

# GUIA DE RESPOSTA AO INCIDENTE

## PREPARAÇÃO

- Trabalhe com a liderança sénior da sua organização e outro pessoal relevante para desenvolver um plano de resposta a incidentes e continuidade de negócios com base nos riscos mais urgentes que foram identificados na avaliação de risco cibernético da sua organização.
  - Desenvolva cenários de ameaças para os tipos de incidentes relacionados com os riscos cibernéticos mais prioritários da sua organização. Concentre-se na capacidade de construir a resposta a esses cenários.
  - Identifique, registre e disponibilize na sua organização uma lista de pontos de contacto para a resposta ao incidente.
  - Identifique e registre informações de contacto para as autoridades e agentes policiais locais e federais.
  - Estabeleça disposições especificando que tipos de incidentes devem ser comunicados, quando devem ser comunicados e a quem.
  - Estabeleça diretrizes escritas que definem a rapidez com que o pessoal deve responder a um incidente e que ações devem ser realizadas, com base em fatores relevantes, como o impacto funcional e de informação do incidente, e a provável recuperação do incidente.
  - Informe todos os funcionários para contactarem a sua equipa técnica - mais frequentemente, será pessoal de TI e/ou CISO/CIO/outro gestor comparável - quando ocorre um incidente.
  - Implemente soluções para monitorizar as ações dos funcionários e para permitir a identificação de ameaças e incidentes.
  - Inclua planos de continuidade de negócios para coordenar como a sua organização irá trabalhar com fornecedores e clientes principais durante uma emergência empresarial, incluindo a forma como conduziria o manual ou operações empresariais alternativas, se necessário.
  - Inclua procedimentos escritos para encerramento e reinício do sistema de emergência.
  - Desenvolva e teste métodos para recuperar e restaurar os dados de cópia de segurança; teste periodicamente os dados de cópia de segurança para verificar a sua validade.
  - Tenha acordos e procedimentos estabelecidos para realizar operações comerciais numa instalação/local alternativo.
  - Tenha um canal de difusão claro implementado para todos os clientes.

## EXERCÍCIO

- Organize pequenos exercícios de mesa com todos os funcionários ou representantes de todos os níveis de pessoal, incluindo executivos da organização, pessoal de PR/comunicações e equipas legais e de conformidade.
- Identifique e participe idealmente em exercícios de simulação de toda a indústria relevantes para a sua organização.
- Establish process to ensure lessons learned from exercises are incorporated and addressed in your company's cybersecurity strategy.

## RESPONDER

- Implemente ações do plano de resposta a incidentes para minimizar o impacto, incluindo o que respeita a danos na reputação.
- Identifique sistemas afetados/comprometidos e avalie os danos.
- Reduza os danos removendo (desligando) os ativos afetados.
- Comece a registar todas as informações assim que a equipa suspeitar que ocorreu um incidente. Tente preservar a evidência do incidente ao desligar/isolar o ativo identificado afetado, por exemplo, recolha os registos de configuração do sistema, rede e deteção de intrusão dos ativos afetados.
- Notifique as partes internas apropriadas, fornecedores terceiros e autoridades e solicite assistência, se necessário.
- Inicie as atividades de notificação e assistência ao cliente em conformidade com as leis, regulamentos e orientações interagências.
- Utilize plataformas de partilha de ameaças como a FS-ISAC ou a MISP para notificar a indústria sobre a ameaça.
- Documente todos os passos que foram tomados durante o incidente para rever mais tarde.

## RECUPERAR

- Restaura os ativos recuperados para "pontos de recuperação" periódicos, se disponíveis, e utilize os dados de cópia de segurança para restaurar os sistemas para o último estado "bom" conhecido.
- Crie cópias de segurança "limpas" de ativos restaurados e certifique-se de que todas as cópias de segurança de ativos críticos são armazenadas num local física e ecologicamente seguro.
- Teste e verifique se os sistemas infetados estão totalmente restaurados. Confirme que os sistemas afetados estão a funcionar normalmente.

## REVER

- Realize uma discussão de "lições aprendidas" depois de o incidente ter ocorrido - reúna-se com o pessoal sénior, consultores de confiança e o(s) fornecedor(es) de suporte informático para rever possíveis vulnerabilidades ou recomendar novos passos a implementar.
- Se possível, identifique as vulnerabilidades (quer em software, hardware, operações comerciais ou comportamento pessoal) que levaram ao incidente e desenvolva um plano para mitigar as mesmas.
- Desenvolva um plano de monitorização para detetar incidentes semelhantes ou adicionais relacionados com os problemas identificados.
- Partilhe lições aprendidas e informações sobre o incidente sobre plataformas de partilha de ameaças, como o FS-ISAC.
- Integre as lições aprendidas nos protocolos de resposta a incidentes da sua organização.

