Política de Proteção de Dados

G&E

Última atualização	29 fevereiro de 2023

Definições

LGPD	Lei Geral de Proteção de Dados. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
Tratamento	Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado pessoal sensível	Dado pessoal sobre 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 natural.

1. Princípios de proteção de dados

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I. **Finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II. **Adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III. **Necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas

finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV. **Livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V. **Qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI. **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respetivos agentes de tratamento, observados os segredos comercial e industrial;

VII. **Segurança**: utilização de medidas 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 difusão;

VIII. **Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX. **Não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X. **Responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

1.1. Finalidade

a. Para garantir que o tratamento de dados sejam coletados para fins específicos, explícitos e legítimos, a [**GE**] deve manter um Inventário de Dados Pessoais (inventários de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD) e Registro de Sistemas (*e.g.*, TI).
b. O Inventário de Dados Pessoais deve ser revisado pelo menos uma vez por ano.
c. Os titulares de dados têm o direito de acessar seus dados pessoais e quaisquer solicitações feitas à [**GE**] e estas solicitações devem ser tratadas em tempo hábil.

1.2. Adequação

a. Todos os dados processados pela [**GE**] devem ser feitos em uma das seguintes bases legais: **(i)** mediante o fornecimento de consentimento pelo titular; **(ii)** para o cumprimento de obrigação legal ou regulatória pelo controlador; **(iii)** pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD; **(iv)** para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; **(v)** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; **(vi)** para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); **(vii)** para a proteção da vida ou da incolumidade física do titular ou de terceiro; **(viii)** para a tutela da saúde, em procedimento realizado por profissionais

da área da saúde ou por entidades sanitárias; **(ix)** quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou **(x)** para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (consulte as orientações da Autoridade Nacional de Proteção de Dados (ANPD) para obter mais informações).

b. A [**GE**] deve anotar a base legal apropriada no Inventário de Dados Pessoais.
c. Quando o consentimento é considerado uma base legal para o processamento de dados, a evidência de consentimento opt-in deve ser mantida com os dados pessoais.
d. Quando as comunicações são enviadas a indivíduos com base em seu consentimento, a opção de o indivíduo revogar seu consentimento deve estar claramente disponível e os sistemas devem estar em vigor para garantir que tal revogação seja refletida com precisão nos sistemas da [**GE**].

1.3. Necessidade

a. A [**GE**] deve garantir que os dados pessoais sejam adequados, relevantes e limitados ao que é necessário em relação aos fins para os quais são processados.
b. [*Adicionar considerações relevantes aos sistemas específicos da [**GE**]*].

1.4. Livre acesso

a. A [**GE**] deve garantir direito do titular dos dados de obter do controlador, nomeadamente a [**GE**], a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controle; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
b. Quando o término do tratamento de dados pessoais ocorrer aquando da transferência a terceiro, conforme descrito no artigo 15.º da LGPD, o titular dos dados tem o direito de ser informado de tal evento e dos requisitos de tratamento de dados dispostos na LGPD.
c. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos dos artigos 33.º e 34.º relativo à transferência internacional de dados no que concerne à LGPD.

1.5. Qualidade dos dados

a. A [**GE**] deve manter medidas técnicas e organizacionais que assegurem que os dados são precisos e, quando necessário, atualizados; devem ser tomadas todas as medidas razoáveis para garantir que os dados pessoais inexatos, tendo em conta os fins para os quais são tratados, sejam apagados ou retificados sem demora.
b. Para garantir que os dados pessoais não sejam mantidos por mais tempo do que o necessário, a [**GE**] deve estabelecer uma política de descarte para cada área em que os dados pessoais são processados e revisar esse processo anualmente.
c. A política de descarte deve considerar quais dados devem ser retidos, por quanto tempo e por quê.

1.6. Transparência

a. Para garantir que o tratamento de dados é lícito, justo e transparente, a [**GE**] deve manter um Inventário de Dados Pessoais (inventários de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD) e Registro de Sistemas (e.g., TI).
b. O Inventário de Dados Pessoais e o Registro de Sistemas deve ser revisado pelo menos uma vez por ano.
c. Os titulares de dados têm o direito de acessar seus dados pessoais e quaisquer solicitações feitas à [**GE**] e estas solicitações devem ser tratadas em tempo hábil.

1.7. Segurança

a. A [**GE**] deve garantir que os dados pessoais sejam armazenados de forma segura, usando medidas técnicas e organizacionais adequadas (*e.g.*, pseudonimização). Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
b. O acesso aos dados pessoais deve ser limitado ao pessoal que precisa de acesso e a segurança adequada deve ser implementada para evitar o compartilhamento não autorizado de informações.
c. Quando dados pessoais são apagados, isso deve ser feito com segurança, de forma que os dados sejam irrecuperáveis.
d. Soluções adequadas de *backup* e recuperação de desastres devem estar disponíveis.
e. [*Para mais detalhes ver : **POSIN** - **PO**lítica de **S**egurança da **IN**formação da [**GE**]].*

1.8. Prevenção

a. A [**GE**] deve garantir o uso de medidas técnicas e organizacionais como Relatórios de Impacto de proteção de dados (RIPD). O RIPD é um documento de comunicação e transparência que orienta a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como medidas, salvaguardas e mecanismos de mitigação.
b. A [**GE**] deve garantir uma cultura de prevenção. (Por exemplo: a **minimização de dados** ajuda a reduzir o risco de se usar dados de maneiras que não correspondem às expectativas dos usuários

– não se pode usar indevidamente os dados que não se coleta ou retém. A minimização diligente de dados pode reduzir ainda mais o número ou a complexidade das práticas de dados que precisam ser comunicadas aos usuários. Os **RIPD**s e as **verificações de conformidade** também podem ajudar a identificar sistematicamente os direitos dos usuários e os requisitos de transparência relativos ao sistema, que são importantes para o **processo de design de privacidade**.

c. [*A ação preventiva é uma atividade intencional que garante que o desempenho futuro do trabalho de proteção de dados esteja alinhado com o plano de gerenciamento de privacidade e proteção de dados. No gerenciamento de proteção de dados, a ação preventiva ajuda a evitar quaisquer incorreções futuras*].

1.9. Não discriminação

a. A [**GE**] deve garantir uma cultura de não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

1.10. Responsabilização e prestação de contas

a. A [**GE**] é responsável pelo cumprimento da LGPD e tem de poder comprová-lo "*responsabilidade e prestação de contas*")

b. [*Evidências podem ser o Inventário de Dados Pessoais, Politica de Privacidade, Política de Segurança da Informação, relatório concernente as avaliações de impacto à proteção de dados pessoais, inclusão de cláusulas contratuais de modo a salvaguardar a proteção de dados, relatório de análise e avaliação de riscos de acordo com a periodicidade definida (sempre que necessário) pela [**GE**], documentação que descreve a arquitetura física e lógica da [**GE**], controles de segurança da informação e matriz de responsabilidades, documento que evidencie um plano de continuidade operacional e plano de contingência, documento que evidencie o processo formal de Gestão de Incidentes, documento que evidencie o processo formal de gestão de solicitações dos titulares de dados, documentos de comprovação de registros de eventos e rastreabilidade*].

2. Pessoas, riscos e responsabilidades

2.1. Disposições gerais

a. Esta política se aplica a todos os dados pessoais processados pela [**GE**].

b. A pessoa responsável deve assumir a responsabilidade pela conformidade contínua da [**GE**] com esta política.

c. Esta política deve ser revista pelo menos uma vez por ano.

2.2. Riscos

A um nível mais elevado, os riscos na [**GE**] podem ser enquadrados por meio de três princípios comuns de segurança da informação oriundos da década de 1960, conhecidos como a tríade C-I-A, ou tríade de segurança da informação:

- Confidencialidade. Prevenção de divulgação não autorizada de informações.
- Integridade. Garantia de que as informações são protegidas contra alterações, modificações ou exclusões não autorizadas ou não intencionais.
- Disponibilidade (*availability*). As informações estão prontamente acessíveis para usuários autorizados.

Outros conceitos avançados de segurança da informação desenvolvidos anos após os princípios acima terem sido estabelecidos incluem:

- Prestação de contas (*accountability*). A propriedade da [**GE**] é rastreável através de documentos de comprovação de registros de eventos e rastreabilidade.
- Garantia. Todos os outros quatro objetivos são atendidos

Essas práticas aplicam um raciocínio de alto nível ao gerenciamento de riscos e definem os objetivos e metas da organização para a segurança de dados. Como as práticas de segurança são baseadas em considerações geográficas, legais, regulatórias e outras, todos os profissionais da [**GE**], especialmente os profissionais de privacidade e proteção de dados, devem compreender as estratégias organizacionais para atendê-las e identificar as partes interessadas para comunicação, colaboração e compartilhamento de informações.

A segurança da informação em geral é um tópico complexo que pode abranger toda a organização. Ao se familiarizar com as partes interessadas, o profissional de privacidade e proteção de dados terá canais abertos de comunicação de e para esses atores-chave em todos os aspectos da gestão do ciclo de vida.

É importante que os controles de segurança sejam parte integrante do processo de avaliação de privacidade.

Deste modo:

a. Sempre que necessário (na probabilidade de resultarem riscos para os titulares de dados), a [**GE**] deve elaborar **Relatórios de Impacto de proteção de dados (RIPD)**. O RIPD é um documento de comunicação e transparência que orienta a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como medidas, salvaguardas e mecanismos de mitigação.
b. A [**GE**] deve realizar **auditorias** concernentes a proteção de dados de acordo com a periodicidade definida (anualmente).
c. [*As auditorias concernentes à proteção de dados podem ser internas e ou externas*].

2.2. Responsabilidades

Todos os que trabalham para ou com a [**GE**] têm alguma responsabilidade por garantir que os dados sejam coletados, armazenados e manipulados de forma adequada.

Cada equipe que lida com dados pessoais deve garantir que eles sejam tratados e processados de acordo com esta política e os princípios de proteção de dados.

No entanto, essas pessoas têm áreas-chave de responsabilidade:

- O **Conselho de administração** e os **Presidentes** são os responsáveis finais por garantir que a [**GE**] cumpra com suas obrigações legais.

- O [**Encarregado de Proteção de Dados**], [**DATASHIELD BRASIL**], é responsável por:
    - Manter o conselho atualizado sobre as responsabilidades, riscos e questões de proteção de dados.
    - Revisão de todos os procedimentos de proteção de dados e políticas relacionadas, de acordo com um cronograma acordado.
    - Organizar treinamento e aconselhamento em proteção de dados para as pessoas abrangidas por esta política.
    - Lidar com questões de proteção de dados de funcionários e qualquer outra pessoa coberta por esta política.
    - Lidar com solicitações de titulares de dados no exercício dos seus direitos nos termos da LGPD, nomeadamente o direito a obter da [**GE**], em relação aos dados do titular pela [**GE**] tratados, a qualquer momento e mediante requisição: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD; (v) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (vi) eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD; (vii) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (ix) revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.
    - Verificar quando solicitado quaisquer contratos ou acordos com terceiros que possam lidar com dados confidenciais da empresa.

- O [**gerente de TI**], [**Richard Sales**], é responsável por:
    - Garantir a elaboração e aplicação da Política de Segurança de Informação.

- Garantir que todos os sistemas, serviços e equipamentos usados para armazenar dados atendam aos padrões de segurança aceitáveis.
- Executar verificações e testes regulares para garantir que o hardware e o software de segurança estejam funcionando corretamente.
- Avaliar quaisquer serviços de terceiros que a [**GE**] está considerando usar para armazenar ou processar dados (*e.g.*, serviços de computação em nuvem).

3. Diretrizes gerais da organização

- As únicas pessoas capazes de acessar os dados cobertos por esta política **devem ser aquelas que precisam deles para seu trabalho**.
- Os dados **não devem ser compartilhados informalmente**. Quando o acesso a informações confidenciais é necessário, os funcionários podem solicitá-lo a seus gerentes de linha.
- A [**GE**] **fornecerá treinamento** a todos os funcionários para ajudá-los a compreender suas responsabilidades ao lidar com dados.
- Os funcionários devem manter todos os dados protegidos, tomando precauções sensatas e seguindo as orientações abaixo.
- Em particular, **devem ser usadas senhas fortes** e nunca devem ser compartilhadas.
- Os dados pessoais **não devem ser divulgados** a pessoas não autorizadas, seja dentro da empresa ou externamente.
- Os dados **devem ser regularmente revisados e atualizados** se forem considerados desatualizados. Se não for mais necessário, ele deve ser excluído e descartado.
- Os funcionários **devem solicitar ajuda** de seu gerente de linha ou do encarregado de proteção de dados se não tiverem certeza sobre qualquer aspecto da proteção de dados.

4. Armazenamento de dados

Estas regras descrevem como e onde os dados devem ser armazenados com segurança. Perguntas sobre como armazenar dados com segurança podem ser direcionadas ao gerente de TI (ver **Política de Segurança de Informação** para mais detalhes). Quando os dados são armazenados em papel, devem ser mantidos em um local seguro, sem acesso por pessoas não autorizadas.

Essas diretrizes também se aplicam a dados que geralmente são armazenados eletronicamente, mas foram impressos por algum motivo:

- Quando não for necessário, o papel ou documentos **devem ser mantidos em uma gaveta trancada ou arquivo**.
- Os funcionários devem se certificar de que o papel e as impressões **não sejam deixados onde pessoas não autorizadas possam vê-los**, como em uma impressora.
- As **impressões de dados devem ser destruídas** e descartadas com segurança quando não forem mais necessárias.

Quando os dados são **armazenados eletronicamente**, devem ser protegidos contra acesso não autorizado, exclusão acidental e tentativas de hacking malicioso:

- Os dados devem ser **protegidos por senhas fortes** que são alteradas regularmente e nunca compartilhadas entre os funcionários.
- Se os dados forem **armazenados em mídia removível** (como um CD ou DVD), eles devem ser mantidos trancados com segurança quando não estiverem sendo usados.
- Os dados devem ser armazenados **apenas em unidades e servidores designados** e devem ser carregados apenas em **serviços de computação em nuvem aprovados**.
- Os servidores que contêm dados pessoais devem ser **colocados em um local seguro**, longe do espaço de escritório geral.
- Os dados devem ser objeto de **backup com frequência**. Esses backups devem ser testados regularmente, de acordo com os procedimentos de backup da [**GE**].
- Os dados **nunca devem ser salvos diretamente** em laptops ou outros dispositivos móveis, como tablets ou smartphones.
- Todos os servidores e computadores que contêm dados devem ser protegidos por um **software de segurança aprovado e um firewall**.

5. Uso de dados

5.1. Disposições gerais

Os dados pessoais não têm valor para [**GE**], a menos que a empresa possa fazer uso deles. No entanto, é quando os dados pessoais são acessados e usados que podem correr o maior risco de perda, corrupção ou roubo:

- Ao trabalhar com dados pessoais, os funcionários devem garantir que **as telas de seus computadores estejam sempre bloqueadas** quando não forem supervisionados.

- Os dados pessoais **não devem ser compartilhados informalmente**. Deve-se sempre usar formas de comunicação seguras aprovadas pelo TI (ver **Política de Segurança de Informação** para mais detalhes).

- Os dados devem ser **criptografados antes de serem transferidos eletronicamente**. O gerente de TI pode explicar como enviar dados para contatos externos autorizados.

- Os dados pessoais **nunca devem ser transferidos para fora do espaço geográfico brasileiro** exceto com o disposto nos termos do art. 33º da LGPD.

- Os funcionários **não devem salvar cópias de dados pessoais em seus próprios computadores**. Sempre acesse e atualize a cópia central de todos os dados.

5.2. Internet

Aviso de Privacidade

A G&E possui aviso de privacidade direcionado aos funcionários e usuários do site disponível no site da empresa.

6. Precisão de dados

A lei exige que a [**GE**] tome medidas razoáveis para garantir que os dados sejam mantidos precisos e atualizados.

Quanto mais importante for a exatidão dos dados pessoais, maior será o esforço que a [**GE**] deve fazer para garantir a sua exatidão.

É responsabilidade de todos os funcionários que trabalham com dados tomar medidas razoáveis para garantir que sejam mantidos o mais preciso e atualizado possível.

- Os dados devem ser **mantidos em poucos lugares conforme necessário**. A equipe não deve criar conjuntos de dados adicionais desnecessários.
- A equipe deve **aproveitar todas as oportunidades para garantir que os dados sejam atualizados**. Por exemplo, confirmando os detalhes de um cliente quando ele liga.
- A [**GE**] tornará mais fácil para os titulares dos dados atualizarem as informações que a [**GE**] mantém sobre eles.
- Os dados devem ser **atualizados à medida que imprecisões são descobertas**. Por exemplo, se um cliente não puder mais ser contatado pelo número de telefone armazenado, ele deve ser removido do banco de dados.

7. Solicitações dos titulares de dados

Todos os titulares de dados que têm os seus dados salvaguardados pela [**GE**] têm o direito de acessar aos seus dados pessoais e às seguintes informações:

- As finalidades do tratamento dos dados.
- As categorias dos dados pessoais em questão.
- Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais.
- Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo.
- A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento.
- O direito de apresentar reclamação a uma autoridade de controle.
- Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados.
- A existência de decisões automatizadas, incluindo a definição de perfis, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Se um titular de dados entrar em contato com a [**GE**] solicitando essas informações, isso é chamado de solicitação de acesso de titulares de dados.

As solicitações de acesso de titulares de dados devem ser feitas por e-mail, endereçadas ao controlador em [**dpo@geservicos.com**]. O controlador pode fornecer um formulário de solicitação padrão, embora titulares de dados não necessitem usá-lo.

O encarregado de dados com o trabalho conjunto da [**GE**] terá como objetivo fornecer os dados relevantes no prazo de até 15 (quinze) dias, contado da data do requerimento do titular conforme a alínea II do Art. 19 da LGPD.

O controlador sempre verificará a identidade de qualquer pessoa que faça uma solicitação de acesso do titular antes de entregar qualquer informação.

8. Divulgação de dados por outros motivos

Em certas circunstâncias, a Lei de Proteção de Dados permite que dados pessoais sejam divulgados para agências de aplicação da lei sem o consentimento do titular dos dados.

Nessas circunstâncias, [**GE**] divulgará os dados solicitados. No entanto, o controlador garantirá a legitimidade da solicitação, buscando ajuda do conselho e da equipe de proteção de dados (incluindo o encarregado de dados) da empresa, quando necessário.

9. Transparência

A [**GE**] visa garantir que os indivíduos estejam cientes de que seus dados estão sendo processados e que compreendam:

- Como os dados estão sendo usados.
- Como exercer seus direitos.

Para tanto, a empresa possui um aviso de privacidade, definindo como os dados relativos a pessoas físicas são usados pela empresa.

[*Disponível mediante solicitação uma versão desta política (em forma de aviso) também está disponível no site da empresa.]*

10. Incidentes de proteção de dados e vazamento de dados

O foco principal ao gerenciar qualquer incidente de privacidade é sempre a prevenção e / ou minimização de danos.

Em caso de violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada de, ou acesso a, dados pessoais, a [**GE**] deve **avaliar imediatamente o risco para os direitos e liberdades dos titulares de dados** e, se apropriado, relatar esta violação para o Titular de Dados e para a Autoridade Nacional de Proteção de Dados.

10.1. Cinco fatores que devem ser considerados:

1. A natureza dos elementos de dados vazados.
2. O número de indivíduos afetados.
3. A probabilidade de que as informações sejam acessíveis e utilizáveis.
4. A probabilidade de o vazamento de dados causar danos.
5. A capacidade da organização de mitigar o risco de danos.

10.2. Compreendendo os principais papéis e responsabilidades

Esta seção enfoca os principais elementos do planejamento de resposta a incidentes, detecção de incidentes, tratamento de incidentes e notificação aos titulares de dados e Autoridade Nacional de Proteção de Dados. A seção começa identificando as funções e responsabilidades que diferentes áreas da [**GE**] previamente identificadas podem desempenhar durante um vazamento de dados.

Os locais mais comuns de informações pessoais ou confidenciais em uma organização são:

- TI ou SI
- Jurídico e equipe DPO
- Recursos Humanos
- Comercial
- Finanças
- Departamento Pessoal
- Faturamento
- Financeiro
- Operacional
- Administrativo

→ TI ou SI

Função durante um vazamento de dados

Dada a incidência e a gravidade potencial dos ataques externos, é quase certo que o grupo de TI será contatado para lidar com o comprometimento dos dados. Como chefe da equipe, o gerente responsável concentrará a experiência do grupo em facilitar e apoiar investigações forenses, incluindo preservação de evidências. Além disso, o TI provavelmente terá a tarefa de supervisionar a exclusão de *malware* embutido e ferramentas de *hacker* e corrigir vulnerabilidades que podem ter precipitado o vazamento.

[*No entanto, embora os recursos internos de TI possam ter experiência e equipamento para investigar incidentes, geralmente é mais vantajoso trazer especialistas externos para identificar a causa e o escopo da violação e o tipo e localização dos dados comprometidos*].

→ Jurídico e equipe DPO

Função durante um vazamento de dados

Uma das principais funções do Jurídico e equipe DPO após um vazamento é aconselhar a privacidade e proteção de dados na [**GE**] e as equipes de gerenciamento sobre os requisitos de notificação de resposta: em particular, quem deve ser notificado, como e quando. Esses grupos normalmente incluem:

- Titulares de dados afetados
- Os meios de comunicação
- Equipes internas (por exemplo, relações públicas ou equipes de comunicação da [**GE**])
- Agências governamentais (e.g., Autoridade Nacional de Proteção de Dados - ANPD)
- Emissores de certidões e outros terceiros

O Jurídico e a equipe DPO também podem recomendar práticas de coleta e preservação de evidências forenses e preparar declarações para a Autoridade Nacional de Proteção de Dados (ANPD) e outros reguladores. O conhecimento sobre as leis e precedentes legais ajuda as equipes a direcionar e gerenciar com mais eficácia os vários elementos inter-relacionados de investigação e resposta a incidentes.

Elaborar e revisar contratos é outra área vital na qual o Jurídico e a equipe DPO devem estar envolvidas. Se os dados pertencerem a um cliente, eles podem interpretar os requisitos de notificação contratual e as obrigações de relatório e remediação. Caso a organização se torne alvo de litígios pós-violação, o Jurídico e a equipe DPO também pode orientar ou preparar a defesa.

→ **Recursos Humanos (RH)**

Função durante um vazamento de dados

Na sequência de um vazamento de dados, os RH pode servir como canal de informações da organização, trabalhando em estreita colaboração com as relações públicas ou comunicações corporativas para informar e atualizar os funcionários sobre o incidente. Durante o vazamento de dados, os funcionários podem ficar preocupados com os efeitos que um evento pode ter em seu emprego, ações da organização ou relações comerciais estratégicas. Portanto, os RH podem trabalhar com recursos internos ou externos para abordar e dissipar essas preocupações.

Se um incidente afetar os registros dos funcionários, a equipe de RH também pode ajudar os investigadores a determinar a localização, o tipo e a quantidade de dados comprometidos. Se a violação for atribuída a um funcionário da organização, espera-se que os RH colaborem com o gerente do indivíduo para documentar as ações do indivíduo e determinar as consequências apropriadas.

→ **Administrativo**

Função durante um vazamento de dados

Os profissionais do Administrativo são comunicadores especializados, especialmente qualificados em pesquisar e elaborar mensagens altamente direcionadas e orientadas ao consumidor. O Administrativo pode trabalhar com as equipes de gerenciamento e Relações públicas para estabelecer e manter uma mensagem positiva e consistente, tanto durante a crise quanto na notificação pós-vazamento de dados.

A experiência em envio de mensagens de correio eletrónico também pode ser benéfica no suporte à resposta ao vazamento de dados.

→ **Comercial**

Função durante um vazamento de dados

Nas mãos de um executivo de vendas ou gerente do desenvolvimento de negócio habilidoso, relacionamentos de alto valor podem florescer por muitos anos. Por causa de sua associação exclusiva com os clientes e do vínculo de confiança construído cuidadosamente ao longo do tempo, os tomadores de decisão do desenvolvimento de negócio são frequentemente solicitados a notificar as contas dos seus clientes e fornecedores principais quando os seus dados são atacados fazendo que ocorra um vazamento de dados. Receber notícias desfavoráveis de um amigo e parceiro de confiança pode diminuir o impacto e mitigar qualquer reação potencial, como por exemplo a perda de confiança ou passar a preferir um concorrente.

Depois de obter os fatos das equipes de TI, jurídico, RP ou outras equipes internas, o responsável deve entrar em contato com os clientes impactados e explicar cuidadosamente o que aconteceu. Precisão e transparência são essenciais. O desenvolvimento de negócio deve se cingir aos fatos conhecidos e, sob nenhuma circunstância, especular ou minimizar qualquer aspecto do vazamento de dados.

Sempre que possível, atualizações ou instruções especiais sobre o vazamento de dados devem ser prontamente fornecidas pelo desenvolvimento de negócio aos clientes e fornecedores principais. Isso fornecerá garantias de que alguém com autoridade executiva está proativamente envolvido na proteção dos interesses e da segurança dos dados.

→ **Finanças**

Função durante um vazamento de dados

Durante um vazamento de dados, a parte financeira aplica o seu conhecimento dos compromissos financeiros, obrigações e posição de caixa da organização para recomendar parâmetros de orçamento para responder ao evento.

Em empresas onde a resposta a incidentes é uma despesa fora do orçamento, a equipe financeira

geralmente tem a tarefa de ser proativa e criativa para garantir os recursos necessários para a resolução e notificação de fundos. Essa soma pode variar de organização para organização.

Antes ou depois de um vazamento de dados, os gerentes financeiros podem trabalhar com as seguradoras para negociar atualizações da apólice de seguro, incluindo melhorias na política geral de responsabilidade comercial (GCL) e a adição de cobertura de seguro “cibernético”.

O seguro cibernético é uma forma relativamente nova de proteção que preenche lacunas normalmente não cobertas pelo plano GCL. As organizações que buscam cobertura de seguro cibernético próprio têm uma gama surpreendentemente diversa de opções, incluindo proteção contra perdas decorrentes de destruição e roubo de dados, extorsão e *hacking*, e perda de receita com intrusão ou interrupção de rede.

Despesas de notificação, como por exemplo impressões e envio de cartas s e suporte de call center, podem ser incluídas em uma apólice, junto com a cobertura de responsabilidade cibernética de terceiros para fornecedores e parceiros. A parte financeira pode oferecer assistência inestimável na avaliação da necessidade e dos custos de atualização da cobertura de seguro.

→ **Presidente (patrocinadora)**

Função durante um vazamento de dados

Uma das primeiras e mais críticas medidas tomadas pelo alto executivo é distribuir prontamente os fundos e a mão-de-obra necessários para resolver o vazamento de dados (junto com jurídico e equipe DPO). Ter recursos prontamente disponíveis ajuda as equipes a conter e gerenciar rapidamente a ameaça e diminuir seu impacto geral.

No período imediatamente após um vazamento de dados, as equipes de relações públicas ou comunicações cuidarão da maior parte da interação com a comunicação social. Em algum momento, no entanto, os principais executivos podem ser chamados a comentar publicamente sobre a causa ou o estado do vazamento de dados.

Como acontece com qualquer organização que tenta administrar uma crise, precisão, autenticidade e transparência são absolutamente essenciais. Atualizações regulares de estado fornecidas pelo TI, suporte fornecido pelo jurídico e equipe DPO, e apoio de RP / comunicações podem preparar o presidente / patrocinadora para o escrutínio dos meios de comunicação potencialmente hostil.

Ao se dirigir ao público, os executivos devem seguir as recomendações de mensagens estabelecidas pela equipe DPO, jurídico e de comunicação. Isso ajuda a garantir a consistência da mensagem e reduz os riscos de comunicar a mensagem incorreta.

O presidente / patrocinadora, apoiado pela equipe DPO e jurídico, também pode ser aconselhado a entrar em contato com as autoridades nacionais de proteção de dados ou reguladores responsáveis para discutir o incidente e assegurar-lhes que o vazamento de dados está sendo tratado pela alta

administração.

Com a exposição de informações pessoais, a vida das pessoas e até mesmo a sua subsistência pode ficar em risco. Portanto, a linguagem e o tom usados para se dirigir ao público devem sempre ser escolhidos com muito cuidado. A sensibilidade com que uma organização responde a um vazamento de dados e as ações dos executivos durante o evento afetará a rapidez com que a confiança na marca da organização e as relações com o cliente são restauradas após o vazamento de dados.

→ **Atendimento ao público**

Função durante um vazamento de dados

Como parte de suas funções normais, os representantes de atendimento ao cliente são treinados para permanecer calmos quando confrontados e para difundir encontros potencialmente voláteis antes que eles aumentem. Esse treinamento, junto com a experiência de trabalho e entrega de mensagens com pré elaboradas em um ambiente cheio de pressão, pode permitir a implantação desses membros da equipe para lidar de forma eficaz com o tráfego de chamadas relacionadas ao vazamento de dados.

Usar recursos internos dessa maneira, no entanto, pode degradar potencialmente a qualidade do serviço para outras chamadas de serviço. Portanto, a perspetiva de aproveitar os recursos existentes para minimizar os gastos com resposta a vazamento de dados pode ser atraente apenas para algumas organizações.

Em empresas onde usar funcionários internos para atender chamadas relacionadas a vazamento de dados não é uma opção, o executivo de atendimento ao cliente deve considerar a contratação de terceirizadores experientes para lidar com o estouro de chamadas ou talvez gerenciar toda a iniciativa. Como parte de suas funções normais, os representantes de atendimento ao cliente são treinados para permanecer calmos quando confrontados e para difundir encontros potencialmente voláteis antes que eles aumentem. Esse treinamento, junto com a experiência de trabalho e entrega de mensagens com script em um ambiente cheio de pressão, pode permitir a implantação desses membros da equipe para lidar de forma eficaz com o tráfego de chamadas relacionadas à violação.

Usar recursos internos dessa maneira, no entanto, pode degradar potencialmente a qualidade do serviço para outras chamadas de serviço de entrada. Portanto, a perspectiva de aproveitar os recursos existentes para minimizar os gastos com resposta a violações pode ser atraente apenas para algumas organizações.

Em empresas onde usar funcionários internos para atender chamadas relacionadas a violações não é uma opção, o executivo de atendimento ao cliente deve considerar a contratação de terceirizados experientes para lidar com o estouro de chamadas ou talvez gerenciar toda a iniciativa.

[*Ver plano de gestão de incidentes para mais detalhes].*

FIM DA POLÍTICA