Procedimento para Gestão de Incidentes de Segurança da Informação e Dados Pessoais

1. Objetivo

O objetivo deste documento é estabelecer diretrizes e detalhar o processo para o gerenciamento de respostas a incidentes de segurança da informação envolvendo dados pessoais, incluindo vazamento, intrusão e mau uso de dados pessoais, de modo a atender aos requisitos da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (LGPD) e assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação, visando à mitigação dos danos aos titulares de dados e ao Grupo B&A.

2. Aplicabilidade

Este documento aplica-se a todos os colaboradores do Grupo B&A, parceiros e terceiros envolvidos no recebimento, gerenciamento e comunicação de incidentes de segurança da informação envolvendo dados pessoais.

3. Conceitos e definições importantes

Dados pessoais
Toda informação relacionada a pessoa natural identificada ou identificável, como: nome, RG, CPF, e-mail, endereço e etc.

Dados pessoais sensíveis
Dados pessoais 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.

Controlador de dados
Entidade que determina os meios e os propósitos do tratamento de dados pessoais.

Operador de dados
Entidade que trata dados pessoais em nome do Controlador.

Confidencialidade
Propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoas, sistemas, órgãos ou entidades não autorizadas ou não credenciados.

Disponibilidade
Propriedade pela qual se assegura que a informação esteja acessível e possa ser utilizada por pessoa física, sistema ou órgão quando necessário.

Integridade
Propriedade pela qual se assegura a preservação da precisão, consistência e confiabilidade dos dados tratados pela organização.

Vazamento de dados
Transmissão não-autorizada de dados de dentro de uma organização para um destino ou recipiente externo, de forma eletrônica ou física.

Intrusão
Invasão externa por agentes externos ou softwares maliciosos que resultem em acesso não autorizado, vazamento, alteração, apagamento, destruição ou encriptação de dados pessoais tratados pela organização.

Violação de dados pessoais
Incidente de segurança da informação que provoque interferência sobre a disponibilidade, integridade e confidencialidade dos dados pessoais.

4. Incidente de segurança com dados pessoais

Um incidente de segurança da informação com dados pessoais é a materialização de **qualquer violação de dados pessoais,** como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma ilícita ou inadequada de tratamento de dados pessoais, que possa colocar em risco os direitos e liberdades dos titulares de dados pessoais e causar danos a estes e ao negócio. São exemplos de incidentes de segurança com dados pessoais:

- Perda/roubo de notebook ou outro equipamento com acesso a arquivos e sistemas contendo dados pessoais;
- Perda de documentos físicos contendo dados pessoais, como fichas cadastrais, formulários, contratos, entre outros;
- Envio de e-mail para destinatário incorreto contendo arquivos ou documentos com dados pessoais;
- Exposição de arquivos contendo dados pessoais em diretório aberto na internet;
- Invasão de sistemas internos por agentes externos através dve falhas técnicas;
- Alteração de dados pessoais sem autorização por falha humana ou ação intencional de terceiro;
- Vazamento/exposição de arquivos na internet;
- Divulgação, em meio físico ou eletrônico, de forma intencional ou não, de informação não autorizada;
- Invasão por vírus, códigos maliciosos e etc;
- Compartilhamento/roubo de senhas;
- Uso ou acesso não autorizado a um sistema;
- Uso impróprio de ativo de informação.

5. Reporte de eventuais incidentes de segurança da informação com dados pessoais

Qualquer colaborador, terceirizado, prestador, parceiro ou fornecedor que tenha conhecimento ou suspeita de materialização de violação de informações confidenciais ou dados pessoais deve reportar imediatamente a situação ao **responsável,** Emily Nayara de Oliveira Sousa, através do seguinte ponto de **contato: privacidade@beacomercial.com.**

O colaborador designado é responsável por monitorar os canais apontados e realizar análise preliminar das comunicações recebidas de forma imediata.

6. Equipe de Resposta a Incidentes (ERI) de violação de dados pessoais

A Equipe de Resposta a Incidentes (ERI) é constituída de forma permanente por representantes dos seguintes setores:

Encarregado de Proteção de Dados
Emily Nayara de Oliveira Sousa
Analista de Gestão de Pessoas
privacidade@beacomercial.com

Suporte Interno da T.I.
Jailma de Medeiros Almeida
aministrativo@beacomercial.com

Membro do Comitê de Privacidade
Carlos Alberto Araújo dos Santos
controladoria@beacomercial.com

Outros setores do Grupo B&A podem ser solicitados a enviar representantes para compor provisoriamente a ERI de acordo com a natureza do incidente de violação de dados pessoais.

7. Atribuições e responsabilidades

7.1 Colaboradores, terceirizado, prestador, parceiro ou fornecedor

- Relatar eventuais ocorrências ou suspeitas de incidente de violação de dados pessoais ao Encarregado de Dados (ver item 5).

7.2 Encarregado de Dados/Responsável

- Direcionar, coordenar e mobilizar esforços da ERI através de elaboração de cronograma para cada estágio de resposta ao incidente;
- Avaliar a necessidade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e titulares de dados pessoais;
- Caso necessário, elaborar, juntamente com os demais membros da ERI, comunicação tempestiva à ANPD e aos titulares de dados afetados;
- Documentar as atividades desenvolvidas pela ERI;
- Definir, juntamente com a Presidência, se, ao final do processo de gestão do incidente, deve ser compartilhada informação internamente para apoiar a conscientização e sensibilização dos demais colaboradores e prevenir incidentes semelhantes (ver item 9.1).

7.3 Suporte Interno de Tecnologia da Informação (TI)

- Receber comunicação preliminar sobre incidente de violação de dados pessoais pelos canais estabelecidos (ponto de contato) (ver item 5);
- Avaliar comunicação e realizar registro formal do comunicado (incluindo nome, e-mail e vínculo com o Grupo B&A do comunicante) e da necessidade de comunicação do incidente à Equipe de Resposta a Incidentes;
- Iniciar o processo de investigação do incidente de violação de dados pessoais através da comunicação da ERI;
- Coletar e analisar tecnicamente as evidências do incidente de violação de dados pessoais visando identificar a causa e orientar o time de segurança nas medidas cabíveis;
- Realizar registro do incidente (ver item 8), incluindo detalhamento técnico do ocorrido, tentando identificar a natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade de dados afetados e consequências concretas e prováveis;
- Apoiar o Encarregado de Dados na elaboração da documentação para comunicação do incidente de violação dos dados pessoais à ANPD e aos titulares de dados, quando necessário;
- Elaborar e acompanhar indicadores de performance e desempenho dos resultados do tratamento de incidentes (ver item 10).

7.4 Presidência

- Apoiar o Encarregado de Dados na elaboração de documentação para comunicação do incidente de violação dos dados pessoais à ANPD e aos titulares de dados, quando necessário;

- Caso o incidente de violação de dados pessoais tenha causa em desvio de conduta ou infração ao Código de Ética por colaborador do Grupo B&A, o representante da Presidência deve direcionar o caso para medidas disciplinares cabíveis conforme contrato de trabalho e legislação aplicável;

- Apoiar o Encarregado de Dados em definir se, ao final do processo de gestão do incidente, deve ser compartilhada informação internamente para apoiar a conscientização dos demais colaboradores e prevenir incidentes semelhantes e, em caso positivo, direcionar a elaboração de comunicado.

8. Registro e notificação do incidente de violação de dados pessoais

A gestão de incidentes de segurança com dados pessoais deve contemplar processos que atendam aos seguintes objetivos:

Detecção: identificação de incidentes por monitoração, relatórios e denúncias - ver item 8.1;
Registro e análise: registro dos incidentes, análise, classificação, priorização - ver item 8.1;
Comunicação: às partes envolvidas e entidades externas caso necessário - ver itens 8.2 e 8.3);
Resposta: contenção do incidente, custódia de evidências, tratamento do incidente e da causa raiz - ver item 9;
Relatório: encerramento formal e análise pós fechamento para identificação de possíveis melhorias em processos e controles - ver item 9.

8.1 Detecção e Registro

A comunicação inicial a respeito de eventual incidente poderá ter várias origens, internas ou externas à companhia, como clientes, imprensa, autoridades, agentes externos, parceiros ou colaboradores, através de diversos canais.

Ao tomar conhecimento de eventual incidente de violação de dados pessoais, qualquer colaborador do Grupo B&A deve realizar a comunicação ao responsável do suporte interno de TI , conforme item 5.

Recebida a comunicação, avaliado seu conteúdo e reunida a ERI, o representante do suporte interno de TI, juntamente com o Encarregado de Dados, deve registrar formalmente o incidente, através do preenchimento do formulário contido no **Anexo I - Registro do Incidente de Violação de Dados Pessoais.**

8.2 Classificação do incidente

A classificação do incidente será realizada pela Equipe de Resposta a Incidentes e observará o tipo de dado e a quantidade de titulares envolvidos no incidente, além dos possíveis impactos financeiro, reputacional, estratégico, entre outros. A classificação deve considerar, minimamente, as seguintes questões:

- Quem são e quantos são os titulares de dados possivelmente afetados?
- Há menores de idade e/ou idosos entre os titulares afetados?
- Quais tipos de dados foram possivelmente afetados?
- Há possibilidade de dados sensíveis terem sido afetados?
- Quais os possíveis impactos aos titulares de dados?

8.3 Notificação à Autoridade Nacional de Proteção de Dados Pessoais (ANPD)

A comunicação da ocorrência de um incidente à ANPD será obrigatória nos casos em que o incidente de segurança de dados pessoais possa gerar riscos ou danos relevantes aos titulares de dados pessoais. A comunicação para a ANPD deve conter as informações do formulário disponível no link a seguir: *https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.*

O comunicado a ANPD deve ser enviado através de preenchimento de formulário eletrônico disponível no site e enviado por meio de peticionamento eletrônico:*https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico.*

A ANPD recomenda que os controladores de dados adotem posição de cautela, de modo a realizar a comunicação mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais podem ser fornecidas posteriormente, devendo informar se serão disponibilizadas informações em momento posterior, bem como quais meios estão sendo utilizados para obtê-las.

8.3.1 Prazo para notificação

O prazo para comunicação não está definido na legislação, que menciona “prazo razoável” (art. 48, §1º). Contudo, enquanto pendente a regulamentação, a ANPD recomenda que, após a ciência do incidente de segurança e havendo risco relevante, a Autoridade seja comunicada com a maior brevidade possível, considerando como parâmetro o prazo de 2 dias úteis, contados da data do conhecimento do incidente.

8.4 Notificação ao titular de dados pessoais

A partir de deliberação prévia da Equipe de Resposta a Incidentes, esta elaborará comunicado aos titulares de dados pessoais referentes ao incidente de violação que possam resultar em alto risco, sem demora injustificada. A comunicação individualizada aos titulares deve conter, se possível, as informações a seguir:

- Qual é o problema;
- Descrição da natureza dos dados pessoais afetados;
- Informação sobre os titulares envolvidos;
- Qual a seriedade do problema e o quão espalhado ele está;
- Indicação das medidas técnicas e de segurança usadas para proteção dos dados pessoais, observando os segredos comercial e industrial;
- Os motivos da demora, caso a comunicação não tenha sido imediata;
- As medidas que foram ou serão adotadas para reverter ou mitigar os prejuízos.

Caso o incidente de segurança e dados pessoais afete um grande volume de registro de titulares e dados pessoais, o Grupo B&A, através de deliberação da Presidência, decidirá se uma notificação pública em massa é mais apropriada que notificações personalizadas individuais. A avaliação levará em conta os recursos necessários para notificar cada titular individualmente e a capacidade da organização de fornecer adequadamente aos titulares de dados a notificação dentro de prazo razoável.

8.5 Decisão de não notificação

O Grupo B&A pode estar isento da notificação obrigatória para ANPD e titulares de dados quando o risco para os titulares não for considerado relevante, após avaliação das informações reunidas no cumprimento dos itens 8.1 e 8.2, sempre mediante deliberação da Presidência. Alguns exemplos para a não notificação são casos de violação de dados disponíveis publicamente, dados vazados mas protegidos por chave confidencial, perda temporária de acesso a dados e dados pessoais enviados acidentalmente para terceiros confiáveis, em virtude de relacionamento prévio com o Grupo B&A.

Se a decisão for pela não notificação, a justificativa para tanto deve ser registrada no Registro do Incidente de Violação de Dados Pessoais - Anexo I. Nesses casos, avaliar comunicação apenas ao gestor do setor de onde se originou o incidente.

9. Lições aprendidas

Na finalização do processamento de cada incidente de segurança com dados pessoais, o Encarregado, com suporte da Equipe de Resposta a Incidentes e demais setores envolvidos, deverá formalizar e registrar as lições aprendidas, objetivando reforçar o conhecimento e subsidiar futuras ações para gestão de incidentes. Deve-se registrar resposta para as seguintes questões:

- As medidas adotadas foram eficazes para a contenção do incidente?
- Os danos previstos foram evitados? (Sim, não, parcialmente)
- A dinâmica da ERI e o contato com outros setores foi eficaz?
- As estratégias de comunicação (interna e externa) foram eficazes?
- Os objetivos foram atingidos? (Sim, não, parcialmente)
- O cronograma para resposta ao incidente precisou de ajustes?
- Quais medidas podem ser tomadas para evitar incidentes semelhantes?

9.1 Comunicação interna - conscientização e sensibilização

Ao final da documentação das lições aprendidas, o Encarregado ou responsável, com suporte da Presidência, deve definir a relevância de compartilhamento da experiência do incidente de segurança com os demais colaboradores do Grupo B&A, visando aumentar a conscientização sobre o tema e prevenir incidentes semelhantes (ver item 7.2). Caso decida-se pelo compartilhamento, a Presidência deve direcionar e aprovar a elaboração de comunicado (ver item 7.5).

10. Monitoramento

O representante do suporte interno de TI será responsável por elaborar e acompanhar os indicadores de performance e desempenho dos resultados do tratamento de incidentes, conforme as métricas descritas abaixo e outras estabelecidas como convenientes:

- Quantidade de alertas recebidos: número de comunicados de incidentes de segurança originados interna ou externamente e comunicados à Equipe de Resposta a Incidentes (ERI);

- Quantidade de incidentes por causas: número de incidentes registrados, classificados pelas causas (falha de sistema, ações maliciosas, falha humana e etc);

- Quantidade de incidentes por nível de impacto: número de incidentes registrados, classificados pelo nível de impacto (muito baixo, baixo, médio, alto e extremo);

- Duração média do incidente: tempo total de duração dos incidentes/ número de incidentes registrados;

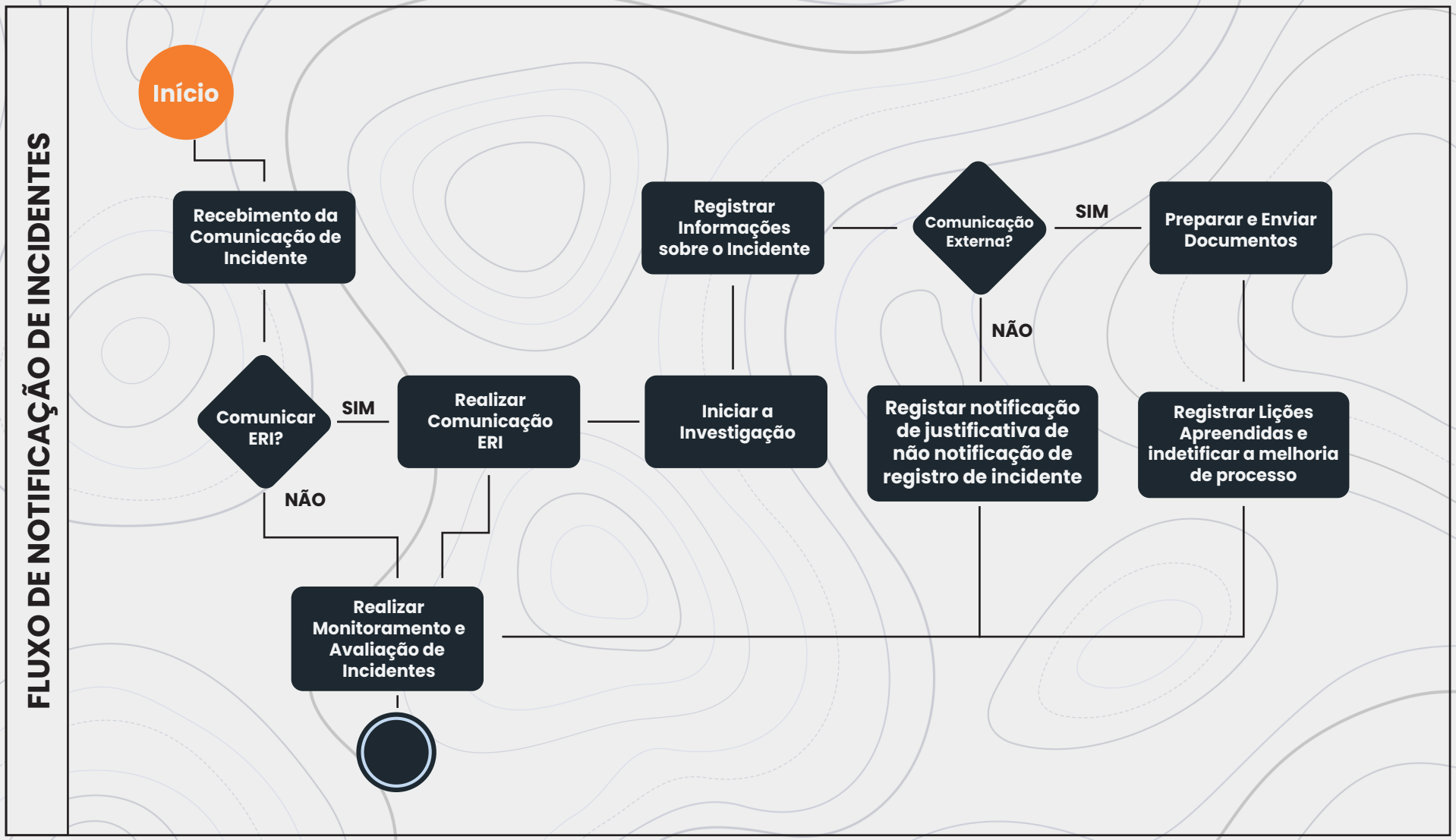
- Tempo médio de detecção: tempo total até a detecção dos incidentes/ número de incidentes registrados;

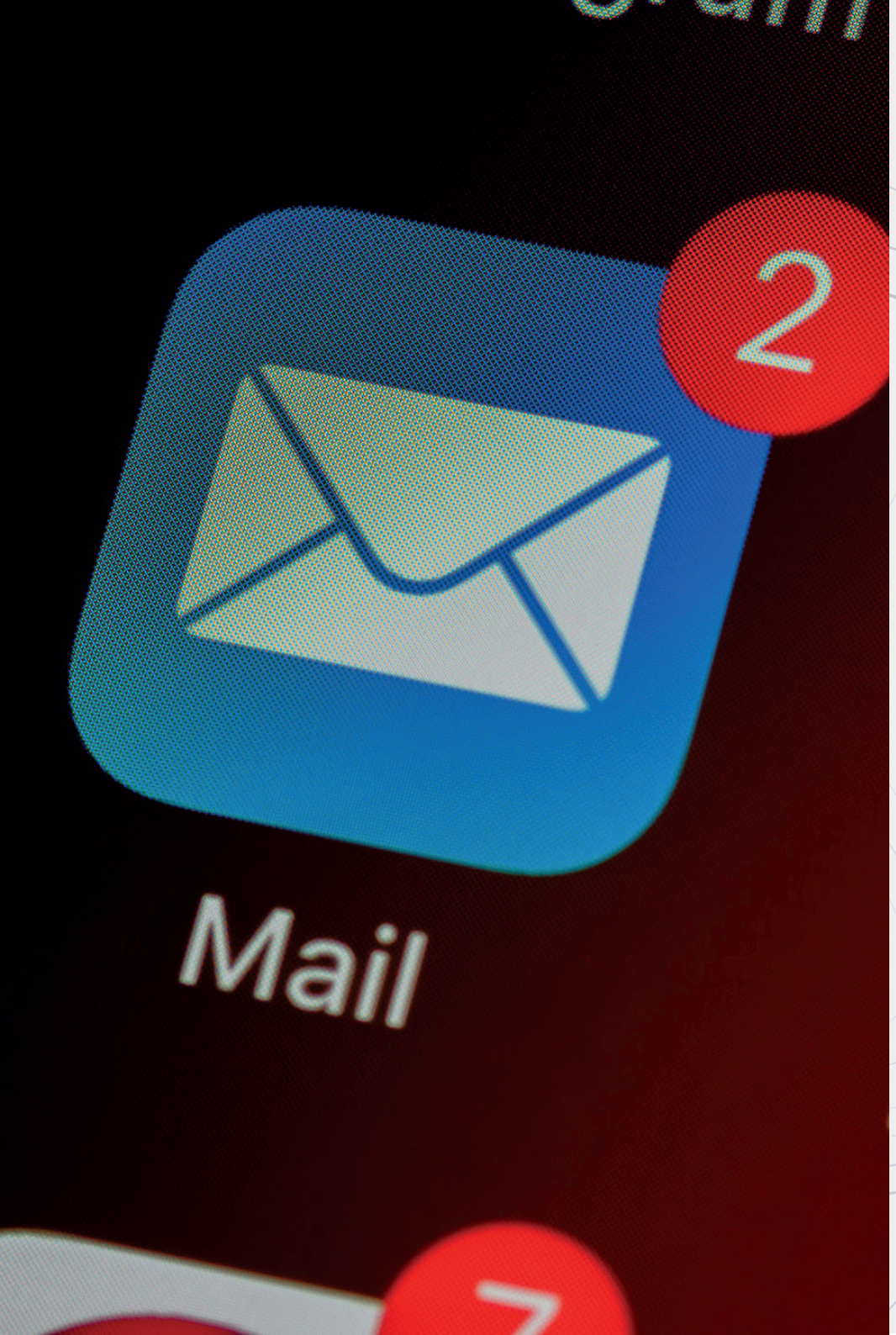
- Tempo médio de resposta ao incidente: tempo total entre a detecção e o encerramento do incidente/ número de incidentes registrados;

- Quantidade de titulares afetados: número de titulares afetados por incidente.

11. Fluxo do processo gestão de incidentes de segurança e dados pessoais

A Figura 1 apresenta o fluxo do processo para gestão de incidentes de segurança de informação e dados pessoais.





Comunicação e Informações

Em caso de dúvidas quanto à execução deste procedimento, entrar em contato com o Encarregado através do e-mail: **privacidade@beacomercial.com**