

# Experiência de simulação: Resposta a incidentes



**Tempo total**  
Duas horas



**Máximo de  
participantes**  
30

## Público-alvo

Funcionários corporativos que fazem parte do plano de resposta a incidentes de suas organizações, independentemente de formação técnica ou nível de escolaridade.

## Visão geral

Um exercício simulado é uma atividade guiada na qual os participantes interpretam cenários. Isso identifica lacunas no alinhamento da equipe e pontos vulneráveis durante períodos tranquilos, criando resiliência para crises reais, quando a coordenação em tempo real é fundamental. O objetivo não é a execução perfeita, mas sim a preparação por meio de testes em cenários práticos.

## Objetivos de aprendizagem

Ao final desta experiência, os participantes serão capazes de:

- Explicar a importância de um plano de resposta a incidentes no local de trabalho.
- Identificar funções e responsabilidades durante um incidente de segurança.
- Raciocinar rapidamente e tomar decisões eficazes em cenários de incidentes.

## Materiais

- Listas de verificação impressas sobre resposta a incidentes
- Temporizador ou cronômetro
- Cartões para os participantes (Líder de segurança de TI, Coordenador de incidentes, Líder de comunicações, Assessor jurídico, Representante de RH e Gerente de departamento)
- Cartões de cenários para representação
- Quadro branco ou flipchart
- Canetas marcadoras
- Canetas e blocos de notas

## Funções no exercício simulado

**Facilitador:** controla o ritmo do exercício, orienta os debates, atualiza os cenários, garante a participação de todos e apresenta informações para testar o foco da equipe.

**Participantes:** desempenham seus papéis durante a simulação, debatem abertamente sobre seus processos de pensamento, apoiam os colegas e respondem aos cenários de acordo com as responsabilidades da função.

**Avaliador:** avalia os pontos fortes e fracos, elabora relatórios pós-ação e analisa o alinhamento aos planos e procedimentos existentes.

**Observador:** oferece conhecimento especializado sem participar diretamente do exercício e dá apoio aos participantes, fazendo perguntas relevantes e orientando-os quando necessário.

**Tomador de notas:** documenta todas as atividades do exercício, os debates, as lacunas identificadas, o alinhamento aos procedimentos oficiais da organização e as melhorias sugeridas.

## Introdução

### Duração: 10 minutos

A resposta eficaz a incidentes requer comunicação clara, funções definidas e adaptabilidade. Diga aos participantes que as atividades simularão cenários e desafios do mundo real para ajudá-los a desenvolver habilidades essenciais de gerenciamento de incidentes de segurança. Reforce que o sucesso da resposta a incidentes depende da **coordenação da equipe** e do **raciocínio rápido**.

---

## Atividade 1: Lista de verificação para resposta rápida

---

 **Duração: 30 minutos**

### Materiais

- Temporizador ou cronômetro
- Canetas e blocos de notas
- Listas de verificação impressas sobre resposta a incidentes (consulte o Anexo da Atividade 1)

### Atividade

Esta atividade testa o plano de resposta a incidentes, a estratégia de comunicação e o processo de tomada de decisões de cada um.

Apresente o seguinte cenário aos participantes:

“Um servidor crítico da sua organização é criptografado por um ransomware, e os invasores exigem uma grande quantia em criptomoeda para descriptografar os arquivos.”

Com o contexto estabelecido:

1. Distribua as listas de verificação de resposta a incidentes para todos os participantes. A lista de verificação contém etapas comuns de resposta a incidentes em ordem aleatória.
2. Dê aos participantes 10 minutos para priorizar, individualmente, as etapas da lista de verificação na ordem que eles considerarem mais adequada para o cenário de ransomware.
3. Peça aos participantes que se dividam em pequenos grupos, com três ou quatro pessoas, e debatam sobre suas prioridades durante 10 minutos, garantindo que cada pessoa preencha sua própria lista de verificação separadamente.
4. Use os últimos 10 minutos para analisar, com toda a turma, quais sequências de resposta são mais eficazes, explicando por que determinadas etapas devem ocorrer antes de outras.

### Gabarito

Com base nas melhores práticas do setor, estes são os principais itens que a lista de verificação deve incluir:

1. Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)
2. Mobilizar a equipe de resposta a incidentes
3. Isolar os sistemas afetados
4. Documentar a cronologia do incidente
5. Avaliar o status do backup de dados
6. Ativar o plano de comunicação da organização para as partes interessadas
7. Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares
8. Acionar o assessor jurídico
9. Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate
10. Entrar em contato com as autoridades legais (de acordo com a política da organização)

---

## Atividade 2: Simulação de resposta a incidentes

---

 **Duração: 35 a 60 minutos**

### Materiais

- Cartões de referência sobre as responsabilidades dos participantes (consulte o Anexo da Atividade 2)
- Cartões de cenários com complicações (consulte o Anexo da Atividade 2)
- Temporizador ou cronômetro
- Quadro branco ou flipchart
- Canetas marcadoras
- Canetas e blocos de notas
- Plano real de resposta a incidentes da organização

### Atividade

Esta atividade testa habilidades de resposta interfuncionais utilizando as funções reais dos participantes na organização, as estratégias de comunicação interna e externa e os processos de tomada de decisão ao enfrentar incidentes com complicações.

Divida os participantes em grupos que representem equipes reais de resposta a incidentes da organização. Cada participante deve assumir sua função real na resposta a incidentes ou a função equivalente mais próxima indicada no cartão do participante.

Instruções:

1. Forneça a cada grupo um cartão de cenário descrevendo um incidente de segurança com complicações
2. Dê aos grupos 20 minutos para debater e formular uma estratégia de resposta usando as funções designadas e os procedimentos da organização
3. Todos os grupos devem apresentar seus planos (cinco minutos por grupo)
4. Adicione mais uma complicação a cada cenário (por exemplo: “A imprensa ficou sabendo do incidente por causa de um vazamento de informações”)
5. Dê aos grupos 10 minutos para ajustar os planos com base nas novas informações e utilizando os procedimentos estabelecidos
6. Os grupos devem apresentar seus planos ajustados e falar sobre como eles se adaptaram dentro das estruturas organizacionais

Instruções adicionais para os grupos:

- Consultem o plano de real de resposta a incidentes da sua organização durante os debates
- “Pensem alto” para tornar a tomada de decisões visível
- Certifiquem-se de que todos os participantes contribuam de acordo com suas responsabilidades reais
- Concentrem-se em ações realistas que vocês executariam de fato em suas funções

---

## Debate

---

 **Duração: 15 minutos**

### Perguntas

- Como o exercício de sequenciamento da Atividade 1 preparou vocês para a simulação?
- Que desafios vocês enfrentaram ao aplicar os procedimentos reais da organização?
- Que lacunas vocês identificaram nos seus atuais procedimentos de resposta a incidentes?
- A comunicação entre os departamentos funcionou bem durante os exercícios?
- Quais treinamentos ou recursos adicionais ajudariam vocês a se sentirem mais preparados para esses cenários nos seus cargos atuais?

### Respostas/sugestões possíveis

- Desafios: coordenação entre departamentos, acesso a informações de contato reais, esclarecimento de quais são as autoridades reais e quem toma decisões
- Lacunas: caminhos de escalonamento pouco claros, informações de contato desatualizadas, autoridades de decisão indefinidas, falta de modelos de notificação
- Melhorias: treinamento multidisciplinar periódico, listas de contatos atualizadas, árvores de decisões mais claras, guias de consulta rápida específicos para cada função
- Recursos: cartões de resposta específicos para cada função, simulações regulares com membros reais da equipe, treinamento atualizado do plano de resposta a incidentes

---

## Conclusão

---

 **Duração: 5 minutos**

Resuma os pontos principais dos dois exercícios:

- O exercício de sequenciamento desenvolveu a compreensão dos procedimentos organizacionais de resposta a incidentes, enquanto a simulação de funções enfatizou os desafios de coordenação do mundo real
- A preparação individual e a resposta coordenada da equipe, utilizando funções organizacionais reais, são igualmente essenciais para uma resposta eficaz a incidentes
- As complicações são inevitáveis, e o sucesso depende da adaptabilidade dentro das estruturas estabelecidas

---

### Próximas etapas

---

- Atualizar o plano de resposta a incidentes da sua organização com base nas lacunas identificadas
- Atualizar listas de contatos e protocolos de comunicação
- Resolver as lacunas identificadas quanto à clareza das funções ou à autoridade na tomada de decisões
- Agendar exercícios simulados periódicos com membros reais da equipe de resposta a incidentes para permitir melhorias contínuas

Anexo da Atividade 1 – Listas de verificação de resposta a incidentes impressas

Imprima uma cópia desta página para cada seis participantes. Corte ao longo das linhas contínuas para criar cartões individuais e entregue um cartão a cada participante. Para maior durabilidade, imprima em cartolina ou papel de alta gramatura.



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> | <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> | <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> |
| <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> | <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> | <div><p><b>Lista de verificação para resposta rápida</b></p><ul style="list-style-type: none"><li><input type="checkbox"/> Isolar os sistemas afetados</li><li><input type="checkbox"/> Relatar o incidente imediatamente (seguindo a política de escalonamento da organização)</li><li><input type="checkbox"/> Avaliar o status do backup de dados</li><li><input type="checkbox"/> Entrar em contato com as autoridades legais (de acordo com a política da organização)</li><li><input type="checkbox"/> Acionar o assessor jurídico</li><li><input type="checkbox"/> Colocar em prática a política da organização sobre resposta a golpes com exigência de resgate (é necessário obter aconselhamento)</li><li><input type="checkbox"/> Ativar o plano de comunicação da organização para as partes interessadas</li><li><input type="checkbox"/> Documentar a cronologia do incidente</li><li><input type="checkbox"/> Seguir os procedimentos de notificação estabelecidos para os requisitos regulamentares</li><li><input type="checkbox"/> Mobilizar a equipe de resposta a incidentes</li></ul></div> |

## Anexo da Atividade 2 – Cartões de referência sobre as responsabilidades dos participantes e cartões de cenários

Imprima este anexo e corte ao longo das linhas contínuas para separar os cartões desta página.

Para maior durabilidade, imprima em cartolina ou papel de alta gramatura.



### Cartão do participante Líder de segurança de TI

Responsável pela contenção e pela análise técnica de incidentes  
Avalia o escopo e a natureza da violação de segurança  
Implementa medidas imediatas de contenção  
Lidera as atividades de análise forense  
Faz a coordenação com os fornecedores externos de segurança



### Cartão do participante Coordenador de incidentes

Líder geral de resposta a incidentes e tomador de decisões  
Coordena todas as atividades da equipe de resposta  
Toma decisões estratégicas críticas  
Informa a liderança executiva  
Aloca recursos e prioridades



### Cartão do participante Líder de comunicações

Gerencia todas as mensagens internas e externas  
Coloca em prática os planos de comunicação existentes  
Elabora as notificações para as partes interessadas  
Faz a coordenação com a equipe de mídia e relações públicas  
Monitora as redes sociais e as notícias



### Cartão do participante Assessor jurídico

Dá aconselhamento sobre implicações legais e conformidade regulamentar  
Garante a conformidade com as leis de notificação de violações  
Dá aconselhamento sobre a preservação de evidências  
Revisa todas as comunicações externas  
Faz a coordenação com as autoridades legais, se necessário



### Cartão do participante Representante de RH

Lida com os aspectos da resposta a incidentes relacionados aos funcionários  
Gerencia as comunicações internas com os funcionários  
Gerencia investigações de ameaças internas  
Coordena os serviços de suporte aos funcionários  
Providencia o necessário para assegurar a continuidade da força de trabalho



### Cartão do participante Gerente de departamento

Representa as operações das unidades de negócios afetadas  
Avalia o impacto sobre os negócios do departamento  
Implementa medidas de continuidade dos negócios  
Faz a coordenação com gerentes de outros departamentos  
Relata o status operacional ao Coordenador de incidentes



### Cenário Ataque de ransomware com roubo de dados

“Os servidores de arquivos da sua organização foram criptografados por um ransomware. Os invasores também roubaram dados financeiros de clientes e estão ameaçando divulgá-los publicamente se o resgate não for pago em 24 horas. Complicação: os sistemas de backup mostram sinais de comprometimento há duas semanas.”



### Cenário Comprometimento de e-mail corporativo

“A conta de e-mail do diretor financeiro foi comprometida e utilizada para autorizar uma transferência eletrônica de US\$ 500 mil para uma conta desconhecida. A transferência foi concluída esta manhã. Complicação: e-mails fraudulentos semelhantes foram enviados a três grandes clientes, solicitando ‘informações de pagamento atualizadas’.”



### Cenário Roubo de dados por pessoas da organização

“Um funcionário que estava deixando o departamento de TI foi flagrado copiando registros confidenciais de clientes para uma unidade USB pessoal. A segurança o deteve na saída, mas ele alega que os dados são ‘apenas arquivos pessoais de trabalho’. Complicação: o funcionário já postou mensagens enigmáticas no LinkedIn sobre ‘levar uma experiência valiosa para minha nova função’.”

## Anexo da Atividade 2 – Cartões de cenários e cartões de complicações adicionais

Imprima este anexo e corte ao longo das linhas contínuas para separar os cartões desta página.

Para maior durabilidade, imprima em cartolina ou papel de alta gramatura.



### Cenário

#### Comprometimento de cadeia de suprimentos

“ O principal fornecedor de software da sua organização informa que o servidor de atualizações deles foi comprometido e que um código malicioso pode ter sido distribuído para os clientes. Os seus sistemas receberam atualizações ontem. Complicação: o fornecedor se recusa a fornecer detalhes técnicos, alegando que está realizando uma investigação interna. ”



### Cenário

#### Violação de segurança física

“ Uma pessoa não autorizada foi encontrada na sala de servidores após o expediente com um laptop conectado à rede. A segurança a acompanhou até a saída, mas ela alegou ser ‘da equipe de suporte de TI’. Complicação: vários funcionários relatam que seus registros de acesso com crachá mostram atividades incomuns após o expediente que eles não realizaram. ”



### Cenário

#### Comprometimento de serviço na nuvem

“ Seu provedor de serviços de armazenamento na nuvem relata um acesso não autorizado ao repositório de dados da sua organização, que contém informações de clientes e segredos comerciais. A violação pode ter durado várias semanas. Complicação: a comunicação inicial do provedor da nuvem contém informações conflitantes sobre a cronologia e o escopo do incidente. ”



### Complicações adicionais

“ Alerta de mídia: um blog de tecnologia publicou um artigo sobre o incidente de segurança da sua organização com detalhes específicos que ainda não foram divulgados publicamente. ”



### Complicações adicionais

“ Notificação regulamentar: o órgão regulador do seu setor entrou em contato com você solicitando informações imediatas sobre o incidente e as suas medidas de resposta. ”



### Complicações adicionais

“ Crise com cliente: seu maior cliente convocou uma reunião de emergência para discutir a segurança dos dados deles e está ameaçando rescindir o contrato. ”



### Complicações adicionais

“ Vazamento interno: os funcionários estão discutindo os detalhes do incidente em sistemas internos de mensagens, e algumas informações parecem estar incorretas. ”



### Complicações adicionais

“ Falha de sistema: durante seus esforços de resposta, um sistema crítico para os negócios foi desligado, possivelmente devido às suas medidas de contenção. ”



### Complicações adicionais

“ Ameaça jurídica: você recebeu uma carta de um escritório de advocacia que representa os clientes afetados, exigindo informações detalhadas sobre a violação e as suas medidas de segurança. ”