Template: Plano de Resposta a Incidentes NIST

Cenário: A
Data: 29/09/2025
Versão: 1.0
Responsável: Luiz Eduardo de Andrade

📊 Informações do Documento

Campo	Valor
Título	Plano de Resposta a Incidentes – Ataque de Ransomware
Classificação	Interno/Confidencial/Restrito/Público
Aprovação	José Menezes
Próxima Revisão	29/09/2025
Distribuição	CSIRT, TI, Segurança, Jurídico

🎯 Escopo e Objetivos

Escopo

Este plano abrange a resposta a Ataque de Ransomware em Banco, incluindo:

- Sistemas críticos afetados
- Dados envolvidos
- Stakeholders impactados
- Processos de negócio

Objetivos

- Minimizar impacto operacional
- Preservar evidências para investigação

- Cumprir obrigações legais e regulatórias
- Restaurar operações normais rapidamente
- Prevenir recorrência do incidente

🏢 Contexto Organizacional

Perfil da Organização

- **Setor:** Financeiro (Banco)
- **Porte:** 1000 funcionários, 15 filiais
- **Receita:** R$ 500M anuais
- **Dados Críticos:** PII, PHI, Cartões de crédito

Infraestrutura Tecnológica

- **Sistemas Críticos:** App do Banco, site do banco, sistema interno do banco, integração com o Banco Central,
- **Fornecedores:** AWS, Azure e GCP, ERP TOTVS
- **Compliance:** [LGPD, PCI-DSS, ISO 27001]

📞 Equipe de Resposta a Incidentes

CSIRT - Computer Security Incident Response Team

Função	Nome	Telefone	Email	Backup
Coordenador CSIRT	José Menezes	21 99987-4782	jose.menezes@bancoluizinho.com.br	Gilson
Líder Técnico	João Pedro	21 98654-7377	Joao.pedro@bancoluizinho.com.br	Joy
Analista Forense	Luiz Eduardo de	11 98543-6751	luiz.eduardo@bancoluizinho.com.br	Carlos

Função	Nome	Telefone	Email	Backup
	Andrade			
Especialista em Redes	Ricardo Luna	11 96576-4200	ricardo.luna@bancoluizinho.com.br	Daniel
Representante Jurídico	Felipe Nogueira	11 99678-5876	felipe.nogueira@bancoluizinho.com.br	Júlio
Comunicação	Paulo Silva	11 99965-4321	paulo.silva@bancoluizinho.com.br	Aparecido

Stakeholders Externos

- **Autoridades:** Polícia Civil/Federal, ANPD
- **Fornecedores:** AWS, Azure e GCP, financeiras
- **Clientes:** Comunicação com o Paulo Silva
- **Mídia:** Assessoria de Imprensa Rebeca Morais

🟣 FASE 1: PREPARAÇÃO

1.1 Políticas e Procedimentos

- Política de Segurança da Informação aprovada
- Procedimentos de backup e recuperação testados
- Plano de Continuidade de Negócios atualizado
- Contratos com fornecedores incluem cláusulas de segurança

1.2 Ferramentas e Recursos

- **SIEM:** [Ex: Splunk, QRadar, ELK Stack]
- **Análise Forense:** [Ex: Volatility, Autopsy, FTK]
- **Comunicação:** [Ex: Slack, Teams, PagerDuty]

- **Monitoramento:** [Ex: Nagios, Zabbix, Datadog]

1.3 Treinamento e Conscientização

- Equipe CSIRT treinada trimestralmente
- Simulados de resposta a incidentes semestrais
- Funcionários treinados em identificação de ameaças
- Procedimentos de escalação conhecidos por todos

1.4 Métricas e Indicadores

- **MTTD (Mean Time to Detection):** [Ex: < 30 minutos]
- **MTTR (Mean Time to Response):** [Ex: < 1 hora]
- **MTTR (Mean Time to Recovery):** [Ex: < 4 horas]
- **RTO (Recovery Time Objective):** [Ex: < 8 horas]

🔍 FASE 2: DETECÇÃO E ANÁLISE

2.1 Indicadores de Comprometimento (IoCs)

Cenário Específico: Segue os detalhes dos IoCs do banco

- Indicador 1 - Arquivos encriptados
- Indicador 2 – Tela com solicitação de pagamento em criptomoeda
- Indicador 3 – Arquivos inacessíveis
- Indicador 4 – Sistema parado

2.2 Fontes de Detecção

- **Logs de Sistema:** Windows Event Logs, Syslog
- **Logs de Rede:** Firewall, IPS/IDS, DNS
- **Logs de Aplicação:** Web servers, Databases
- **Usuários:** Relatos de funcionários/clientes
- **Terceiros:** Threat intelligence, fornecedores

2.3 Processo de Análise Inicial

Passo 1: Validação do Incidente (< 15 min)

```
# Comandos para verificação inicial
Verificar logs de eventos
Verificar qual máquina foi infectada primeiro e quais permissionamentos ela tinha como usuário, administrador, root
```

Passo 2: Classificação (< 30 min)

- **Severidade:** Crítico
- **Impacto:** [Confidencialidade/Integridade/Disponibilidade]
- **Categoria:** Malware (Ransomware)
- **Urgência:** Imediata

Passo 3: Coleta de Evidências Iniciais

- Screenshots de alertas/sistemas afetados
- Logs relevantes preservados
- Memória RAM capturada (se aplicável)
- Tráfego de rede capturado
- Depoimentos iniciais coletados

2.4 Escalação e Ativação

Critérios de Escalação

- Impacto em sistemas críticos
- Exposição de dados sensíveis
- Paralisação de operações
- Repercussão midiática potencial
- Valor financeiro envolvido > R$ 100 milhões

Processo de Ativação do CSIRT

1. **Detecção inicial** → Analista de plantão
2. **Validação** → Líder técnico (< 15 min)

3. **Escalação** → Coordenador CSIRT (< 30 min)
4. **Ativação completa** → Toda a equipe (< 1 hora)

⚡ FASE 3: CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

3.1 Contenção Imediata (< 1 hora)

Objetivos

- Parar a propagação do incidente
- Preservar evidências
- Manter sistemas críticos funcionando
- Minimizar impacto nos negócios

Ações de Contenção - [Cenário Específico]

```
# Comandos de contenção específicos
Isolar a máquina que contém o arquivo malicioso
Verificar se outras máquinas foram infectadas, e fazer a limpeza destas máquinas com backups testados
```

Checklist de Contenção:

- Restaurar os backups validados
- Subir os sistemas com imagens limpas e sem vírus ou qualquer tipo de malware que prejudique o sistema e volte a ter problemas
- Verificar por onde o malware entrou e como ele conseguiu criptografar todos os dados
- Porque não conseguimos evitar a criptografia do nosso sistema
- Comunicação às partes interessadas
- Documentação das ações realizadas

3.2 Coleta de Evidências Forenses

Ordem de Volatilidade (RFC 3227)

1. **Memória RAM** → Mais volátil
2. **Estado do sistema** → Processos, conexões
3. **Disco rígido** → Arquivos, logs
4. **Logs remotos** → SIEM, syslog
5. **Configurações** → Menos volátil

Procedimentos de Coleta

```
# Exemplo de comandos forenses
Fazer a coleta de dados dos logs
Verificar de onde partiu o ataque
Fez alguma movimentação lateral?
A máquina infectada tinha qual tipo de acesso?
```

3.3 Erradicação (< 4 horas)

Identificação da Causa Raiz

- Vetor de ataque identificado
- Vulnerabilidade explorada mapeada
- Timeline de comprometimento estabelecida
- Extensão do comprometimento avaliada

Ações de Erradicação

- Ação específica 1 – Verificar e retirar o ransomware do servidor
- Ação específica 2 – Verificar de onde veio o arquivo malicioso
- Ação específica 3 – Isolar a máquina onde o arquivo foi encontrado pela primeira vez
- Ação específica 4 - Atualização de sistemas e das defesas necessárias para que isso não ocorra mais.

3.4 Recuperação (< 8 horas)

Plano de Recuperação

1. **Sistemas Críticos** (Prioridade 1)
    - App do Banco para dispositivos móveis
    - Site do Banco
2. **Sistemas Importantes** (Prioridade 2)
    - ERP do banco
    - Banco de Dados dos clientes
3. **Sistemas Auxiliares** (Prioridade 3)
    - Sistema interno do banco
    - Sistema de comunicação com o banco Central

Validação da Recuperação

- Funcionalidade restaurada
- Performance normal
- Conectividade verificada
- Dados íntegros
- Usuários conseguem acessar

📝 FASE 4: ATIVIDADES PÓS-INCIDENTE

4.1 Relatório de Incidente

Resumo Executivo

- **Tipo de Incidente:** Ransomware
- **Data/Hora:** 25/09 as 04:00 25/09 12:00
- **Duração:** 8 horas
- **Sistemas Afetados:** Sistema bancário, app para dispositivos móveis, site do banco, site de integração com o Banco Central.
- **Impacto:** Impacto Total sistemas criptografados, sem acesso aos bancos de dados, sem acesso as informações do cliente, app do banco inoperante, site inoperante

- **Custo Estimado:** R$ 500 milhões

Timeline Detalhada

Timestamp	Evento	Responsável	Evidência
04:00:00	Criptografia	Luiz Eduardo de Andrade	https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware

4.2 Lições Aprendidas

O que funcionou bem?

- Backups testados e em diversos lugares diferentes
- Plano de Recuperação de Desastres
- Plano de Continuidade de Negócios

O que precisa melhorar?

- Regras de Firewall mais restritivas
- Proteção de e-mails com links maliciosos
- Treinamentos constantes com a equipe sobre a Segurança dos Dados e não clicar em links suspeitos sempre consultar a equipe de TI quando tiver dúvidas sobre algum link recebido por e-mail ou em uma página da internet.

Recomendações

1. **Prevenção:**

- Treinamentos regulares para funcionários
- Instalar IPS para o bloqueio de malwares conhecidos

2. **Detecção:**
    - Investir em SIEM e SOAR para verificar eventos suspeitos.
    - Ter um SOC 24/7 para tomar as ações o mais rápido possível
3. **Resposta:**
    - Resposta mais rápida quando o sistema for comprometido
    - Equipe melhor preparada para lidar com incidentes graves

4.3 Plano de Ação

Ação	Responsável	Prazo	Status
Restaurar os backups limpos e sem vírus	Carla Maria	25/09/2025	Concluído
Sistemas do banco totalmente operacionais	Luiz Eduardo de Andrade	27/09/2025	Concluído

4.4 Métricas do Incidente

Métrica	Valor	Meta	Status
MTTD	1 hora	1 hora	✅
MTTR	1 hora	1 hora	✅
Downtime	4 horas	1 hora	❌

📞 Comunicação

Comunicação Interna

- CEO/Diretoria notificada
- TI notificado
- RH notificado (se aplicável)
- Jurídico notificado
- Auditoria notificada

Comunicação Externa

- Autoridades notificadas
- Clientes notificados
- Fornecedores notificados
- Seguradoras notificadas
- Mídia

Templates de Comunicação

- Link para template de comunicação interna
- Link para template de comunicação externa
- Link para template de notificação regulatória

⚖️ Considerações Legais e Regulatórias

LGPD (Lei Geral de Proteção de Dados)

- Incidente envolve dados pessoais?
- Notificação à ANPD necessária? (72 horas)
- Notificação aos titulares necessária?
- Registro no relatório de impacto

Outras Regulamentações

- Regulamentação específica do setor bancário
- Padrão de compliance aplicável
- Certificação que pode ser impactada

🗄 Anexos

A. Procedimentos Técnicos Detalhados

- Link para playbook de contenção
- Link para playbook de análise forense
- Link para playbook de recuperação

B. Formulários e Checklists

- Link para formulário de relato de incidente
- Link para checklist de contenção
- Link para log de ações

C. Contatos de Emergência

- Lista completa de contatos
- Procedimentos de escalação 24/7

D. Ferramentas e Recursos

- Lista de ferramentas disponíveis para
- Credenciais de acesso (referência segura)
- Documentação técnica

📝 Controle de Versões

Versão	Data	Autor	Alterações
1.0	29/09/2025	Luiz Eduardo de Andrade	Versão inicial