

REPORTAR INCIDENTE DE SEGURANÇA

Interno

HOME

PERGUNTAS FREQUENTES:

O que é um incidente de segurança da informação?

Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação.

São exemplos de incidentes de segurança da informação: furto de equipamentos que contenham informações institucionais, vazamento de informações não públicas (considerar que esta propriedade pode variar durante o ciclo de vida da informação), e-mails enviados sem autorização do remetente a partir do e-mail institucional (@scielo.org), e-mails suspeitos não classificados como SPAM que principalmente tenham por finalidade coletar informações pessoais, comprometimento da integridade da informação, perda de informações institucionais, etc.

Por que devo reportar incidentes?

Reportar incidentes de segurança desempenha um papel importante na segurança da informação dentro do SciELO, bem como na segurança da Internet de modo geral. Quanto mais se sabe sobre os principais incidentes, melhor será a compreensão sobre as ameaças existentes. Isso aumenta a capacidade de responder a casos futuros e fortalece os planos e procedimentos de contingência do SciELO, nos auxiliando na análise dos riscos de segurança oferecendo dados para o estabelecimento dos projetos em torno do assunto. Em outras palavras, a notificação de incidentes permite gerar estatísticas, correlacionar dados e identificar tendências que ajudarão a elaborar recomendações e materiais de apoio, a orientar campanhas para adoção de boas práticas e a estabelecer ações em cooperação.

Para quem devo notificar os incidentes ocorridos no SciELO?

É possível reportar um incidente de segurança no SciELO enviando um e-mail para helpdesk@scielo.org, ou utilizando o [Suporte SciELO](#).

Um incidente de segurança da informação está sempre relacionado à TI?

Não. No entanto, como há um grande volume de informações armazenadas em meio eletrônico, boa parte dos incidentes de segurança reportados estão relacionados aos serviços e soluções de tecnologia da informação.

Quais informações devo incluir em uma notificação de incidentes?

A ideia principal que deve-se ter em mente é a coleta e o armazenamento de evidências. Para que os responsáveis pela rede de onde partiu o incidente possam identificar a origem da atividade é necessário que a notificação contenha dados que permitam esta identificação.

São dados essenciais a serem incluídos em uma notificação:

- nome, departamento, e-mail e telefone da pessoa que reporta o incidente;
- data, horário e timezone (fuso horário) da ocorrência da atividade sendo notificada;
- localização (onde ocorreu o incidente?)
- qual é o tipo do incidente? (vírus, roubo, invasão, spam, etc.)
- qual foi o efeito do incidente?
- como ele foi descoberto
- demais dados do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

Observa-se que para cada tipo de incidente existem informações específicas que podem ser coletadas. Estes detalhes serão apresentados ao usuário no momento que selecionar a categoria do incidente a ser reportado no Suporte SciELO.

Onde posso encontrar outras informações a respeito de notificações de incidentes?

O CERT.br mantém uma FAQ (Frequently Asked Questions) com respostas para as dúvidas mais comuns relativas ao processo de notificação de incidentes. A FAQ pode ser encontrada em: <http://www.cert.br/docs/faq1.html>.

Revision #2

Created 3 May 2022 16:40:53 by Rondineli G. Saad

Updated 23 February 2023 18:23:57 by Rondineli G. Saad