível, seguindo o **plano de comunicação de crise** definido na fase de preparação.

✅ Manter a **postura de resposta alinhada** com as diretrizes de segurança e conformidade da organização.

🔹 **1.2 Análise e Relato de Ameaças**

✅ Enviar **amostras de malware não detectadas** para:

* **Provedor de segurança de endpoint** para análise e atualização de assinaturas.
* **Sandboxes privadas** para investigação detalhada.
* ✅ Reportar **URLs maliciosas, domínios e IPs desconhecidos** para o **provedor de segurança perimetral**.

🔹 **1.3 Bloqueio de Comunicação com Atacantes**

✅ **Interromper conexões ativas** com **servidores de Comando & Controle (C2s)**.

✅ **Bloquear IPs suspeitos** usados pelos invasores.

✅ **Isolar VLANs comprometidas**, interconexões, entidades, regiões e parceiros de negócios afetados.

## **Isolamento de Sistemas e Contas Comprometidas**

🔹 **2.1 Desativação de Contas Suspeitas**

✅ **Desativar imediatamente** contas comprometidas ou criadas pelos atacantes.

✅ **Reforçar autenticação multifator (MFA)** para todas as contas privilegiadas.

🔹 **2.2 Desconectar e Isolar Dispositivos Comprometidos**

✅ **Remover da rede todos os dispositivos identificados como infectados**.

✅ Se estiver usando um **EDR (Endpoint Detection & Response)**:

* **Manter a conectividade do EDR/XDR**, mas **desativar o acesso à Internet**.

🔹 **2.3 Isolamento de Compartilhamentos de Rede**

✅ Se não for possível desconectar o dispositivo, **desabilitar ou remover compartilhamentos de rede** para evitar propagação do ataque.

📌 **Comando para remover unidade de rede compartilhada:**

*pgsql*

*CopyEdit*

*NET USE x: \\unc\path\ /DELETE*

**REMEDIAÇÃO**

**🎯 OBJETIVO:** Restaurar o sistema para operações normais de forma segura e minimizar o risco de reinfecção.

## **Medidas de Remediação e Recuperação**

🔹 **1.1 Atualizar Assinaturas de Segurança**

✅ Atualizar **antivírus, EDR/XDR e ferramentas de SIEM** com os **binários maliciosos identificados** para bloqueá-los.

✅ Garantir que **todas as máquinas** estejam protegidas antes da reconexão à rede.

🔹 **1.2 Garantir a Integridade dos Sistemas**

✅ Certifique-se de que **nenhum malware** permanece no ambiente antes de colocar sistemas em produção.

✅ Utilize **varreduras forenses** para garantir que não há **backdoors ou persistência de ameaças**.

🔹 **1.3 Normalizar o Tráfego de Rede**

✅ Monitore o tráfego para garantir que ele **voltou ao normal** e não há **comunicação suspeita** com servidores maliciosos.

✅ **Bloqueie conexões suspeitas** identificadas durante a análise do ataque.

🔹 **1.4 Restaurar Documentos a Partir de Backups**

✅ Restaurar **apenas de backups confiáveis**, garantindo que **não foram comprometidos** durante o ataque.

✅ Priorizar a recuperação com base no **Plano de Recuperação de Desastres (DRP)**.

## **Procedimentos de Recuperação Segura**

🔹 **2.1 Verificação e Limpeza do Backup**

✅ Antes de restaurar qualquer dado, **verifique se o backup está íntegro** e se o dispositivo onde ele será restaurado **está limpo**.

✅ Nunca conecte um backup a um sistema potencialmente comprometido.

**OU**

🔹 **2.2 Refazer a Imagem do Sistema**

✅ Se houver dúvida sobre a segurança do ambiente, **realizar uma reinstalação limpa** do sistema operacional.

✅ Implementar novamente **softwares essenciais e configurações de segurança**.

🔹 **2.3 Redefinição de Credenciais**

✅ **Trocar todas as senhas e credenciais** do sistema, priorizando:

* Contas administrativas e de acesso privilegiado.
* Credenciais usadas em serviços críticos.
* Senhas compartilhadas ou reutilizadas em múltiplos sistemas.

✅ Implementar **MFA (Autenticação Multifator)** para todas as contas de alto privilégio.

## **Monitoramento Contínuo e Medidas Adicionais**

🔹 **3.1 Monitorar a Rede e os Sistemas**

✅ Continuar analisando o tráfego para detectar **possível reinfecção ou atividades incomuns**.

✅ Criar **regras de detecção** para atividades relacionadas ao ataque.

🔹 **3.2 Aplicar Filtragem Geográfica no Firewall**

✅ Se possível, restringir acessos de países que **não possuem operações relevantes para a organização**.

✅ Bloquear domínios e IPs conhecidos de **infraestruturas de ransomware**.

🔹 **3.3 Monitorar Vazamento de Dados na Dark Web**

✅ Acompanhar sites de **agentes de ameaças e fóruns de ransomware** para verificar se dados foram vazados.

✅ Implementar um serviço de **Dark Web Monitoring** para alertas proativos.

**LIÇÕES APRENDIDAS**

**🎯 OBJETIVO:** Documentar os detalhes do incidente, discutir as lições aprendidas e ajustar planos e defesas para evitar recorrências.

## **📄 Relatório do Incidente**

Após a contenção e recuperação do incidente, um **relatório detalhado** deve ser elaborado e compartilhado com todas as partes interessadas. O documento deve conter as seguintes informações essenciais:

### **📌 1. Causa Inicial da Infecção**

* Como o ataque foi iniciado? (Phishing, RDP exposto, vulnerabilidade explorada, malware, credenciais comprometidas).
* Identificação do vetor de ataque principal e análise das fragilidades exploradas.

### **📌 2. Ações e Cronogramas de Eventos Importantes**

* **Linha do tempo** do incidente:
  + Momento da detecção.
  + Medidas tomadas para contenção e erradicação.
  + Tempo necessário para recuperação.
* Registros de todas as ações executadas durante a resposta ao incidente.

### **📌 3. O Que Deu Certo**

* Quais controles de segurança funcionaram conforme esperado?
* Quais processos foram eficazes na mitigação do incidente?
* Ferramentas e práticas que ajudaram na detecção e resposta rápida.

### **📌 4. O Que Deu Errado**

* Gaps na resposta ao incidente (falta de visibilidade, atraso na detecção, falha de comunicação).
* Processos que não funcionaram ou precisaram de ajustes.
* Recursos e treinamentos que deveriam ter sido aplicados previamente.

### **📌 5. Custo do Incidente**

* Impacto financeiro direto (tempo de inatividade, perda de dados, custos de recuperação).
* Impacto operacional (paralisação de serviços, danos à reputação, esforços da equipe).
* Multas ou penalidades por conformidade/regulação (LGPD, ISO 27001, GDPR).

### **📌 6. Indicadores de Comprometimento (IoCs)**

* Listagem de **IPs, domínios, hashes de arquivos maliciosos** identificados durante a investigação.
* Indicadores que podem ser usados para reforçar **monitoramento e prevenção de futuros ataques**.

## **📈 Capitalização: Melhorias nos Processos de Segurança**

Com base na experiência do incidente, é essencial **definir ações para fortalecer a detecção e resposta** a ameaças futuras:

✅ **Reforçar processos de detecção**

* Melhorar regras de SIEM, firewall e EDR para identificar sinais precoces de ataques.
* Implementar alertas automatizados para comportamentos anômalos.

✅ **Aprimorar segurança de endpoints e redes**

* Aplicar segmentação de rede para limitar movimentos laterais.
* Atualizar e reforçar políticas de controle de acesso e autenticação multifator (MFA).

✅ **Treinamento e conscientização**

* Simulações de ataques para preparar equipes de resposta.
* Treinamento contínuo de segurança para reduzir riscos de phishing e engenharia social.

✅ **Revisar e atualizar planos de resposta a incidentes**

* Ajustar planos de recuperação com base nos desafios encontrados.
* Melhorar processos de comunicação interna e com fornecedores/parceiros.