CONCEITO A
FREDERICO WESTPHALEN/RS

PID | PAID | PRISDP

ADEQUAÇÃO A LEI 13.709[v]/2018 | dpo@philipepires.adv.br

criado com:

PHILIPE PIRES
ADVOCACIA

1. PROTEÇÃO
E AÇÃO DE INCIDENTES DE DADOS

As **Políticas e Planos** aqui apresentados tem como objetivo preparar a **CONCEITO A** para lidar com a gestão de incidente, garantindo que responda de forma rápida, organizada e eficiente ao evento, minimizando suas consequências para os envolvidos. O nível da resposta dependerá do tipo de dados e da complexidade do tratamento aplicado.

De maneira geral, um **incidente** é uma situação inesperada, capaz de alterar a ordem normal das coisas e, no caso da proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com a Instituição.

O *National Institute of Standards and Technology* (NIT), define um incidente de segurança como uma violação ou ameaça de violação da política de segurança computacional, política de uso aceitável ou padrões de prática de segurança. De acordo com o artigo 46 da Lei Geral de Proteção de Dados (LGPD).

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Nossa atuação aqui consiste em identificar, prever e descrever possíveis situações de violação de dados, bem como as respectivas ações que deverão ser tomadas, os prazos e as formas de registro, garantindo que em situações reais se tenha um plano de ação previamente traçado. O planejamento deverá conter, no mínimo:

a. a previsão de possíveis situações de sinistros bem como as formas de monitoramento e a ação que deverá ser tomada em caso de sua ocorrência;

b. a definição da área que deverá ser informada em situação de ocorrência do sinistro e como reportar;

c. o detalhamento das ações necessárias deve levar em conta a criticidade do evento.

2. PID - POLÍTICA DE INCIDENTES DE DADOS

A **CONCEITO A** adota como prática máxima o uso da **transparência** na relação com os TITULARES de dados pessoais, sendo objetiva nas suas ações e priorizando a segurança para que em seus serviços o cliente, em especial, tenha a melhor experiência para poder usufruir, tanto de forma recreativa, profissional ou para o seu uso diário.

Através de nosso CONTROLADOR assumimos as responsabilidades de ao sermos notificados sobre incidentes que envolvam recursos ou informações de nossa responsabilidade, devemos colaborar com eventuais investigações (técnicas, policiais e judiciais) e tratar os incidentes com a devida urgência e ações pré-definidas.

De forma objetiva **são considerados Incidentes de Dados** quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de dados por um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio e seus objetivos em riscos.

Em nossa empresa todos os colaboradores devem estar em capacidade de identificar incidentes de dados por qualquer meio físico ou eletrônico quando for testemunhado. E todos os colaboradores devem **notificar** qualquer evento de incidente de dados ou de segurança ou fragilidade observada que possam causar: prejuízos, interrupções, maus funcionamentos, imprecisão ou vazamento de informação nos sistemas da empresa.

Nesse aspecto ainda de forma preventiva as vulnerabilidades ou fragilidades suspeitas devem sempre ser imediatamente, e não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar nossas **POLÍTICAS**, bem como provocar danos aos serviços ou recursos tecnológicos.

2.1 DA CONCEITO A

A **CONCEITO A** assume o compromisso de utilizar informações confiáveis e íntegras, atuando profissionalmente e sob a ótica das leis nacionais que regem a sua modalidade de prestação de serviço de forma a:

Preservar a informação, confidencialidade, integridade e disponibilidade: Garantindo que as informações sejam acessadas somente pelas pessoas devidamente autorizadas e conscientes administrativamente e juridicamente, para a qualquer momento, com a sua exatidão e integridade, salvando as informações em meios de armazenamentos seguros, e quando em agentes terceirizados que os mesmos estejam adequados à LGPD, em conformidade com regulações técnicas e a legislação pertinente.

2.2 DO PRAZO PARA COMUNICAÇÃO DE INCEDENTE

Qual o prazo para comunicar um incidente de segurança?

A lei determina que os incidentes de segurança devem ser comunicados aos titulares de dados e à Autoridade em prazo razoável, que foi definido pela Autoridade Nacional de Proteção de Dados (ANPD) em um regulamento próprio, sendo assim determinado que:

Para preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, recomenda-se que a comunicação seja feita o mais breve possível, **em até 2 (dois) dias úteis da ciência do fato**.

A comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD.

Qual o papel do CONTROLADOR e do OPERADOR no processo de comunicação de incidentes de segurança?

A obrigação legal de comunicar o incidente de segurança aos titulares e à ANPD é do **controlador**, nos termos do art. 48 da LGPD. No entanto, a obrigação de adotar medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais se estende a **todos os agentes de tratamento de dados, inclusive aos operadores.**

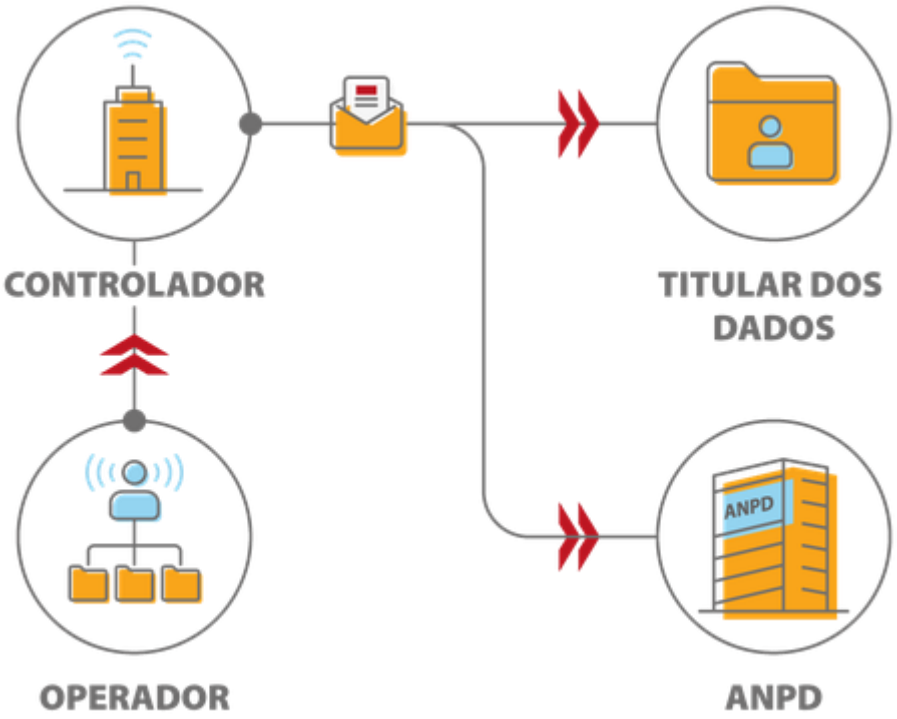
Quando um incidente de segurança ocorre, o operador deverá informar o fato, sem demora injustificada, ao controlador dos dados. Todas as informações necessárias à comunicação do incidente de segurança à ANPD e aos titulares deverão ser fornecidas pelo operador ao controlador.

A função do operador de dados, conforme prevista na Lei Geral de Proteção de Dados (LGPD), é garantir que todas as atividades realizadas com dados pessoais sejam realizadas de maneira a proteger a privacidade e os direitos dos titulares dos dados. Isso inclui desde a coleta, armazenamento, processamento, compartilhamento e destruição de dados pessoais.

O **operador é responsável por garantir que todas as atividades relacionadas aos dados pessoais sejam realizadas de acordo com as disposições da LGPD**, incluindo o cumprimento dos princípios de privacidade, transparência, finalidade limitada, adequação, minimização, exatidão, integridade e confidencialidade. Além disso, o operador também deve registrar todas as atividades que envolvam dados pessoais, incluindo as finalidades para as quais os dados são coletados, as fontes dos dados, as categorias de dados coletados, entre outros.

O **registro das atividades é importante** para garantir a transparência nas operações com dados pessoais e a proteção dos direitos dos titulares dos dados. Além disso, ele permite que as autoridades regulatórias possam verificar se as atividades com dados pessoais estão sendo realizadas de acordo com as disposições da LGPD e tomar as medidas necessárias em caso de descumprimento da lei.

Ilustra-se brevemente para que seja melhor compreendido, caso ocorra incidente de dados, qual o padrão a ser utilizado na comunicação:



Excepcionalmente, na hipótese de o controlador não dispor de informações completas a respeito do incidente ou não conseguir notificar a todos os titulares no prazo recomendado, a comunicação à ANPD poderá ser realizada em **etapas: preliminar e complementar.**

PRELIMINAR:

Entender quais são os dados e quais titulares foram afetados, isso pode ser feito cum uma análise simples das rotinas de tratamentos de dados, onde o operador irá explanar quais eram as informações contidas para que seja filtrada e separada essas informações de dados e titulares, de modo que se possa gerar um **aviso de incidente** em que se colocou em risco de vazamento. Dessa forma deve-se ser avisado pelo contato registrado do titular que seus dados passaram por uma possível exposição e que estes devem ficar atentos, mesmo que não seja este titular efetivamente vítima do incidente.

COMPLEMENTAR:

Após mediada a primeira comunicação, controlador e operador deverão aprofundar as análises para interpretar os danos reais causados pelo incidente, adotando novas medidas e mais minuciosas para verificação real do ocorrido.

Assim, especificar quais dados foram acessados e de qual localização (ou aproximada) e se conseguiram definir para onde foram transferidos.

Também devem ser revelados aos titulares quais possíveis danos podem ocorrer em caso de uso dos dados por terceiros com intenções maliciosas, e quais as medidas básicas como: registro de boletim de ocorrência, verificação de *logins* e senhas, monitoramento de uso de CPF e aberturas de contas bancárias (através do Banco Central na ferramenta: https://registrato.bcb.gov.br/) .

A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pelo controlador. A complementação deverá ser encaminhada o mais breve possível e, no mais tardar, em **30 dias corridos** contados da comunicação preliminar.

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar, por meio de petição intercorrente.

Para o devido cumprimento da POLÍTICA DE INCIDENTES DE DADOS apresenta-se o PLANO DE INCIDENTES DE DADOS (PAID) a seguir.

3. (PAID) PLANO DE AÇÃO DE INCIDENTES DE DADOS

A PID recorre-se ao PAID da **CONCEITO A** para a necessidade de cumprimento do devido e estrito poder legal, mas também para a segurança de todos os usuários de seu trabalho. Estes contemplam e podem ser acionados em sua loja física e canais digitais para que o TITULAR obtenha respostas sobre incidentes qualificados com seus dados, e seguirão as etapas ilustradas na figura abaixo e descritas na sequência:

ETAPAS DA RESPOSTA A INCIDENTES

3.1. PLANEJAMENTO

Dentro de nossa estruturação o nosso recurso de proteção técnico compreende etapas a serem cumpridas para casos de incidentes, conforme apresenta-se em cada caso. Contudo nosso roteiro de detalhamento em caso incidente é:

3.2. IDENTIFICAÇÃO

Deve-se definir os critérios para detectar, identificar e registrar as situações de incidentes e descrever os recursos utilizados para a identificação de alertas de segurança e acionamento das equipes responsáveis para que sejam tomadas as devidas providências. Devem ser avaliadas todas as possíveis fontes capazes de representar uma ameaça à proteção de dados. Abaixo, algumas situações que devem ser consideradas suspeitas:

- Recebimento de e-mails com caracteres e/ou arquivos anexos suspeitos;
- Comportamento inadequado de dispositivos;
- Problema no acesso a determinados arquivos ou serviços;
- Furto ou roubo de dispositivos de armazenamento ou computadores com informações;
- Alerta de software antivírus;
- Consumo excessivo e repentino de memória em servidores ou computadores;
- Tráfego de rede incomum;
- Conexões bloqueadas por firewall;
- Furto ou roubo de dados físicos ou digitais.

Análise dos *logs* de tentativas de acesso não autorizado aos servidores. Situações de não cumprimento dos procedimentos internos também podem oferecer riscos à segurança dos dados pessoais, deste modo, a observação da Cartilha de Boas Práticas é de extrema importância. Todos os colaboradores e parceiros da Instituição são responsáveis por reportar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança

da informação. A notificação deve ser registrada por e-mail ao Encarregado de Proteção de Dados.

3.2 CATEGORIAS DA VIOLAÇÃO DE SEGURANÇA

A violação de segurança será classificada dentre as categorias citadas a seguir:

a. **Material:** quando o incidente envolve dados armazenados em dispositivos físicos. Exemplos: perda de HD, pastas de arquivos perdidas, smartphones perdidos, etc.

b. **Verbal:** quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.

c. **Cyberespaço:** quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o hackeamento, mau gerenciamento de patches, codificação incorreta, medidas de segurança insuficientes etc.

3.3 AVALIAÇÃO DA CRITICIDADE DE SEGURANÇA

Alguns fatores serão determinantes na definição da criticidade de um incidente:

I. A categoria da criticidade: de maneira genérica, o incidente será classificado em uma das categorias abaixo:

a. Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF;

b. Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF, e/ou pelo menos um dado sensível, não incluído raça, religião, nome social e dados de saúde;

c. Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

II. Dados legíveis/ilegíveis: dados protegidos por algum sistema de pseudonimização (criptografia, por exemplo).

III. Volume de dados pessoais: expresso em quantidade de registros, arquivos, documentos e/ou em períodos de tempo (uma semana, um ano, etc.).

IV. Facilidade de identificação de indivíduos: facilidade com que se pode deduzir a identidade das pessoas a partir dos dados envolvidos no incidente.

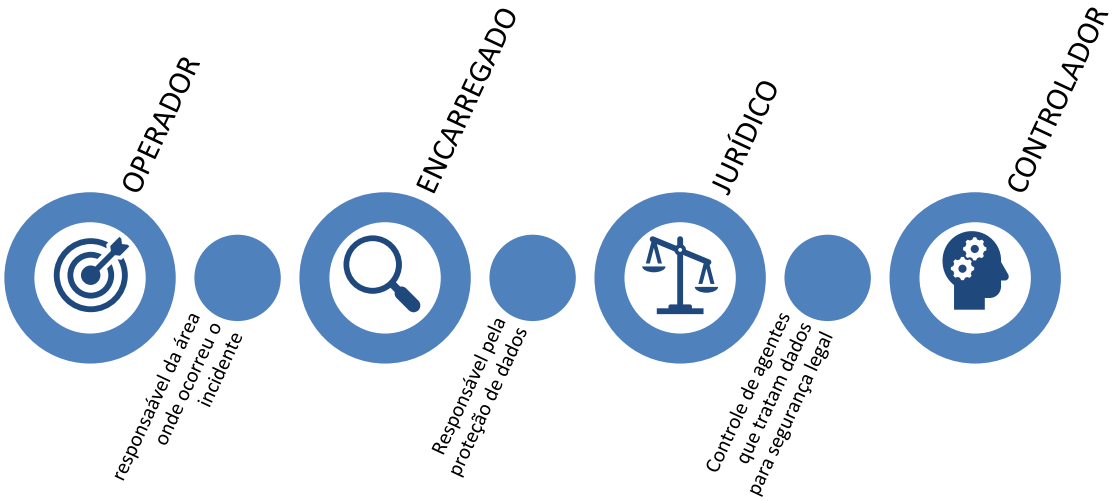
V. Indivíduos com características especiais e criança e adolescente: se o incidente afeta pessoas com características ou necessidades especiais.

VI. Número de indivíduos afetados: dentro de uma determinada escala, por exemplo, mais de 100 indivíduos.

3.4 CONTENÇÃO

Após um incidente ser identificado como uma violação de segurança, o mesmo deverá ser contido para evitar que outros sistemas sejam afetados ou que ocasionem danos maiores, deve ser previsto ações para a contenção de curto prazo, *backup* do sistema e contenção a longo prazo. Durante a contenção, deve haver o registro do

incidente e das medidas de contenção que foram adotadas, evitando ao máximo a perda de evidências e as provas do ocorrido. É importante lembrar da necessidade de trabalho colaborativo de toda a Instituição, sobretudo dos membros destacados a seguir:



4. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

4.1 DA LEI À RESPOSTA

Seguindo o disposto no artigo 48 da referida Lei, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional, tendo em seu conteúdo, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

4.2 FLUXO DA RESPOSTA A INCIDENTES.

Responsável pelo tratamento de dados da área afetada pelo incidente: a partir do momento que foi identificado um possível incidente de segurança de dados, a área responsável pela categoria de dados deve imediatamente informar o encarregado de dados para iniciar o processo de contenção.

- **Operador:** os operadores de dados, assim como os colaboradores internos, têm a responsabilidade de informar a ocorrência de incidente de segurança ao encarregado de dados, imediatamente.
- **Encarregado da Proteção de Dados:** após ser informado, o encarregado de proteção de dados deverá avaliar a existência do plano de ação para tal incidente e inicia-lo, e caso identifique o fato concreto de vazamento de dados pessoais, preencher o documento de Comunicação de Incidente de Segurança, para notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.
- **Jurídico:** deve ser comunicada no intuito de auxiliar no processo de comunicação à ANPD e titulares de dados e tomar as medidas jurídicas cabíveis.
- **Tecnologia da Informação:** será comunicada sempre que o incidente for relacionado a segurança da informação e que seja necessário medidas técnicas de tecnologia.
- **Administração:** deve validar as medidas propostas no Plano de Respostas a Incidentes e oferecer subsídios para que as mesmas sejam efetivamente cumpridas.

4.3 ERRADICAÇÃO

Após a ameaça ter sido contida, é necessário proceder com a sua remoção e a restauração dos sistemas que foram afetados, de modo que voltem a operar em sua normalidade.

4.4 RECUPERAÇÃO

Os sistemas afetados são restabelecidos e voltam a operar em ambiente de produção. É necessário definir as ações que devem ser tomadas para que o sistema volte a sua normalidade. Deve ser realizada uma varredura para identificar as perdas ocorridas e como recuperar o que foi perdido.

4.5 LIÇÕES APRENDIDAS

É fundamental que os mesmos erros não voltem a acontecer. Assim, é necessário que os incidentes sejam documentados, especificando quais foram os procedimentos de respostas utilizadas para contorná-los, de forma a manter um histórico das ocorrências e das ações tomadas.

TODAS AS POSSIBILIDADES QUE NÃO FOREM CONTEMPLADAS NESSE DOCUMENTO DEVEM SER DISCUTIDAS E ANALISADAS COM OS TITULARES, ENCARREGADO E CONTROLADOR.

De Mafra/SC para Frederico Westphalen/RS 19 de abril de 2023.