Capítulo 7

# Resposta a incidentes de segurança

As empresas passam por crises diversas, e, com a especialização de criminosos virtuais, com ataques cada vez mais sofisticados, tornam-se essenciais alguns planos para prevenção e gerenciamento de crises no setor de tecnologia. Neste capítulo abordaremos conceitos importantes, como o gerenciamento de crises e incidentes de segurança e como promover um planejamento estratégico e prático para essas situações.

Vamos lá?

# 1 Fundamentos de grupos de segurança e resposta a incidentes (CSIRTs)

As empresas que trabalham com dados virtuais estão cada vez mais propensas a ataques cibernéticos. Para lidar com diferentes tipos de ameaça, as organizações criam os chamados grupos de resposta a incidentes de segurança em computadores (computer security incident response team – CSIRT), cuja função é identificar o problema e criar planos/estratégias para combatê-los.

Para Scarfone et al. (2008), cada instituição, dentro de seus contextos, cria maneiras de responder a esses incidentes. A figura 1 a seguir mostra de forma generalizada os passos que regem a resposta a ataques:

**Figura 1 – Ciclo de vida da resposta a incidentes**


Fonte: adaptado de Scarfone et al. (2008).

Sendo assim, os CSIRTs são responsáveis por passar à empresa informações relevantes que possam ajudá-la em momentos de crise. Eles recebem, analisam e respondem notificações e atividades referentes aos problemas de segurança nos computadores, indicam quais ferramentas, tecnologias e recursos as empresas podem utilizar para se protegerem, além de terem como objetivo principal manter a segurança da informação e estar de acordo com a Lei Geral de Proteção de Dados.

# 2 Conceitos de gerenciamento de crise

Crise é um momento peculiar, difícil, perigoso ou decisivo na vida de pessoas, empresas e instituições. Tem características gerais e

singulares dependendo do setor, do contexto dinâmico sociopolítico e do ambiente econômico (ESESP, 2018).

À medida que as organizações começam a implantar o seu mecanismo de resposta a incidentes, elas procuram determinar a melhor estratégia para montar esta estrutura (CERT, 2004). Assim, as empresas têm adotado estratégias de segurança robustas e, dentre elas, surge a criação de um grupo de resposta a incidentes de segurança em computadores, conhecido pela sigla CSIRT (computer security incident response team).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2004), cada grupo é criado de acordo com a demanda e as particularidades da empresa, sem funções padronizadas, podendo criar planos para ajudar de forma personalizada. Apesar de haver diferenças nos planos de ação, existem pontos-chave que devem constar na CSIRT, como: apoio dos superiores (que auxiliarão na área de atuação de cada profissional envolvido no processo), definição de um plano estratégico (prazos, organização), coleta de informações significativas para o contexto (definição de qual foi o incidente e suas consequências para o ambiente de trabalho e produto), identificação dos componentes-chave que deverão constar no CSIRT, implementação e anunciação e, por fim, avaliação da eficácia do grupo.

As motivações para o estabelecimento de CSIRTs incluem, segundo o Cert (2004):

- um aumento generalizado na quantidade de incidentes de segurança sendo reportados;
- um aumento generalizado na quantidade e variedade de organizações sendo afetadas por incidentes de segurança em computadores;

- uma maior consciência, por parte das organizações, da necessidade de políticas e práticas de segurança como parte das suas estratégias globais de gerenciamento de riscos;
- novas leis e regulamentos que afetam a maneira como as organizações precisam proteger as suas informações;
- a percepção de que administradores de redes e sistemas não podem proteger sozinhos os sistemas e as informações da organização.

A incidência de ataques se torna cada vez mais presente por conta da criação de ferramentas mais agressivas na busca de informações dentro dos sistemas de segurança virtuais. A criação dos grupos mostra que não existe somente uma solução, mas sim muitas possibilidades de combater essas ameaças, que dependem das necessidades e dos contextos de cada organização.

# 3 Planejando a crise

Prevenção: análise de risco, levantamento (diagnóstico) de situação atual; mapeamento detalhado dos pontos vulneráveis. Neste momento, a empresa enxerga os pontos que precisam de atenção e identificam as crises.

- Transparência: números amplamente divulgados, gerenciamento participativo e equipes multifuncionais. Para a instituição trabalhar de forma harmoniosa, ele deve saber lidar com seus funcionários, entender o que está acontecendo e contar com todos os recursos para se recuperar.
- Elaborar um manual de gerenciamento de crise: cada empresa sabe quais são suas necessidades e demandas. Portanto, é importante que saiba identificar seus pontos "indefesos", problemas

que podem se tornar maiores (crise) e como enfrentar os possíveis ataques.

- Atuar com uma gestão profissional: os responsáveis da organização precisam estar capacitados (técnicos) para que possam, da melhor maneira possível, trabalhar a crise em sua totalidade, especialmente no resgate e na reconquista da confiança por parte de seus funcionários e clientela.

- Organização de um comitê de crises: é necessário que a organização tenha um comitê de crises com a participação de dirigentes e colaboradores de áreas estratégicas, como comunicação e marketing, jurídica, recursos humanos, tecnologia, administrativo-financeira, os quais são responsáveis por todas as ações a serem tomadas em um momento de crise.

Esse comitê é responsável, entre outras atividades, por:

- Assessorar na tomada de decisões.
- Responder com agilidade aos questionamentos.
- Integrar-se a todos os setores da organização, conhecendo detalhes e variáveis dos conflitos.
- Levantar soluções para o bom relacionamento com os públicos envolvidos e a imprensa.

Segundo o Cert (2004), a análise dos recursos a seguir auxiliará também nesse processo de planejamento:

- organogramas da empresa e de unidades de negócio específicas;
- topologias de redes e sistemas da organização ou da comunidade que será atendida;
- inventários dos sistemas e recursos críticos;
- planos existentes de recuperação de desastres ou de continuidade dos negócios;

- normas existentes para comunicar violações de segurança física;
- quaisquer planos de resposta a incidentes já existentes;
- quaisquer regulamentos institucionais existentes;
- quaisquer políticas e procedimentos de segurança existentes.

Para auxiliar o planejamento da elaboração de um manual de gerenciamento de crise, existe uma ferramenta importante conhecida como 5W2H. De acordo com Avila et al. (2016), a sigla resumidamente responde às seguintes questões:

- What: o que será feito?
- Why: por que será feito?
- Where: onde será feito?
- When: quando será feito?
- Who: por quem será feito?
- How: como será feito?
- How much: quanto vai custar?

Essa ferramenta foi criada no Japão com foco na fase do planejamento. São ações previamente estabelecidas que auxiliam no desenvolvimento e mapeamento de questões em momentos de crise. Ela pode ser considerada uma checklist que tem como objetivo garantir que todas as fases do gerenciamento de crise ocorram de forma harmoniosa e efetiva, sem que haja dúvida nos responsáveis envolvidos (gestores e colaboradores).

Portanto, o conhecimento das respostas destas perguntas básicas é essencial para o desenvolvimento da execução da ação pretendida dentro de uma organização, e podem ser utilizadas como roteiro, além de ser possível organizá-las conforme as necessidades internas (AVILA et al., 2016).

# 4 Análise de risco e ranking dos riscos

A análise de riscos na segurança da informação é um processo que busca identificar falhas e vulnerabilidades que podem expor dados e informações da empresa a ameaças. Nessa análise são avaliadas situações e suas prováveis consequências em configurações de redes, problemas em aplicativos, softwares que podem causar falhas futuras, entre outras situações que podem fragilizar a instituição (ABNT, 2009).

A identificação dos riscos é fundamental para que os responsáveis dentro da empresa possam classificar e rankear as ameaças de forma que fiquem claras e seja possível estabelecer as prioridades na tomada de decisões. São considerados também neste momento as probabilidades de acontecimento e recorrência do risco.

Sendo assim, deve-se fazer uma análise das causas (por responsáveis qualificados e especializados na questão de riscos), fontes, consequências positivas e negativas para ação contra o ataque, e como a ação deve ser conduzida, além da sua eficiência no controle do problema.

Ao rankear um risco, os responsáveis ponderam o contexto, a dimensão do problema e as consequências que essa ameaça trará para o ambiente de trabalho. Para definir a prioridade, a empresa procura analisar requisitos legais, regulatórios e outras questões que serão determinantes no momento da tomada de decisão e ação contra o risco, como gastos e continuação das atividades da instituição. Por conseguinte,

> Em algumas circunstâncias, a avaliação de riscos pode levar à decisão de se proceder a uma análise mais aprofundada. A avaliação de riscos também pode levar à decisão de não se tratar o risco de nenhuma outra forma que seja manter os controles existentes. Esta decisão será influenciada pela atitude perante o risco da organização e pelos critérios de risco que foram estabelecidos (ABNT, 2009, p. 18).

As ameaças são riscos como danos físicos, eventos naturais, paralisação de serviços essenciais, comprometimento da informação, falhas técnicas, ações não autorizadas, e comprometimento de funções. Consideram-se então, de forma generalizada, os riscos, a gestão dos riscos, os envolvidos, a fonte do risco, evento (ocorrência ou mudança), consequência, probabilidade e controle de mecanismos para lidar com as ameaças que podem acometer a empresa.

# 5 Conceitos de incidentes de segurança

Os incidentes de segurança podem ser definidos como quaisquer eventos adversos, confirmados ou sob suspeita, relacionados à segurança dos sistemas de computação ou das redes de computadores. São considerados eventos indesejados ou até mesmo inesperados. De acordo com a ABNT (2005), eles podem provocar obstrução ou erro no momento da execução de processos organizacionais, causar dificuldades em ação dos agentes organizacionais (tanto humanos quanto computacionais), prejudicar o desempenho das atividades da empresa e impactar de forma significativa a performance da equipe como um todo.

Os incidentes são, na verdade, os eventos negativos que ocorrem na segurança da informação. Quanto mais incidentes ocorrem dentro de uma empresa, maiores são as probabilidades de outros acontecerem. Para evitar que isso aconteça, os gestores precisam criar mapeamentos das ocorrências para identificar o que está causando o problema.

# 6 Plano de respostas a incidentes

Plano de resposta a incidentes (IRP) é um conjunto de instruções impressas que definem como a empresa deve reagir a um ciberataque. Tem por objetivo preparar a empresa para lidar com uma situação de invasão nos sistemas e minimizar danos ao negócio, procurando ser

eficiente e rápida no restabelecimento do sistema, reduzindo o tempo de resposta ao ataque e consequentemente os custos de recuperação (CERON et al., 2009).

Conforme já citado em tópicos anteriores, após criar o plano, é importante que se tenha um backup atualizado, criação de tabela com possíveis incidentes de segurança e como se prevenir e manter-se atualizado em regulamentações e leis vigentes.

Pesquisar o custo-benefício de ter uma equipe de segurança da informação terceirizada e contratar um seguro cibernético podem ser medidas importantes a se considerar.

De acordo com Ceron et al. (2009), o processo que envolve a resposta aos incidentes engloba cinco pontos:

- Identificação: saber se realmente há um problema.
- Coordenação: a equipe responsável precisa identificar e quantificar os danos, para depois traçar um plano de ação para resolvê-lo.
- Mitigação: isolar o problema, determinar sua intensidade e evitar que haja propagação.
- Investigação: time de resposta coleta e analisa as evidências.
- Educação: avaliar o processo e verificar a efetividade do plano colocado em prática.

# 7 Incidentes mais comuns

Como exemplos de incidentes de segurança, temos:

- Investidas para tentar acessar um canal não autorizado a sistemas ou a seus dados.
- Promoção de uma interrupção indesejada ou negação de serviço.

- Realizar o uso não autorizado de um sistema para processamento ou armazenamento de dados.
- Modificar características de hardware, firmware ou software de um sistema, sem conhecimento, instruções ou consentimento prévio do responsável por uma empresa.

Um incidente muito comum que ocorre no meio virtual é conhecido como phishing, que significa 'fisgar'. Esta técnica nada mais é do que manipular, enganar as pessoas para que compartilhem suas informações confidenciais, como senhas e números de cartão de crédito.

As empresas devem buscar meios de evitar essas ocorrências e proteger tanto os negócios quanto os usuários que dela dependem. Portanto, ter uma boa equipe de gestão de riscos é mostrar à clientela que ela pode confiar no trabalho oferecido.

**PARA SABER MAIS**

Recentemente, a empresa Eletronic Arts sofreu um ataque hacker em que teve códigos-fontes roubados, além da exposição de uma grande quantidade de dados. Para conhecer melhor o ocorrido, acesse a matéria na página da Tecmundo (PALMEIRAS, 2021).

# 8 Como recuperar incidentes

Após a ameaça, o incidente e o dano causado, temos a situação de recuperação de incidentes.

Nesta etapa acontece a recuperação do incidente e o retorno à operação normal. As etapas que envolvem a recuperação, conforme já discutido, são identificação, coordenação, mitigação, investigação e educação. As medidas de segurança adotadas aqui são corretivas e avaliativas. É importante possuir um plano de retorno para os ativos de

segurança, de forma que as atividades de retorno não se tornem ameaças reais para a continuidade da operação (PORTAL ISO 27000, 2021).

Assim, tem-se como objetivo central o de minimizar as consequências e tomar as medidas para a volta da operação normal do negócio em um tempo razoável, o que pode ocorrer mesmo se o incidente ainda estiver em curso.

Cada empresa determina o plano de respostas a incidentes de segurança, focando em suas prioridades, especialmente podendo continuar a operar, mesmo com a ameaça ainda presente. Contudo, antes da elaboração do plano de recuperação de acidentes, é imprescindível que a empresa tenha outras ações já elaboradas:

- Plano de continuidade de negócio: prosseguir mesmo com a presença do risco em operação.
- Avaliação de riscos: quais são os danos mais importantes e que devem ser tratados de forma mais urgente.
- Análise de impacto de negócios (BIA): análise de processos e recursos de uma empresa, tempo de recuperação após um ataque e impactos de uma possível inatividade.

A recuperação de cada organização está diretamente relacionada a seus gestores e os planos de ação que são traçados por eles. Definir prioridades e agir de forma rápida e eficiente garantem que haja continuidade dos negócios e credibilidade frente ao mercado.

# 9 Treinar os funcionários em caso de incidentes

O treinamento dos funcionários da empresa é fundamental para qualquer função, pois promove uma reavaliação de posturas e técnicas adotadas, bem como desenvolve competências técnicas e comportamentais essenciais ao negócio.

Um elemento necessário em relação aos planos é fazer sua divulgação entre os membros da empresa, especialmente entre aqueles que serão responsáveis por executá-los, se necessário. Além disso, é preciso testar os planos. Para isso, pode-se fazer uso de diferentes opções, desde uma revisão da lista de verificação (checklist) de recuperação criada pelas necessidades de cada empresa até um teste de interrupção completa (full interruption test), onde as operações são interrompidas no lugar primário e transferidas para um lugar de recuperação.

De acordo com Baars (2018, p. 142):

> O propósito de um processo de gerenciamento de incidentes é garantir que os incidentes e as deficiências relacionadas aos sistemas de informação sejam conhecidos, de forma que as medidas apropriadas possam ser tomadas em tempo hábil.
>
> Funcionários, pessoal temporário e usuários externos devem estar todos cientes dos procedimentos para reportar os vários tipos de incidentes e deficiências que possam influenciar a confiabilidade da informação e a segurança dos ativos da empresa.
>
> Deve ser requerido aos funcionários e usuários que reportem o mais rápido possível todos os incidentes e deficiências à central de atendimento ou a uma pessoa de contato. Naturalmente, é do interesse de todos que a organização responda rapidamente.

Assim, pontos importantes a serem tratados com os funcionários são: reconhecimento das técnicas de phishing; deixá-los cientes de que o fortalecimento de senhas é fundamental; treiná-los para saberem identificar e lidar com ameaças e riscos que podem acometer o ambiente de trabalho; e orientá-los a como conduzir uma resposta efetiva ao problema.

## Considerações finais

Vimos neste capítulo que crises são comuns no cenário organizacional, e o setor de tecnologia da informação tem sido alvo de muitos

incidentes. Os profissionais gestores devem atentar-se sempre aos ataques que podem ocorrer que prejudiquem o andamento do negócio.

Sabemos que nenhuma empresa está livre de sofrer ameaças e ter suas operações colocadas em risco. Porém, contar com uma equipe qualificada e determinada a prevenir ameaças e identificar riscos para eliminá-los é a chave para a continuação do empreendimento.

Elaborar planos de ação e agir de forma estratégica, envolvendo todo o time necessário, pode ser um diferencial e ajudará na proteção contra os riscos de segurança.

# Referências


ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 17799** – Gestão de incidentes de segurança da informação e melhorias. Rio de Janeiro: ABNT, 2005.

AVILA NETO, Clovis Antunes de et al. Aplicação do 5W2H para criação do manual interno de segurança do trabalho. **Espacios**, v. 37, n. 20, ano 2016, p. 19. Disponível em: https://www.revistaespacios.com/a16v37n20/16372019.html. Acesso em: 1 jul. 2021.

BAARS, H. et al. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Criando um Grupo de Respostas a Incidentes de Segurança em Computadores**: Um Processo para Iniciar a Implantação. 2004. Disponível em: https://www.cert.br/certcc/csirts/Creating-A-CSIRT-br.html. Acesso em: 1 jul. 2021.

CERON, J. et al. O processo de tratamento de incidentes de segurança da UFRGS. WORKSHOP DE TECNOLOGIA DA INFORMAÇÃO DAS IFES, 3., 2009, Belém. **Anais**... Belém: UFPA, 2009.. Disponível em: https://lume.ufrgs.br/handle/10183/16096. Acesso em: 1 jul. 2021.

ESESP. **Gerenciamento de crise**: eixo comunicação. 2018. Disponível em: https://esesp.es.gov.br/Media/esesp/Apostilas/Gerenciamento%20de%20Crise.pdf. Acesso em: 1 jul. 2021.

PALMEIRAS, Carlos. EA sofre ataque hacker e tem dados de FIFA 21 e Frostbite roubados. **Tecmundo**, [s.l.], 10 jun. 2021. Disponível em: https://www.tecmundo.com.br/voxel/218971-ea-sofre-ataque-hacker-tem-dados-fifa-21-frostbite-roubados.htm. Acesso em: 01 jul. 2021.

PORTAL ISO 27000. **Ciclo de vida de um incidente**. 2021. Disponível em: http://www.iso27000.com.br/index.php/site-map/articles/78-ciclo-de-vida-de-um-incidente. Acesso em: 1 jul. 2021.

SCARFONE, Karen et al. **Computer security incidente handling guide**. Gaithersburg: Nist, 2008. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final. Acesso em: 01 jul. 2021.