Segurança em Ação: Tratamento e Respostas a Incidentes

every

CYBERSECURITY GRC PRIVACY

UN GLOBAL COMPACT

CERTIFICADA ISO 27001 SEGURANÇA DA INFORMAÇÃO

CERTIFICADA ISO 27701 PRIVACIDADE DA INFORMAÇÃO

O presente Ebook abordará a adoção de medidas e práticas fundamentais para proteger sistemas de informação contra ameaças de segurança. Entre as recomendações indicadas, destacam-se os esforços em prol da implementação de políticas, procedimentos e controles de segurança — incluindo firewalls, criptografia, autenticação e gestão de acesso.

Segurança da Informação

No contexto organizacional, a área de Segurança da Informação é responsável por coordenar as atividades de proteção dos ativos informacionais. Em geral, isso compreende adotar um conjunto de medidas e práticas de segurança, as quais incluem identificar ameaças, usar senhas fortes, manter sistemas atualizados e preparar planos de ação para eventuais problemas.

Iniciativas de caráter preventivo evitam incidentes, garantindo a segurança das informações e mantendo a privacidade (tanto das pessoas quanto das organizações). De modo a alcançar tais objetivos, três pilares sustentam a Segurança da Informação:

Confidencialidade **Integridade** **Disponibilidade**

Confidencialidade:
Refere-se à garantia de que as informações são acessíveis apenas para pessoas autorizadas. Isso envolve proteger os dados contra acessos não autorizados, vazamentos ou divulgações indevidas.

Integridade:
Envolve garantir que as informações são precisas, completas e livres de qualquer alteração não autorizada. A integridade das informações é fundamental para evitar manipulações indesejadas e garantir a confiabilidade.

Disponibilidade:
Consiste em garantir que as informações e sistemas estejam acessíveis e operacionais quando necessário, sem interrupções indevidas. A disponibilidade assegura que os recursos e serviços de TI estejam disponíveis para uso, de forma contínua e confiável.

TRATAMENTO E RESPOSTAS A INCIDENTES

Quando algum desses pilares é comprometido, ocorre um Incidente de Segurança da Informação. Esse tipo de evento pode incluir violação de dados, ataques cibernéticos, perda de informações, interrupções de serviço, entre outros incidentes relacionados à segurança.

Exemplos de Incidentes:

Phishing:

Ataque no qual criminosos personificam entidades confiáveis, com o objetivo de enganar a vítima, convencendo-a a compartilhar informações pessoais e confidenciais.

Vazamento de Dados:

Exposição não autorizada de dados pessoais e informações privadas.

Operação inadequada:

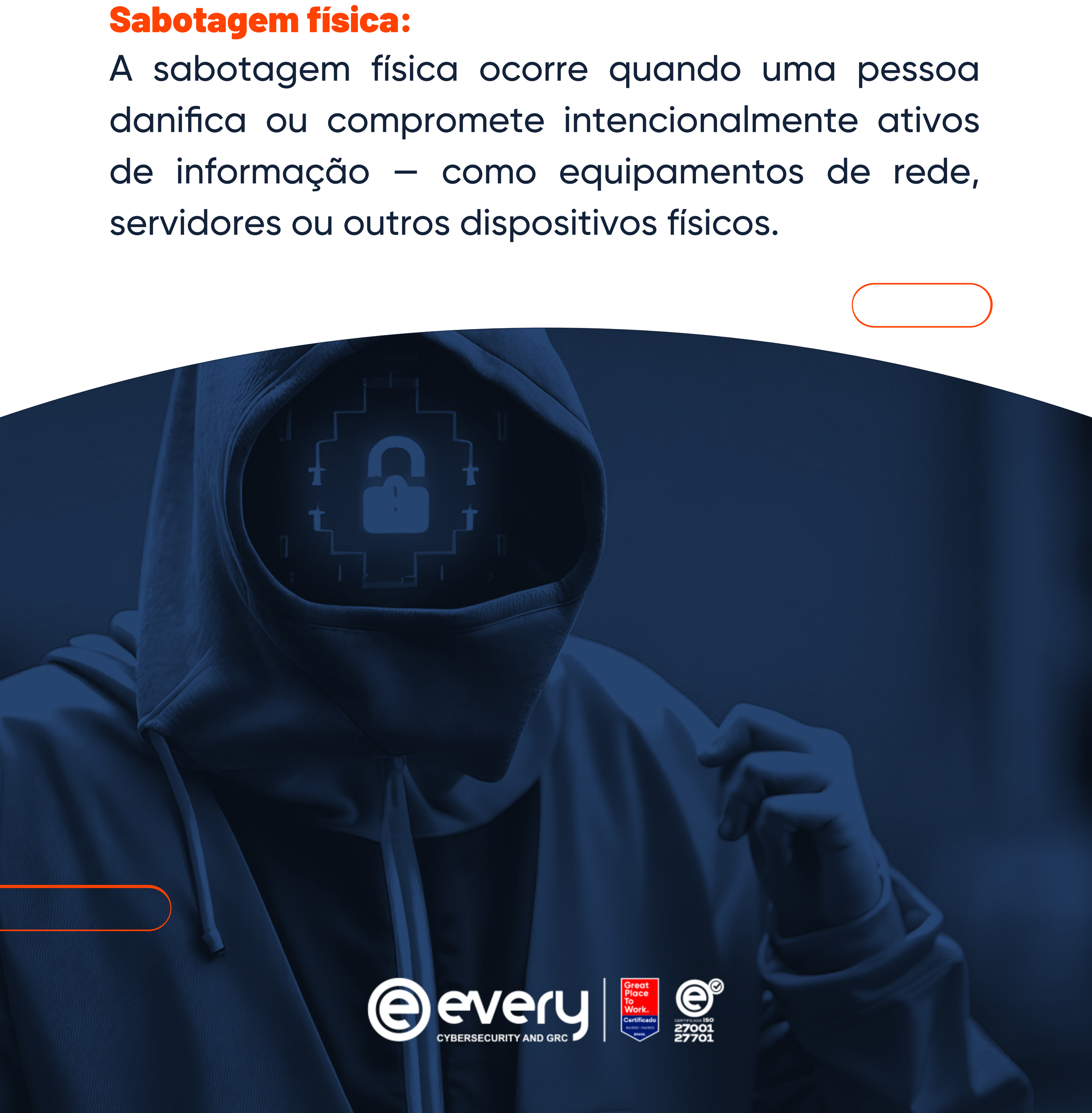
Uso impróprio de aparelhos da organização. Exemplos nesse sentido incluem a instalação de softwares não autorizados ou a utilização de ferramentas institucionais para a realização de projetos pessoais.

Ransomware:

Ataque envolvendo um *software* malicioso que criptografa arquivos, tornando-os inacessíveis. Sob a promessa de descriptografá-los, em geral, os cibercriminosos exigem um resgate.

Sabotagem física:

A sabotagem física ocorre quando uma pessoa danifica ou compromete intencionalmente ativos de informação — como equipamentos de rede, servidores ou outros dispositivos físicos.



Coloque boas práticas em ação:

Treinamentos de conscientização:

Realize treinamentos regulares de conscientização em segurança da informação, abordando assuntos relacionados às melhores práticas de segurança — identificar ameaças, evitar phishing, proteger informações sensíveis etc.

Controle de acessos:

Implemente um sistema de controle de acesso, de modo a garantir que informações confidenciais estejam disponíveis somente para pessoas autorizadas. Isso pode ser alcançado mediante adoção de autenticação em dois fatores, restrições de privilégios e revisões periódicas de acesso.

Segurança física:

Mantenha as instalações físicas seguras, mediante restrição de acesso a áreas sensíveis. Esse controle de segurança também pode envolver a adoção de medidas contra roubo e/ou contra perda de dispositivos.

Atualizações:

Mantenha todos os sistemas e softwares corporativos atualizados, pois instalar as versões mais recentes evita que ativos possuam vulnerabilidades conhecidas.

Monitoramento de rede:

Implemente soluções de monitoramento contínuo na rede, de modo a detectar invasões e atividades suspeitas passíveis de constituir uma violação de segurança.

Backup e recuperação de dados:

Realize backups regulares de todos os dados críticos da organização e teste periodicamente o processo de recuperação, para garantir a eficácia dos backups em caso de crise.

Gerenciamento de dispositivo móvel:

Estabeleça políticas e procedimentos de segurança específicos para os dispositivos móveis utilizados pelos funcionários.

Gerenciamento de vulnerabilidades:

Realize avaliações regulares de vulnerabilidade em sistemas e redes corporativas, com o objetivo de identificar falhas de segurança e corrigi-las ou mitigá-las o mais rápido possível.

VPN:

Utilize uma VPN (Rede Privada Virtual) criptografada ao conectar dispositivos remotos aos servidores organizacionais. Isso adicionará uma camada adicional de proteção contra ataques cibernéticos.

Autenticação multifator:

Habilite a autenticação de múltiplos fatores para acessar os sistemas da organização. Essa camada extra de segurança deve ser implementada em conjunto com senhas fortes, especialmente para evitar roubos de logins por cibercriminosos.

ISO 27001:2022 e a Segurança da Informação:

A norma ISO 27001:2022 é um padrão internacional que estabelece requisitos para um Sistema de Gestão da Segurança da Informação. Esse documento contém um conjunto abrangente de controles e processos recomendados para que organizações gerenciem riscos de Segurança da Informação.

every
CYBERSECURITY AND GRC

Great Place To Work. Certificado

CERTIFICADA ISO 27001 27701

Esse normativo auxilia na implementação de medidas adequadas para proteger as informações e os ativos da organização — garantindo a confidencialidade, integridade e disponibilidade dos dados.

Nesse sentido, a ISO 27001:2022 desempenha um papel importante como guia de boas práticas. As determinações apresentadas orientam a identificar, avaliar e tratar os riscos de segurança, de forma sistemática e contínua.

Ao adotar a ISO 27001:2022 e estabelecer uma estrutura de gestão eficaz, as organizações demonstram compromisso com a Segurança da Informação. Como resultado, atinge-se uma maturidade elevada no que se refere à capacidade de lidar com riscos e desafios de segurança

SIEM: Monitoramento a fim de evitar o incidente

O Gerenciamento de Informações e Eventos de Segurança (SIEM) é uma tecnologia que monitora o ambiente organizacional, de modo a evitar incidentes de segurança.

Esse tipo de solução de segurança analisa diversos processos de forma automatizada – como logs de firewall, dispositivos de segurança e sistemas hospedeiros – e correlaciona os resultados.

A partir da identificação dos dados que circulam na rede e do uso de regras de segurança pré-definidas, o SIEM alerta sobre possíveis ameaças, detectando anomalias e atividades suspeitas. Essa ferramenta auxilia na prevenção e resposta a incidentes de segurança.

Classificação dos níveis de incidente acordo com o NIST 800-61:

O NIST 800-61 é um guia publicado pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) onde fornece orientações detalhadas para que as organizações possam se preparar para lidar com incidentes de segurança cibernética de maneira eficaz.

Nível 1	Não houve nenhum efeito na capacidade da organização de fornecer todos os serviços a todos os usuários.
Nível 2	O efeito foi mínimo, a organização ainda pode fornecer todos os serviços críticos para todos os usuários.
Nível 3	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Nível 4	A organização não é mais capaz de fornecer alguns serviços críticos a nenhum usuário.

Quando notificar autoridades?

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) obriga os responsáveis pelo tratamento de dados pessoais a informar, à Autoridade Nacional de Proteção de Dados (ANPD), sobre qualquer incidente de segurança que possa resultar em risco ou dano significativo aos titulares dos dados. Quando trata-se de organizações gov.br, também é necessário notificar ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov)

O prazo para notificar a ANPD sobre tais incidentes é de 72 horas (3 dias úteis) após a descoberta do ocorrido. A comunicação sobre o evento deve incluir informações como o nome do responsável pelo tratamento dos dados, o tipo de incidente, a data e hora do incidente, uma descrição do ocorrido, o impacto do incidente, as medidas adotadas para mitigá-lo e quaisquer informações adicionais relevantes.

Nesse sentido, destaca-se que a ANPD possui autoridade para conduzir investigações, atuando para garantir a proteção dos direitos dos titulares dos dados pessoais.

Diferenciação: Incidentes Cibernéticos e Incidentes de Segurança da Informação

Incidente Cibernético:

Incidente cibernético é uma categoria específica no campo da Segurança da Informação, trata-se de violações a computadores, redes ou sistemas de comunicação. A título de exemplo: ataques de negação de serviço (DDoS), ataques de phishing e criptografia de dados.

Incidente de Segurança da Informação:

Por outro lado, um incidente de Segurança da Informação se caracteriza por ser mais amplo, visto que inclui eventos como perda ou roubo de dispositivos físicos e acesso não autorizado a informações confidenciais.

Etapas do processo de tratamento do incidente cibernético:

Além de abordar métodos e boas práticas para a prevenção dos incidentes, faz-se necessário reiterar as medidas de remediação e resolução de eventos de segurança. A fim de preparar organizações para uma reação rápida e eficaz, o framework NIST SP 800-61 estrutura um Plano de Resposta, durante a crise, em quatro etapas.

01 Fase de Preparação:

Nessa etapa, ocorre a preparação para lidar com um incidente. Isso envolve desenvolver um plano de resposta a incidentes, estabelecer papéis e responsabilidades claras e testar o plano para garantir sua eficácia.

02

Fase de Detecção e Análise:

Nessa fase, o foco está na detecção e análise de incidentes. Isso inclui monitorar constantemente os sistemas em busca de atividades suspeitas, investigar os incidentes identificados, bem como avaliar a gravidade e o impacto de cada incidente.

03 Fase de Contenção, Erradicação e Recuperação:

Nessa etapa, são implementadas medidas para conter, eliminar o incidente e restaurar os sistemas afetados. Isso pode envolver ações como isolar o sistema comprometido, remover malwares presentes, recuperar dados perdidos e corrigir as vulnerabilidades que foram exploradas.

04

Fase de Ações Pós-Incidente:

Nessa fase, é realizada uma análise detalhada do incidente. Para evitar que ele ocorra novamente, são adotadas algumas medidas — as quais incluem: documentar o incidente, identificar suas causas raiz, bem como implementar melhorias na postura de segurança, como atualizações de políticas e procedimentos, treinamento adicional e aprimoramento das medidas de segurança em geral.

every

CYBERSECURITY AND GRC

every.com.br (61) 3548-1994 everycybersecurity contato@every.com.br