LGPD NA FCAV

CARTILHA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Cuide do que tem valor

Fundação Vanzolini

CARTILHA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Cuide do que tem valor

SUMÁRIO

O que é a LGPD? 3
Quando se aplica? 3
Direitos dos titulares 4
Segurança da Informação 5
O que são ameaças? 5
E uma vulnerabilidade? 6
Ameaça + Vulnerabilidade = RISCO 6
Ataques digitais mais comuns 7
Incidentes de Segurança de Violação de Dados Pessoais 9
Cuidados diários para a segurança da informação 10
Termos de definições 12

O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais, conhecida pela sua sigla, LGPD, *(Lei no 13.709/18)*, é a lei que regula o tratamento de dados pessoais com o objetivo de proteger a pessoa natural (pessoa física), aqui chamada titular de dados.

Em outras palavras, a LGPD estabelece as "regras do jogo" para tudo que é feito com informações de pessoas físicas.

QUANDO SE APLICA?

Aplica-se a qualquer tratamento de dados pessoais, realizado em meio físico ou digital, por pessoa física ou jurídica de direito público ou privado.
Ex. dados em meio físico: formulários de cadastramento, cópias impressas, currículos em papel, rascunho, arquivos físicos, provas, trabalhos e exercícios em papel, receitas médicas etc.

Ex. dados em meio digital: cópias digitais, documentos em e-mail, WhatsApp.

ATENÇÃO: A LGPD não se aplica quando o tratamento é realizado por pessoa física para fins particulares e não econômicos.

DIREITOS DOS TITULARES

O titular deverá exercer o controle sobre seus próprios dados, e, para isso, a lei fornece a este uma série de direitos que podem ser exercidos diretamente perante a organização que trata seus dados, são eles:

- Confirmação da existência de tratamento: o titular tem o direito de saber se a organização trata seus dados;
- Acesso aos dados: o titular poderá obter cópia de seus dados pessoais;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- Portabilidade dos dados a outro fornecedor (pendente de regulação pela ANPD);
- Eliminação dos dados tratados com base no consentimento;
- Informação das entidades públicas e privadas com as quais a organização compartilhou dados;
- Informação sobre a possibilidade de não fornecer consentimento e consequências da negativa;
- Revogação do consentimento: tão simples quanto o consentimento pode ser concedido, poderá ele ser retirado a qualquer momento;
- Petição contra o controlador perante a Autoridade Nacional;
- Oposição a tratamento que descumpra a lei;
- Revisão de decisão baseada em tratamento exclusivamente automatizado.

COMO ATENDER AOS DIREITOS DOS TITULARES?

A lei não estabeleceu o formato, mas visando facilitar o recebimento, processamento e resposta destas requisições pelo nosso Encarregado pela Proteção de Dados Pessoais (DPO), a FCAV estabeleceu um canal de comunicação específico para isso, por meio do e-mail: **atendimentolgpd@vanzolini.org.br** ou pelo formulário disponibilizado no Portal FCAV, endereço eletrônico **https://vanzolini.org.br/lgpd/.**

SEGURANÇA DA INFORMAÇÃO

De forma geral, a segurança da informação é a garantia da confiabilidade da informação, que consiste na preservação da confidencialidade, integridade e disponibilidade das informações.

• CONFIDENCIALIDADE: As informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados.

• INTEGRIDADE: Precisão e integridade.

• DISPONIBILIDADE: Ser acessível e utilizável sob demanda por uma entidade autorizada.

Para isso adotamos medidas físicas (que protegem fisicamente um ativo), técnicas (implementadas na infraestrutura de TI e sistemas), e organizativas (relacionadas a políticas, processos, pessoas).

Logo, podemos afirmar que, a segurança da informação exige a implementação de medidas e controles aptos a proteger as informações contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos do negócio e maximizar o retorno sobre os investimentos e as oportunidades do negócio.

O QUE SÃO AMEAÇAS?

Uma ameaça é a potencial causa de um incidente indesejado, que pode resultar em danos a um sistema ou organização. Geralmente, conta com um "agente de ameaça" que explora uma vulnerabilidade visando obter, danificar, extrair, alterar ou destruir um ativo de forma intencional ou acidental.

Exemplos:

• **Ameaça humana:**

Intencional: danos a informação causados por pessoas de forma proposital.

Ex.: invasores, fraudes, furto, roubo, vírus, vandalismo.

Não intencional: danos causados por pessoas de forma involuntária.

Ex.: acidentes, negligência, falha humana, despreparo.

• **Ameaça não humana:** Causadas por influências externas (naturais/ambientais). **Ex.:** Raios, inundações, incêndios.

E UMA VULNERABILIDADE?

A vulnerabilidade é a fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças.

Exemplos:

• TÉCNICA: falta de antivírus, software desatualizado, senhas fracas, conexão com internet
desprotegida.

• ORGANIZATIVA: Falta de treinamento da equipe, falta de conscientização dos colaboradores, perfis inadequados para as funções desempenhadas, processos de controle de acesso deficientes, processos de trabalho mal desenhados.

• FÍSICAS: Ausência de local seguro para guardas de documentos físicos.

AMEAÇA + VULNERABILIDADE = RISCO

De forma ampla, um risco é o efeito das incertezas sobre os objetivos do negócio.

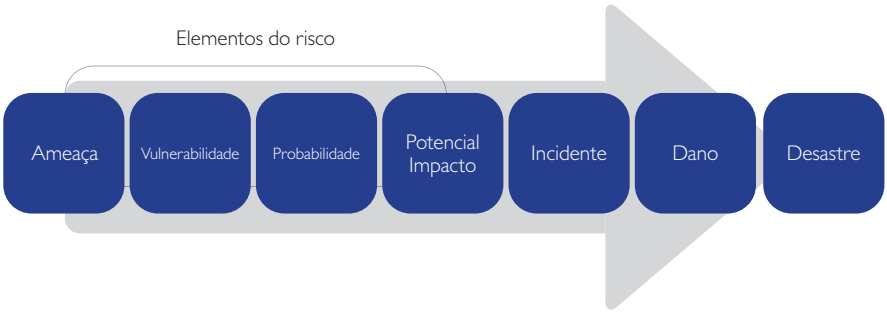
Isto é, os riscos terão um impacto para a FCAV que será causado por um agente de ameaça no momento em que explora uma vulnerabilidade, caso se concretizem.

No entanto, para a segurança da informação o risco está associado ao potencial de que as ameaças explorem vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, portanto, causar danos a uma organização.

É preciso, ainda, verificar qual a probabilidade de ocorrência deste evento adverso para que seja possível avaliar os riscos e estabelecer a melhor forma de tratá-lo[1].

De uma forma geral, a concretização de um risco acarreta um incidente que pode ocasionar danos para a FCAV ou até mesmo comprometer a continuidade dos negócios, momento em que é classificado como desastre.
Elementos do risco

[1] Modificar, reter, evitar, compartilhar ou aceitar o risco (ISO/IEC 27005:2019).



ATAQUES DIGITAIS MAIS COMUNS

Algumas ameaças podem impedir a organização de funcionar, outras proporcionar que a organização perca informações importantes. Dentre elas, destacamos o spam, phishing, malware (ransomware), sendo preciso estar atento a estes fatores, monitorando e conscientizando colaboradores no intuito de corrigir vulnerabilidades e assim mitigar a manifestação de riscos advindos destes.

Os malwares (termo genérico) se referem a qualquer tipo de software de computador com intenção maliciosa, como, por exemplo, vírus, worms, spyware, hoax, ransonware, cavalo de troia (trojan), sendo uma medida padrão e efetiva para segurança a utilização de antivírus e firewalls.

Os malwares podem explorar vulnerabilidades, por exemplo, no momento em que realizamos o download de um arquivo infectado ao clicar em links enviados por remetentes desconhecidos ou sites não confiáveis, decorrentes de fraudes ou até mesmo plugar dispositivos removíveis infectados no computador.

• **Vírus:** é um pequeno programa de computador que se replica e carrega o código executável. Tem natureza destrutiva.

• **Worms:** é um pequeno programa de computador que se replica e não depende de ação do usuário para se espalhar pela rede.

• **Spyware:** programa de computador que coleta informação de um computador e envia para um terceiro.

• **Hoax:** é uma mensagem que tenta convencer o leitor da sua veracidade e então persuadi-lo a fazer alguma ação.

• **Cavalo de troia (trojan):** é um programa que conduz atividades secundárias não percebidas pelo usuário. É utilizado frequentemente para coletar informações confidenciais do sistema infectado.

• **Bomba lógica:** É um código deixado dentro de um sistema que é programado para ativar em determinadas circunstâncias.

• **Ransomware:** É um conjunto de vírus do tipo malware e tem sido massivamente utilizada para a prática de crimes de extorsão de dados — prática também conhecida como sequestro de dados.

O programa torna os dados armazenados em um equipamento inacessíveis, geralmente usando criptografia e exige pagamento de resgate em criptomoedas para restabelecer o acesso ao usuário. Ações comuns deste tipo de malware são, por exemplo, impedir o acesso ao equipamento (Locker ransomware) ou o acesso aos dados armazenados no equipamento, geralmente usando criptografia (Crypto ransomware).

Phishing é uma forma de fraude na internet através da engenharia social. A engenharia social é uma forma de manipulação psicológica para obtenção de informações confidenciais ou realizar a prática de determinada ação.

Um caso típico de phishing é aquele em que o agente envia um e-mail para a vítima, mas também pode ser por meio de aplicativos de mensagens ou até mesmo ligações, solicitando que ela verifique ou confirme determinada informação junto de um banco ou outro canal.

Por fim, spams são mensagens indesejadas, normalmente recebidas por e-mail, ou mensagens publicitárias indesejadas encontradas em sites.

INCIDENTES DE SEGURANÇA DE VIOLAÇÃO DE DADOS PESSOAIS

A LGPD determina a adoção de medidas de segurança da informação quanto aos dados pessoais, contudo, nenhum sistema é invulnerável, de modo que a lei também dispõe sobre o que fazer quando da ocorrência de um incidente de segurança que envolva dados pessoais.

O que é um incidente de segurança de dados pessoais?

Acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, resultante de incidente de segurança.

O exemplo mais citado de incidente é a "disponibilização indevida de dados pessoais", mas a este não se limita, possuindo um conceito muito mais abrangente, conforme acima.

O que fazer quando houver um incidente?

A consequência legal de um incidente é: Comunicar incidentes de segurança com risco ou dano relevante envolvendo dados pessoais à ANPD e aos titulares envolvidos.

Contudo, até a determinação pela comunicação, deve-se ter um processo interno no qual busca-se o levantamento das circunstâncias do incidente, com comunicação ao Encarregado pelo Tratamento de Dados Pessoais para análise da necessidade de comunicação do incidente ou não.

Em todos os casos, independentemente de comunicação, o incidente deverá ser registrado para fins de gestão, tomada de decisões e até apresentação em eventual fiscalização, inclusive com a justificativa pela decisão de não-comunicação.

Portanto, se você se deparar com alguma vulnerabilidade ou um incidente de segurança comunique imediatamente o gestor da área bem como encarregado pela proteção de dados pessoais pelo e- mail: **suportelgpd@vanzolini.org.br.**

CUIDADOS DIÁRIOS PARA A SEGURANÇA DA INFORMAÇÃO

Você já parou para pensar a quantidade de informações que você tem acesso e são compartilhadas diariamente, na rua, no ônibus, na Internet, nas mídias sociais e até mesmo na sua organização? Sim, são inúmeras.

Para nós, a informação é essencial, especialmente aquela que custodiamos de nossos clientes! Se utilizada da maneira correta ela pode garantir resultados melhores e acertados. Contudo, quando utilizada de maneira indevida, mesmo que por desconhecimento, pressa ou proatividade, ela pode se tornar um risco.

Pratique segurança diariamente! Contamos com você para proteção de nossos ativos.

FIQUE ATENTO ÀS DICAS ABAIXO:

Além dos serviços prestados, as nossas informações, de nossos clientes, nossa marca e reputação são valiosos. Por isso devem ser protegidos e utilizados somente para as finalidades profissionais e autorizadas.

A ORGANIZAÇÃO É PROPRIETÁRIA DE TODAS AS INFORMAÇÕES QUE VOCÊ CRIA, ACESSA OU RECEBE!

Preserve o sigilo de nossas informações e também de nossos clientes! Mantenha-as sob seu controle e não compartilhe em serviços públicos na Internet, como Facebook, Whatsapp ou Dropbox, e até mesmo para e-mails particulares ou de terceiros não autorizados.

CUIDE DA SUA SENHA E NÃO COMPARTILHE O SEU CERTIFICADO DIGITAL.

Utilize apenas programas e recursos tecnológicos disponibilizados ou autorizados. Não instale programas, abra arquivos ou acesse links desconhecidos, pois são porta de entrada de vírus.

Faça o uso ético e legal de nossos recursos tecnológicos. Não os utilize para acesso ou transmissão de conteúdo ilegal, racista, agressivo, discriminatório ou

contendo ameaças, por exemplo.

Respeite os direitos de propriedade intelectual. Antes de utilizar um software ou conteúdo verifique se você possui as licenças e as permissões necessárias.

PROTEJA OS DISPOSITIVOS MÓVEIS, COMO NOTEBOOKS, TABLETS, SMARTPHONES!

Mantenha-o, sempre que possível, bloqueado e sob sua supervisão em lugares públicos ou de grande circulação como saguões de hotéis, aeroportos ou restaurantes.

Seja claro e específico. Ao enviar mensagens para colaboradores, clientes, prestadores de serviços ou fornecedores, seja formal e profissional, evite excesso de intimidade, frases de duplo sentido ou genéricas que possam ser mal interpretadas pelos leitores.

Todos os recursos tecnológicos devem ser bloqueados e os armários, gavetas, arquivos e salas trancadas, sempre quando não utilizadas.

Mantenha a mesa e a tela limpa! Não deixe informações expostas na mesa de trabalho, nas impressoras, salas de reuniões ou abertas na tela de seu dispositivo desbloqueado.

Cuidado ao repassar informações para terceiros, independente se por telefone, mídias sociais, aplicativos de comunicação instantânea, e-mail ou pessoalmente. Na dúvida, não passe nenhuma informação sem autorização.

Se as mídias sociais e os aplicativos de comunicação instantânea fazem parte de sua vida, atenção aos comentários sobre sua rotina profissional, detalhes de serviços ou dados de nossos clientes. Esteja atento com o que você compartilha com seus amigos. Certifique-se de que não é uma informação confidencial.

RESPEITE O SIGILO LEGAL E PROFISSIONAL TAMBÉM NOS AMBIENTES DIGITAIS!

Não tire fotos ou grave áudio/vídeo de nossos ambientes, colaboradores, clientes, prestadores de serviços ou fornecedores. Além disso, não compartilhe

na Internet, mídias sociais ou em aplicativos de comunicação instantânea.
Sempre alerta! Lembre-se que nossos ambientes físicos e lógicos são monitorados para a sua segurança e dos demais colaboradores, clientes, ativos e informações.
Trabalhe seguro! Qualquer problema ou dúvida procure seu Gestor.
A segurança da informação não é nada sem você! Participe dos treinamentos e palestras. Seja proativo ao zelar pela segurança de nossa organização.
Dissemine essa ideia e conte conosco!

TERMOS DE DEFINIÇÕES

Agente de Tratamento: Controlador e Operador

Ameaça: Risco ou potencial perigo de um incidente, que pode resultar em dano à FCAV.

ANPD ou autoridade nacional de proteção de dados: Órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da lei geral de proteção de dados pessoais aplicável.

Ativo: É qualquer coisa que tenha valor e precisa ser adequadamente protegido.

Ativo Intangível: Todo elemento que possui valor e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou percetível, a exemplo, mas não se limitando à dados, reputação, imagem, marca e conhecimento.

Autenticidade: Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

Backup: Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em caso de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado,

fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venham a ter relacionamento profissional, direta ou indiretamente com a organização.

Controlador: Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio.

Dado pessoal: Informação relacionada a pessoa física identificada ou identificável.

Dado pessoal sensível: Dado pessoal sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física.

Disponibilidade: Garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos Móveis: equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo.

Dispositivos Removíveis de Armazenamento de Informação: Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e pen drive.

Encarregado pelo tratamento de dados pessoais: Pessoa física ou jurídica indicada pela FCAV e que atua como canal de comunicação entre a FCAV com os Titulares dos dados pessoais ou a ANPD.

Evento adverso (ou ofensivo): é um evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou

execução de malware que destrói dados, entre outros

Evento: é qualquer ocorrência visível em uma rede ou sistema de informação. **Exemplos**: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.

Gestor da informação: Colaborador responsável pela criação/recebimento, classificação, divulgação, compartilhamento, eliminação e destruição da informação. Também é incumbido da gestão de validação, liberação e cancelamento dos acessos à informação destes. Vale ressaltar que tais atividades podem ser delegadas para outro colaborador, desde que concedidas pelo Gestor da informação.

Homologação: Processo de avaliação e aprovação técnica de Recursos de Tecnologia da Informação e Comunicação para serem utilizados dentro do ambiente da organização.

Identidade Digital: É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria.

Incidente de Segurança com Dados Pessoais: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular dos dados pessoais.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede, que indica possível violação à Política de Segurança da Informação ou Normas Complementares, falha de controles ou situação previamente desconhecida, que possa ser relevante à segurança da informação.

Informação: Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento,

contidos em qualquer meio, suporte ou formato.

Integridade: Garantia de que as informações estejam íntegras durante o seu ciclo de vida.

Internet: Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede, desde que configurado adequadamente.

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do Ordenamento Jurídico em vigor.

Operador: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados

Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

Repositórios Digitais (Cyberlockers): Plataformas de armazenamento na Internet, a exemplo de Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd.

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

Segurança da Informação: é a preservação da confidencialidade, integridade, disponibilidade, legalidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidades de transação.

Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação. Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos.

Dúvidas?

Envie um e-mail para:

suportelgpd@vanzolini.org.br

LGPD NA FCAV

Fundação Vanzolini