

**COMISSÃO DE PRIVACIDADE E PROTEÇÃO DE
DADOS - OAB/SP**

**COORDENADORIA
EDUCACIONAL**

INCIDENTES DE SEGURANÇA

O QUE SÃO E QUAIS MEDIDAS TOMAR
QUANDO ACONTECEM

JULHO/2021

SEGURANÇA DA INFORMAÇÃO

O QUE É INFORMAÇÃO?

É TODO DADO* OU CONJUNTO DE DADOS QUE TENHA ALGUM SIGNIFICADO PARA AQUELE QUE A RECEBE E CONSEQUENTEMENTE NECESSITA SER ADEQUADAMENTE PROTEGIDA.



SEGURANÇA

A SEGURANÇA DA INFORMAÇÃO (S.I.) SE DEFINE COMO A PROTEÇÃO DA INFORMAÇÃO, OU DE UM CONJUNTO DE INFORMAÇÕES QUE TENHAM VALOR A UM INDIVÍDUO OU A UMA ORGANIZAÇÃO.

PILARES DA S.I

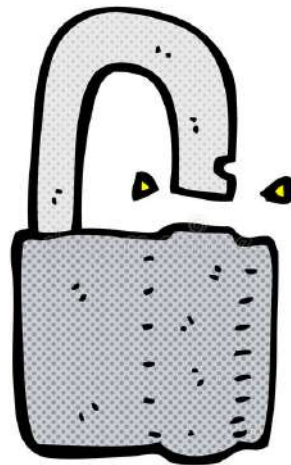
- INTEGRIDADE*
- CONFIDENCIALIDADE*
- DISPONIBILIDADE*



A INFORMAÇÃO PODE SER ARQUIVO* DE IMAGEM, ÁUDIO, VÍDEO, IMPRESSA OU ESCRITA EM PAPEL. PODE SER TRANSMITIDA PELOS CORREIOS, MEIOS ELETRÔNICOS E SER ARMAZENADA.

INCIDENTE DE SEGURANÇA

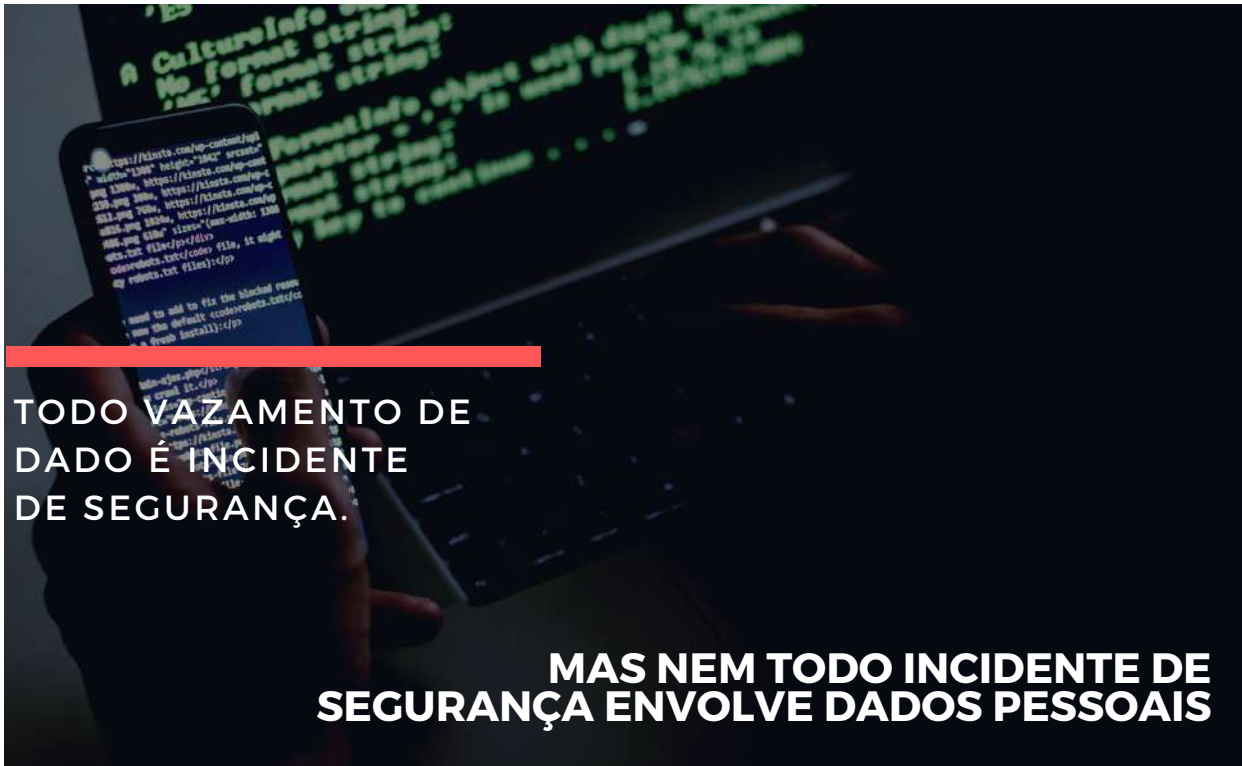
Uma ameaça à segurança da informação geralmente está ligada à ausência de um dos pilares da S.I. e, quando esta vulnerabilidade* acontece, podem ocorrer incidentes* de segurança, que são eventos adversos, ainda que sob suspeita, relacionados à segurança de sistema de computação ou rede de computadores.



EXEMPLOS

**ACESSO NÃO AUTORIZADO;
MODIFICAÇÃO DE DADOS NÃO AUTORIZADA;
DESTRUIÇÃO DE DADOS PESSOAIS;
PERDA DE DADOS;
DIVULGAÇÃO DE DADOS;
VAZAMENTO* DE DADOS
VIOLAÇÃO* DE DADOS**

VIOLAÇÃO DE DADOS VS. VAZAMENTO DE DADOS



TODO VAZAMENTO DE DADO É INCIDENTE DE SEGURANÇA.

MAS NEM TODO INCIDENTE DE SEGURANÇA ENVOLVE DADOS PESSOAIS

A **violação de dados** consiste em um ataque a dados privados por alguém ou uma entidade não autorizada, como por exemplo uma invasão de um hacker/cracker* a um banco de dados.

O **vazamento de dados** é a transmissão* não autorizada de informações para destinatários externos, seja na forma física ou digital.

A VIOLAÇÃO
OCORRE DE
FORA PARA
DENTRO E O
VAZAMENTO DE
DENTRO PARA
FORA

DICAS PARA PREVENIR

UM INCIDENTE* DE SEGURANÇA




MANTENHA-SE VIGILANTE COM O QUE ESTÁ A SEU ALCANCE.

- **Confirmação de dados:** Fique atento, não confirme dados que venham por e-mail, mensageiro instantâneo (WhatsApp), rede social, telefone ou SMS. As instituições bancárias, educacionais e órgãos públicos utilizam seus meios oficiais e suas próprias ferramentas para contato com os usuários.
- **Cadastre novos e-mails** em sites de e-commerce, como medida preventiva.
- **Utilize senhas seguras**, com um mínimo de 8 dígitos.
- **Cadastro no App "Caixa Tem"** para acesso a serviços sociais, evitando que terceiros façam este cadastro com seus dados, após recente vazamento*.
- **Utilize sites seguros.**
- **Proteja seus idosos:** Ajude a rever senhas, e-mails, criar autenticação em duas etapas, oriente e crie códigos seguros de comunicação.

COMO ESCOLHER UMA
SENHA

SEGURA

 Username

 Password

LOGIN

- Escolha senhas fortes, misture números, letras e caracteres (3xem\$PI0);
- Fuja de datas de aniversário;
- Não coloque nome de parente ou animal de estimação;
- Esqueça o "123456";
- Utilize criptografia*;
- Utilize gerenciador de senhas.

**NÃO DEIXE A
SENHA
ANOTADA EM
POST IT NO SEU
MONITOR!**

MEUS DADOS **VAZARAM**. E AGORA?

QUAIS MEDIDAS DEVEM SER ADOTADAS PARA MITIGAR OS EFEITOS DE UMA VIOLAÇÃO* DE DADOS PESSOAIS?

O USO INDEVIDO E NÃO AUTORIZADO DE DADOS PESSOAIS PODE CAUSAR INÚMEROS TRANSTORNOS AOS TITULARES*.

SE ISSO ACONTECER COM VOCÊ, ADOTE AS SEGUINTE PROVIDÊNCIAS:

1. NÃO APAGUE AS CONVERSAS E E-MAILS

Não apague as mensagens que contenham evidências* dos dados*.

2. PROVAS

Obtenha o maior número possível de provas e evidências* possíveis. Isso pode ser obtido através de prints* de mensagens, notícias ou testemunhas.

3. BOLETIM DE OCORRÊNCIA

Dirigir-se imediatamente à Delegacia de Polícia mais próxima para registrar um boletim de ocorrência. Em São Paulo temos a 3ª Delegacia de Polícia sobre Violação de Dispositivo.





4. INFORME FAMILIARES E AMIGOS

Avise os amigos, familiares e em redes sociais a fim de evitar que caiam em algum golpe.

5. NOTIFIQUE INSTITUIÇÕES BANCÁRIAS

Acompanhe também os extratos da conta bancária e de cartão de crédito.

6. MONITORE A MOVIMENTAÇÃO DO SEU CADASTRO NO SPC/SERASA

Atualmente empresas especializadas em proteção ao crédito oferecem serviços de alerta para monitorar a movimentação, consultas, fraudes, restrições e alterações de registro pessoal entre outros.

7. ACIONE A ANPD

Se ainda o vazamento* não foi informado pelos canais de comunicação ou pela Empresa ou pela Pessoa que estava sob a tutela* e responsabilidade pelo tratamento* dos dados pessoais* notifique a ANPD através de peticionamento eletrônico.

O BANCO CENTRAL DISPONIBILIZA, VIA SITE, CONSULTA GRATUITA A INFORMAÇÕES DE CHAVES PIX, EMPRÉSTIMOS E FINANCIAMENTOS, CONTAS EM BANCO E OUTROS EM NOME DO TITULAR DOS DADOS - [HTTPS://WWW.BCB.GOV.BR/CIDADANIAFINANCEIRA/REGISTRATO.](https://www.bcb.gov.br/cidadaniafinanceira/registrato)

VAZAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES



CABE ÀS INSTITUIÇÕES DE ENSINO E DEMAIS ENTIDADES QUE TRATAM DADOS PESSOAIS* DE CRIANÇAS E ADOLESCENTES, A MANUTENÇÃO DE POLÍTICAS RELATIVAS À SEGURANÇA DA INFORMAÇÃO SEMPRE ATUALIZADAS, A PROMOÇÃO DA EDUCAÇÃO DIGITAL DAQUELES QUE LIDAM COM OS DADOS*, ASSIM COMO TRAÇAR MEIOS PARA IDENTIFICAÇÃO E CONTENÇÃO DE INCIDENTES*.

O vazamento* de dados de crianças e adolescentes não diz respeito exclusivamente à LGPD*, mas também ao Estatuto da Criança e do Adolescente, que prevê, no artigo 17, a proteção à inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem e da identidade.

É importante reforçar a necessidade da preservação da privacidade* e integridade* de qualquer menor que tenha seus dados* expostos.

A ideia não é impedir, por completo, a exposição e o tratamento* de dados pessoais* de crianças e adolescentes, o que lhes negaria o direito de participação na sociedade da informação.

Porém, seus dados* devem ser tratados* somente quando requerido, e apenas os dados mínimos necessários, considerando, especialmente, seu direito – e vontade – de integração, sua peculiar condição de vulnerabilidade* e qualidade de ser em desenvolvimento.

VAZAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES



Importante lembrar também a máxima que "conteúdo na internet não tem devolução". Assim, os dados* e informações coletados, publicados e compartilhados, poderão, em eventuais ataques e vazamentos, fugir do controle do menor, dos seus responsáveis e do próprio Controlador*.

EM CASO DE PUBLICAÇÃO DE CONTEÚDO NÃO AUTORIZADO EM REDE SOCIAL, O MARCO CIVIL DA INTERNET* (LEI 12.965/14) PREVÊ A REMOÇÃO DO CONTEÚDO QUE EXPÕE A CRIANÇA/ADOLESCENTE, MANTENDO-SE A PRESERVAÇÃO DOS DADOS QUE POSSAM IDENTIFICAR POSSÍVEIS AUTORES DA PUBLICAÇÃO.

A existência de riscos não significa que dados pessoais* de crianças e adolescentes não podem ser tratados. Porém, é importante lembrar que é imprescindível que se avalie:

- a real necessidade;
- os possíveis riscos; e
- em regra, é preciso obter consentimento* de forma específica e destacada, dentro da lei.



GLOSSÁRIO

Ação preventiva - Ação para eliminar a causa potencial, não conformidade ou outra situação indesejável, ou seja, ação para prevenir o acesso aos dados pessoais ou mesmo vazamento, como por exemplo: criação de senhas com maior segurança, não remetendo a datas de aniversário, apelidos, etc., não divulgar senhas - que devem ser pessoais e intransferíveis-, não utilizar sempre a mesma senha, instalar programas de computadores para detectar vírus, nunca inserir ou fornecer seus dados pessoais para pessoas desconhecidas, e-mails , etc. Jamais deixe extratos bancários impressos, cartões de créditos, imposto de renda, documentos fiscais ou contas de telefone à vista. Recomenda-se, inclusive, destruir essas informações, caso pretenda jogar fora tais documentos. Proteja suas informações seja no ambiente residencial, público ou escritórios e escolas.

Ameaça - Causa potencial de um futuro incidente indesejado. Tome cuidado com e-mails estranhos, mensagens para obrigar a instalação de softwares, mensagens por whatsapp, torpedos pelo celular solicitando cadastramento de dados pessoais e senhas. Essas atividades podem resultar no dano aos seus dados pessoais ou ao sistema de informação (computadores e celulares).

Arquivo - Conjunto de documentos produzidos e acumulados por uma entidade coletiva, pública ou privada, pessoa ou família, no desempenho de suas atividades, independentemente da natureza do suporte.

Arquivo digital - Conjunto de bits que formam uma unidade lógica interpretável por um programa de computador e armazenada em suporte apropriado.

Ataque - Uma tentativa de destruir, expor, alterar, inutilizar, roubar e obter acesso não autorizado, ou fazer uso não autorizado de informações pessoais.

Ativo - Qualquer coisa que tenha valor para organização ou empresa. Esta é uma definição ampla, você pode pensar nas instalações, informação, softwares (programas de computador), hardwares (computadores e servidores).

Autenticidade - Propriedade de uma entidade ser o que afirma o que é.

Confiabilidade - Acessar sites, contatos, conteúdos que dão segurança ao usuário, estão em ambiente seguro, protegidos por senha com a figura de um cadeado no endereço de acesso.

Confidencialidade - Controle do acesso à informação, conforme autorização e necessidade da empresa. O conceito de confidencialidade busca prevenir a divulgação intencional ou não intencional do conteúdo de uma mensagem. A perda de confidencialidade pode ocorrer de várias maneiras, tais como pela divulgação intencional de uma informação privada de um cidadão ou de uma empresa ou pelo mau uso de credenciais de acesso à rede, como por exemplo acesso à internet, cuidado ao usar wi-fi que não tenham senha protegendo.

Consentimento - Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador - A pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Quem obteve os dados pessoais diretamente do titular de dados pessoais.

GLOSSÁRIO

Criptografia - Método de codificação de dados segundo algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam restabelecer sua forma original. Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos; e proteger o sigilo de comunicações pessoais e comerciais.

Dado - Representação de todo e qualquer elemento de conteúdo cognitivo, passível de ser comunicada, processada e interpretada de forma manual ou automática.

Dados pessoais - Informação relacionada a pessoa natural identificada ou identificável, ou seja, qualquer dado em que a pessoa possa ser identificada direta ou indiretamente, como o nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, econômica, cultural, social e outros, tais como nome, CPF, CNH, número do celular, tatuagem, foto, nome na rede social, e-mail, entre outros.

Dados pessoais sensíveis - Se os dados pessoais forem sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, político, ou filosófico, referente à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, são considerados Dados Pessoais Sensíveis. Esses dados podem sujeitar seu titular a práticas discriminatórias ou permitir a sua identificação sem qualquer dúvida.

Evidências - Todo tipo de informação documentada que possa fazer prova de algo, comprovação de uma ação.

Exposição - Exposição é uma circunstância de estar exposto aos prejuízos oriundos de um agente ameaçador, por exemplo sites, links, propagandas, anúncios de cursos, produtos de interesse, jogos de perfis em algumas redes sociais, mostrar excessivamente a vida no facebook, instagram, twitter, sites de relacionamento, que na verdade podem tornar-se em uma armadilha potencial.

Gerenciamento de riscos - Atividades coordenadas para direcionar uma organização no que diz respeito ao risco.

Gestão da informação - Gestão da informação descreve os meios pelos quais uma organização planeja, coleta, organiza, usa, controla, dimensiona, e descarta a sua informação e através da qual garante que o valor dessa informação seja identificado e explorado em toda a sua extensão.

Hacker - Usam sua inteligência de maneira positiva, constroem coisas, crackers só destroem. Infelizmente, a confusão é tanta que existem casos de livros e mesmo filmes legendados, onde o termo "Cracker" é substituído por "Hacker" pelo tradutor. (Carlos E. Morimoto. Dicionário de Termos Técnicos de Informática - 3a. edição (Locais do Kindle 2465-2466). Edição do Kindle.)

Incidente - 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 e Comunicações.

GLOSSÁRIO

LGPD - Lei Geral de Proteção de Dados Pessoais - A Lei nº 13.709/2018, que foi criada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A lei cuida do tratamento de dados pessoais, que estejam em meio físico ou digital, realizado por pessoa física ou jurídica, de direito público ou privado, e compondo um amplo conjunto de operações realizadas em meios físicos ou digitais.

Marco Civil da Internet - A Lei nº 12.965/2014, que estabeleceu um conjunto de princípios e garantias, direitos e deveres para o uso da Internet no Brasil e, além de garantir a privacidade e proteção de dados pessoais, assegura a disponibilização desses dados mediante ordem judicial.

Não repúdio - Habilidade de provar a ocorrência de um suposto evento ou ação e sua origem.

Prints - Imagens registradas de telas, tais como computadores, celulares, notebooks, tablets.

Privacidade - É relacionado ao privado, ao círculo restrito da pessoa, sendo a intimidade algo interno à pessoa humana. "A privacidade é um bem da personalidade de grande relevância e poderá ser afetada de modo contundente com a divulgação indevida de dados". (Silmara J. Chinellato, CC Manole, p.127, 2021).

Segurança da Informação - A segurança da informação é a proteção contra a uma gama ampla de ameaças, a fim de garantir a continuidade dos negócios, e proteger os usuários e clientes.

Titular (de dados pessoais) - Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. É o dono dos dados pessoais.

Transmissão - Movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.

Tratamento - Toda e qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, a eliminação ou a destruição (LGPD, art. 5º, X).

Vazamento - O vazamento de dados é configurado como um incidente de segurança que torna públicas informações confidenciais que podem ser analisadas, roubadas, copiadas e usadas por terceiros sem acesso permitido.

Violação - Ocorre quando a sua empresa/organização sofre um incidente de segurança relativo aos dados pelos quais é responsável que resulta numa violação da confidencialidade, da disponibilidade ou da integridade dos dados.

Vulnerabilidade digital - É uma fraqueza apresentada por sistemas computacionais, que permitem a invasão e colocam em risco as informações e dados dos titulares. É causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da empresa/organização. Fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças, como, por exemplo: antivírus desatualizado, credenciais administrativas padrão (admin/admin).

Coordenação:

Carolina Chiavalon

Criação:

Ana Carolina Paes de Mello

Camilla D'Agostino

Denise Berzin Reupke

Fernanda Natali Queiroz

Karem Luiza da Costa

Marisol Gonzalez Martinez

Paula Krupp Freire de Carvalho

Pietra Quinelato

Priscilla Ferreira Tricate

Arte:

Ana Carolina Paes de Mello

Camilla D'Agostino

Rosalia Toledo Veiga Ometto

Realização:

Comissão de Privacidade e Proteção de Dados OAB/SP

Diretoria Executiva:

Patrícia Peck Pinheiro - Presidente

Marcelo Lapolla - Vice-Presidente

Marcelo Crespo - 1º Secretário

Gabriela De Ávila Machado - 2ª Secretária