Comunicar para Educar
Janeiro/2023 - Ano 4 - nº 35

# BIM
Boletim Informativo Mensal

Documento atualizado em 07/02/2023

## Saiba o que é *Cyberbullying* e como evitar que crianças sejam vítimas deste abuso.

A intimidação sistemática *on-line*, conhecida como *bullying* virtual ou *Cyberbullying*, é caracterizada por ofensas recorrentes, acarretando desconforto e sentimentos negativos a quem é vítima. O fato de ser feito virtualmente agrava o problema, já que pode partir de qualquer lugar e a qualquer momento.

Quando a vítima é uma criança, as intimidações causam ainda mais traumas, como estresse, ansiedade e outros problemas psicológicos. Portanto, é importante saber identificar situações de risco e proteger os pequenos.

Aqui vão algumas dicas para reconhecer efeitos de *bullying* virtual:

- esteja atento às alterações de comportamento, como desgaste físico e psicológico, alterações do sono, ansiedade ou se estiver evitando a *internet* ou a escola;


- reconheça a diferença entre brincadeiras e *cyberbullying*: insultos repetitivos que causam sentimento de incapacidade ou vergonha e tristeza, vindos de várias pessoas simultaneamente, indicam abusos; e

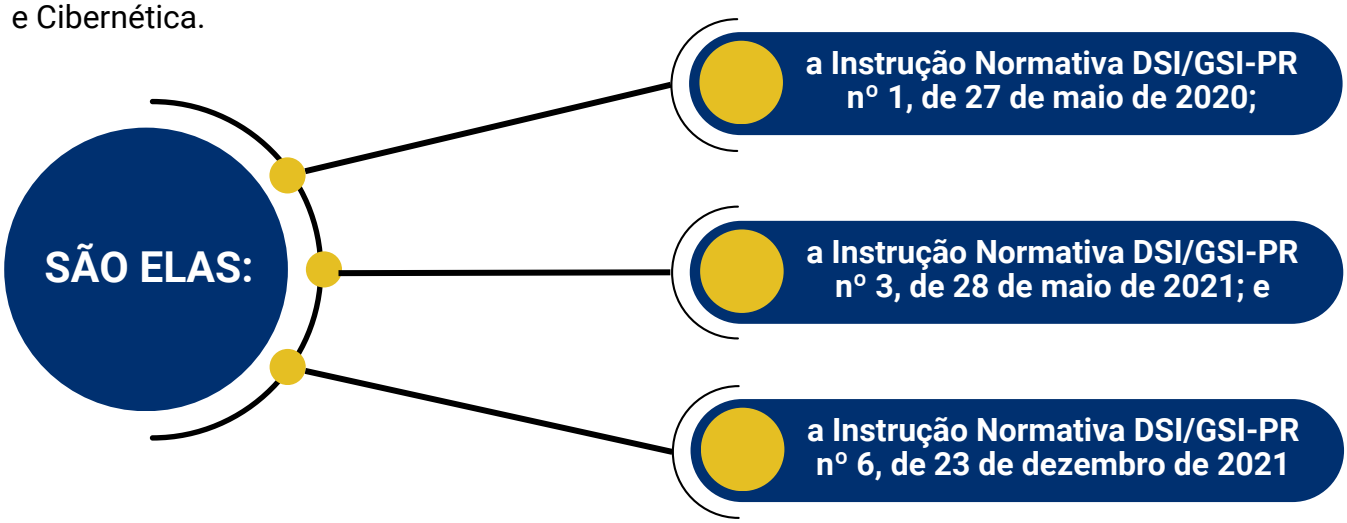
- redes sociais podem ser palco de cyberbullying, fazendo com que a vítima se sinta impotente por ser atacada por todos os lados. Observe sinais de tensão, nervosismo ou tristeza.

Ao identificar sinais de abuso, é importante manter o diálogo e estimular um canal de confiança para que a vítima possa se sentir confortável para detalhar o problema. Confira algumas ações importantes:

- é importante amparar as vítimas e tomar as medidas para restringir os ataques e buscar a responsabilização de agressores. Normalmente a vítima está fragilizada. Seja gentil e compreensivo neste momento;
- use as configurações de privacidade para restringir a interação de desconhecidos;
- evite a exposição excessiva de detalhes pessoais, rotina familiar e aspectos íntimos;
- redes sociais oferecem canais de denúncia de perfis abusivos. Use estes recursos; e
- em casos mais graves, é importante reunir evidências, como capturas de tela, para comprovar ataques virtuais em um possível boletim de ocorrência.

## Publicada a Instrução Normativa GSI/PR nº 7

No dia 29 de novembro de 2022, foi publicada a Instrução Normativa DSI/GSI-PR Nº 07. Ela altera algumas instruções já publicadas pelo Departamento de Segurança da Informação e Cibernética.




Foram contempladas mudanças nas competências de alguns integrantes da gestão de segurança da informação e do processo de Avaliação de Conformidade nos aspectos de segurança da informação. Veja no quadro abaixo as principais alterações.

**IN GSI nº 01**

⇨ A coordenação do comitê de segurança da informação do órgão ou da entidade será realizada pela maior autoridade designada.

**IN GSI nº 03**

⇨ No processo de Avaliação de Conformidade, seguem as novas atribuições:

- agente responsável — elaborar relatório de avaliação de conformidade e remeter ao gestor de segurança da informação;
- gestor de segurança da informação — emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentar ao comitê de segurança da informação;
- alta administração — aprovar o processo de avaliação de conformidade; e
- comitê de segurança da informação — adotar as providências cabíveis descritas nesse relatório aprovado.

**IN GSI nº 06**

⇨ A administração e a gerência dos perfis institucionais mantidos em mídias sociais agora poderão ser realizadas por equipes compostas por servidores, militares ou empregados públicos, não apenas por servidores efetivos e militares de carreira dos órgãos ou entidades.

### Teste seu conhecimento em Segurança Cibernética!

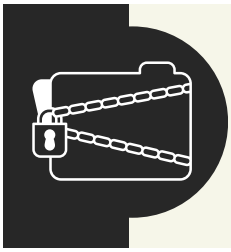
**Qual das frases a seguir está correta?**

**A** Podemos dizer que a informação classificada é um subconjunto do grande conjunto das informações sigilosas.

**B** Podemos dizer que a informação sigilosa é um subconjunto do grande conjunto das informações classificadas.

Resposta do teste no final deste BIM

**Você sabia que o acesso à informação classificada não depende apenas do credenciamento?**



Pois é... De acordo com as normas jurídicas que tratam do assunto, para um indivíduo poder ter acesso a uma informação classificada, seja ela RESERVADA, SECRETA ou ULTRASSECRETA, além da credencial de segurança compatível com o grau de sigilo da informação, ele deve possuir a **necessidade de conhecer** aquele assunto.

Tanto a Lei de Acesso a Informação como o Decreto nº 7.724/2012 definem que "o acesso, a divulgação e o tratamento de **informação classificada** em qualquer grau de sigilo ficarão restritos a pessoas que tenham **necessidade de conhecê-la** e que sejam credenciadas".

A **necessidade de conhecer** é a condição inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa tenha acesso a dados ou conhecimentos sigilosos. É fator restritivo do acesso, independente do grau hierárquico ou do nível da função exercida pela pessoa.

Ou seja, um servidor de determinado Ministério que tenha credencial para tratamento de informação classificada só terá acesso aos documentos que ele necessite para sua atividade profissional. Caso o Ministério tenha documentos classificados com informações que não tenham relação com a atividade do servidor, ele não deverá acessá-los, independente do grau de sua credencial de segurança.

Assim, nota-se que a **necessidade de conhecer** é condição indispensável para o acesso e o tratamento de informação classificada, seja qual for o grau de sigilo atribuído à informação ou o nível de acesso da credencial da pessoa que deseja acessá-la.

Para saber mais sobre este assunto e outros relacionados à segurança da informação acesse: https://www.gov.br/gsi/pt-br/assuntos/dsi .

## GSI aprova o Plano de Gestão de Incidentes Cibernéticos (PlanGIC)

O Gabinete de Segurança Institucional (GSI) publicou a Portaria GSI/PR nº 120, de 21 de dezembro de 2022, que aprova o Plano de Gestão de Incidentes Cibernéticos (PlanGIC) para a administração pública federal.

O Plano, elaborado pelo Departamento de Segurança da Informação e Cibernética (DSIC/GSI), visa estabelecer procedimentos de gestão de incidentes cibernéticos para os participantes da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

Os procedimentos estabelecidos neste Plano incluem ações a serem desenvolvidas pelos diversos níveis da administração, sendo fundamental na atuação das Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIRs).

Acesse no sítio: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918

**Resposta do teste - Letra A**

Fonte: https://www.gov.br/gsi/dsi/ https://www.gov.br/ctir
Editorial/redação/diagramação: SSIC Sugestões: educa.si@presidencia.gov.br