NONAME

PRIS-TAG

ABRIL DE 2023

Identificar e Responder a incidentes de Segurança

Documento sobre Respostas a Incidentes de Segurança em Dados Pessoais da Pris-TAG

Criado por:

Felype N. de Souza
Emilly Gabrielly
Sara Leal
Henrico Bela
Daniel Faria

Para:

Projeto Pris-TAG

Contextualização

A Lei Geral de Proteção de Dados (LGPD), Lei n.° 13.709/2018, tem como um de seus principais pilares a implementação de medidas de Segurança da Informação, que visam conscientizar entidades públicas e privadas sobre a importância da proteção dos dados. A LGPD considera que é mais grave não se prevenir e não adotar as medidas necessárias para proteger os dados do que sofrer um ataque ou vazamento de dados.

Dessa forma, a atividade de adequação às regras da LGPD não se resume apenas ao uso de medidas tecnológicas e padrões de segurança, mas também à elaboração, manutenção e revisão de documentos que garantam a adequação à lei e que otimizem os processos internos da entidade. Além disso, essas medidas também podem proteger a reputação da entidade, seus servidores, usuários dos serviços prestados e parceiros.

Definições Gerais

Para auxiliar a compreensão deste documento, serão estabelecidas conceitos às seguintes palavras referentes aos incidentes:

Agente de Tratamento: seguindo a LGPD, são aqueles que podem exercer algumas ações no tratamento de um incidente que coloque em risco a segurança dos dados pessoais. Os agentes são:

- **Controlador**: pessoa natural ou jurídica, de direito público ou privado, responsável por tomar as decisões sobre o tratamento dos dados pessoais. Na administração pública federal, os órgãos exercem as funções típicas do controlar.
- **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador, seguindo as instruções fornecidas pelo controlador. O operador é responsável por executar o processamento de dados conforme os padrões e políticas estabelecidas pelo controlador.

Em determinadas situações, o controlador e o operador podem precisar atuar como canal de comunicação entre os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), dependendo do contexto.

Encarregado: Uma pessoa pode ser indicada pelo controlador ou pelo operador para atuar como intermediária na comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Preservação das evidências:

1. Objetivos do plano: garantir que todas as evidências digitais sejam coletadas, armazenadas e preservadas adequadamente para uso em investigações e processos legais e de auditoria, sendo esses os arquivos de vídeo, áudio, imagens e outros tipos de arquivos que se mostrem necessários para o procedimento.

2. Sistemas e equipamentos envolvidos:

1. Sistemas de monitoramento: Câmeras acopladas nos pátios, refeitórios e corredores, com as configurações de visão noturna e reconhecimento de indivíduos;
2. Armazenamento e backup: uso da ferramenta Bucket S3 da AWS para armazenamento do Data Lake gerado;
3. Os sistemas utilizados para ETL(Extract Transform Loading) de dados: bancos de dados SQL e NoSQL

3. Políticas e procedimentos de prevenção de incidentes: aplicação de treinamentos e disponibilização de documentação sobre a manipulação e cuidados com os dados tratados, sendo assim, garantindo que todos os funcionários tenham ciência sobre o uso aceitável dos dados.

4. Controle de acesso: implementação das políticas de IAM (Identity Access Manager) para garantir que os acessos sejam liberados apenas para os que possuem autorização para tal.

5. Política de Backup:

1. Todos os dados importantes devem ser copiados e armazenados em um local seguro regularmente, seguindo uma programação de backup adequada.
2. O backup completo deve ser feito pelo menos uma vez por semana.
3. Backup incremental deve ser feito diariamente.
4. Os backups devem ser armazenados em um local separado do original para garantir a segurança dos dados.
5. A integridade dos backups deve ser verificada regularmente para garantir que os dados possam ser recuperados em caso de necessidade.
6. Uma pessoa responsável deve ser designada para gerenciar e monitorar o processo de backup e garantir que a programação de backup esteja sendo seguida.
7. A política de backup deve ser revisada e atualizada regularmente para garantir que esteja alinhada com as necessidades do negócio.

6. Período de retenção:

1. A política de retenção deve ser estabelecida para garantir que os dados sejam mantidos por tempo suficiente para cumprir com as obrigações legais, regulatórias ou de negócios, além de garantir que os dados estejam disponíveis para auditoria e investigações internas.
2. Os dados devem ser retidos por um período mínimo de 12 meses.
3. O período de retenção pode ser estendido para até 7 anos para cumprimento das regras de compliance.
4. Os dados que não são mais necessários devem ser excluídos ou arquivados de acordo com a política de retenção.
5. Uma pessoa responsável deve ser designada para gerenciar e monitorar a política de retenção e garantir que esteja sendo seguida.
6. A política de retenção deve ser revisada e atualizada regularmente para garantir que esteja alinhada com as necessidades do negócio e com as regulamentações aplicáveis.

Comunicação à Seguradora, quando pertinente

A resposta imediata à seguradora seria em um prazo de 5 horas após ocorrido o vazamento dos dados, sempre mantendo contato direto com as autoridades, e deixando os nossos clientes a par da situação.

Exemplo de comunicação com a seguradora:

“Prezada Seguradora,

Gostaríamos de comunicar que ocorreu um vazamento de dados em nossa empresa em relação ao serviço de localização de prisioneiros nas unidades prisionais. Embora tenhamos implementado medidas de segurança rigorosas para proteger as informações de nossos clientes, ocorreu uma violação em nosso sistema que resultou no vazamento de dados confidenciais.

Lamentamos profundamente o ocorrido e estamos trabalhando para remediar a situação o mais rápido possível. Tomamos medidas imediatas para reforçar a segurança de nossos sistemas e para garantir que isso não aconteça novamente. Além disso, estamos trabalhando em conjunto com as autoridades competentes para investigar o ocorrido e tomar as medidas necessárias.

Queremos garantir que tomamos todas as precauções para proteger a integridade de nossos clientes e suas informações. Estamos empenhados em garantir a segurança e privacidade dos dados dos nossos clientes e faremos todos os esforços para assegurar que este incidente não afete nossa relação de confiança e parceria com sua seguradora.

Pedimos desculpas pelo ocorrido e permanecemos à disposição para fornecer qualquer informação adicional que possa ser necessária.

Atenciosamente,

Equipe NoName”

Comitê de Crise

Dependendo do tipo e categoria dos dados violados, o comitê será composto por indivíduos identificados com base no tipo e necessidades da crise, com um membro atuando como líder. Com a constituição do comitê, será desenvolvido um plano de ação e treinamento para qualificar cada membro do comitê. A comunicação pode ser melhorada através da criação de canais diretos entre membros do comitê.

Ao lidar com uma crise, o plano deve ser revisado periodicamente para garantir sua eficácia no gerenciamento da crise.

Em seguida o passo a passo para a criação e formação do comitê de crise:

1. Identificar as necessidades e objetivos específicos para o comitê de crise.
2. Definir o escopo e autoridade do comitê, incluindo sua composição e mandato.
3. Identificar os membros do comitê com base em suas áreas de especialização.
4. Designar um líder do comitê de crise.
5. Desenvolver um plano de crise detalhado.
6. Capacitar os membros do comitê mediante treinamentos.
7. Estabelecer canais de comunicação claros e eficientes.
8. Revisar e atualizar regularmente o plano de crise e procedimentos.

Causa-raiz do Incidente

Nossa empresa leva muito a sério a proteção das informações confidenciais de nossos clientes e está comprometida em garantir a segurança dos dados que mantemos. No entanto, reconhecemos que vazamentos de dados podem ocorrer mesmo com as melhores medidas de segurança em vigor. É por isso que estabelecemos um plano de contingência para lidar com tais situações, composto pelos seguintes passos:

1. Identificação do incidente: se ocorrer um vazamento de dados, nossa equipe de segurança da informação trabalhará para identificar o incidente o mais rápido possível. Isso envolverá a coleta de informações sobre o que aconteceu, quando e quais dados foram comprometidos.

2. Isolamento do problema: em seguida, trabalharemos para isolar o problema para evitar que se espalhe ainda mais. Isso pode envolver a desativação de sistemas ou aplicativos, que foram comprometidos ou a suspensão do acesso a determinados dados.

3. Notificação das partes interessadas: assim que tivermos informações suficientes sobre o incidente, notificaremos todas as partes interessadas, incluindo nossos clientes, fornecedores e outras partes relevantes. A notificação será realizada o mais rapidamente possível e conforme as leis e regulamentos aplicáveis.

4. Investigação do incidente: uma vez que o incidente foi isolado e as partes interessadas foram notificadas, nossa equipe de segurança da informação trabalhará para investigar o incidente em mais detalhes. Isso pode envolver a análise de logs de sistema, a identificação de possíveis pontos de entrada ou outros processos forenses para identificar a origem do problema.

5. Remediação do problema: assim que tivermos uma compreensão completa do que aconteceu e como, trabalharemos para remediar o problema o mais rapidamente possível. Isso pode envolver a correção de vulnerabilidades de segurança, a atualização de sistemas ou aplicativos comprometidos e outras medidas para garantir a segurança dos dados.

6. Avaliação do incidente: por fim, localizaremos o incidente e seguiremos medidas para lidar com ele. Isso incluirá a identificação de áreas onde podemos melhorar nossa segurança de dados e a implementação de novas medidas de segurança para evitar futuros vazamentos.

Nosso plano de contingência para vazamentos de dados nos permite lidar com essas situações de maneira eficaz e eficiente. Se você tiver alguma dúvida sobre nossas medidas de segurança de dados, não hesite em entrar em contato conosco.

Contenção da vulnerabilidade

Para lidar com a contenção de vulnerabilidades, nossa empresa estabeleceu um processo rigoroso que envolve a identificação, isolamento e remediação das vulnerabilidades. Esse processo inclui:

1. Identificação da vulnerabilidade: nossa equipe de segurança da informação é responsável por monitorar continuamente nossos sistemas e dados em busca de vulnerabilidades. Quando uma vulnerabilidade é identificada, a equipe trabalha imediatamente para avaliar a gravidade do problema e determinar o melhor curso de ação.

2. Isolamento da vulnerabilidade: a equipe de segurança da informação trabalhará para isolar a vulnerabilidade para minimizar seu impacto em nossos sistemas e dados. Isso pode envolver a suspensão do acesso a determinados sistemas ou dados afetados pela vulnerabilidade.

3. Remediação da vulnerabilidade: uma vez que a vulnerabilidade tenha sido isolada, nossa equipe de segurança da informação trabalhará para desenvolver e implementar um plano de ação para corrigir o problema. Isso pode envolver a aplicação de patches de segurança, atualizações de software ou outras medidas para proteger nossos sistemas e dados.

4. Monitoramento contínuo: depois que a vulnerabilidade foi remediada, nossa equipe de segurança da informação supervisionará continuamente nossos sistemas e dados para garantir que a vulnerabilidade não ressurja e que nossos sistemas permaneçam seguros.

Nosso compromisso com a segurança de seus dados é contínuo e nossa equipe de segurança da informação está sempre trabalhando para garantir que nossos sistemas e dados estejam protegidos contra ameaças cibernéticas.

Identificação da exposição de dados

A identificação da exposição de dados é um passo crítico em nossos esforços de resposta a incidentes. Pois é nesse passo em que identificamos a gravidade da exposição e há uma série de etapas para a realização desse esforço. Além desses passos é importante realizar um processo contínuo para a identificação de eventuais violações de segurança para serem tomadas as devidas ações a fim de mitigar possíveis riscos que a empresa e seus clientes possam sofrer.

1. Monitoramento de sistemas e redes: Utilizar ferramentas de monitoramento, como sistemas de detecção de intrusão (IDS), sistemas de prevenção de intrusão (IPS), firewalls, e outros, para identificar atividades suspeitas, tentativas de acesso não autorizado ou tráfego incomum nos sistemas e redes da empresa.

2. Análise de registros de eventos: Analisar registros de eventos de sistemas, aplicativos e infraestrutura de rede para identificar anomalias ou comportamentos suspeitos, como tentativas de login falhadas, acesso a arquivos ou pastas sensíveis, alterações não autorizadas de configuração, entre outros.

3. Monitoramento de atividades de usuários: Monitorar as atividades dos usuários com acesso aos dados sensíveis, como funcionários, contratados e terceiros, para identificar comportamentos anormais, acesso excessivo ou inesperado a sistemas, ou dados, ou atividades suspeitas.

4. Varredura de vulnerabilidades: Realizar varreduras de vulnerabilidades nos sistemas e redes da empresa para identificar possíveis brechas de segurança que possam expor dados sensíveis.

5. Análise de incidentes anteriores: Analisar incidentes de segurança anteriores e suas causas raiz para identificar possíveis exposições de dados e áreas de vulnerabilidade que precisam ser abordadas.

6. Revisão de políticas e práticas de segurança: revisar as políticas, procedimentos e práticas de segurança da empresa para identificar possíveis lacunas ou falhas que resultem na exposição de dados.

7. Auditoria de sistemas e redes: Realizar auditorias de segurança periódicas em sistemas e redes para identificar vulnerabilidades, configurações inadequadas ou exposições de dados.

8. Monitoramento de atividades externas: Monitorar atividades externas, como ataques de hackers, vazamentos de dados em outras empresas ou sites de venda ilegal de dados, para identificar se os dados da empresa foram expostos.

Monitoramento da surface e deep web

A varredura da web é o processo de coleta de informações na internet que envolve o monitoramento da surface web e da deep web para melhor entendimento do problema. Isso pode ser feito usando ferramentas de busca convencionais para a surface web, e mecanismos de busca especializados para a deep web. No entanto, é fundamental garantir que a varredura da web seja realizada de forma ética e legal, em compliance com as leis e regulamentos aplicáveis, e com respeito à privacidade e aos direitos de propriedade intelectual de terceiros. É recomendável que seja realizada por profissionais experientes e dentro dos limites legais e éticos, é importante ressaltar que a varredura deve ser realizada em loop durante todo o processo investigativo.

Elaboração de Score de gravidade do incidente

Fator de Gravidade	Valores Possíveis
Impacto nos Negócios (IN)	Baixo (1-3) / Médio (4-7) / Alto (8-10)
Quantidade de Dados Afetados (QDAfet)	Baixo (1-3) / Médio (4-7) / Alto (8-10)
Tipo de Dados Afetados (TDAfet)	Públicos (1-3) / Internos (4-7) / Sensíveis (8-10)
Tempo de Duração do Incidente (TDInc)	Curto (1-3) / Médio (4-7) / Longo (8-10)
Causa do Incidente (CInc)	Acidente (1-3) / Negligência (4-7) / Malicioso (8-10)

Métricas de avaliação:

$$SG = (IN + QDAfet + TDAfet + TDInc + CInc) / 5$$

O valor resultante do score de gravidade varia de 1 a 10, na qual 1 indica um incidente de baixa gravidade e 10 indica um incidente de alta gravidade.

Comunicação aos Titulares e às Autoridades

Diante de um incidente, nossa empresa agiria imediatamente para solucioná-lo e adotaremos as seguintes medidas comunicativas para salientar os nossos clientes:

Através da rede social Twitter, encaminharemos em postagem a seguinte declaração pública:

“Caros usuários, gostaríamos de informá-los que identificamos uma possível violação de segurança em nossa rede social, que pode ter afetado dados pessoais. Estamos trabalhando incansavelmente com especialistas em segurança para solucionar o problema e garantir a segurança de nossos usuários.”

“Assim que tivermos mais informações, atualizaremos todos os usuários sobre a situação. Pedimos desculpas pelos transtornos causados e reiteramos nosso compromisso inabalável com a proteção da privacidade e segurança de nossos usuários.”

“Agradecemos sua compreensão e cooperação durante este processo.

Atenciosamente,
Noname.”

Também realizaremos as seguintes declarações abertas a possíveis mídias jornalistas:

Assunto: Comunicação sobre incidente de segurança
Prezados,

Gostaríamos de informá-lo(a) que ocorreu um incidente de segurança em nossa rede social que pode ter afetado seus dados pessoais. Estamos entrando em contato para fornecer informações sobre o incidente, as medidas que estamos tomando para solucioná-lo e as ações que você pode tomar para proteger seus dados pessoais.

No dia (data referida), identificamos que houve uma violação de segurança em nosso sistema. A investigação inicial indica que informações pessoais, como dados pessoais dos apenados, quantidade de condenados nas celas, podem ter sido acessadas por terceiros não autorizados.

Assim que tomamos conhecimento do incidente, adotamos as seguintes medidas para solucioná-lo:

Isolamos a área afetada e desativamos o acesso não autorizado. Realizamos uma análise completa do incidente para identificar as causas e implementamos melhorias nos nossos sistemas para evitar que incidentes semelhantes ocorram novamente.

Estamos trabalhando com autoridades e especialistas em segurança de dados para garantir a proteção dos dados pessoais de nossos usuários.

Embora não tenhamos evidências de que seus dados pessoais tenham sido usados indevidamente, recomendamos que você tome as seguintes medidas para proteger seus dados pessoais:

Altere sua senha de acesso à nossa rede social e a qualquer outra conta que você tenha usado a mesma senha. Fique atento(a) a mensagem de phishing ou fraudes que possam tentar se passar por nossa rede social ou outras empresas relacionadas.

Estamos comprometidos em proteger a privacidade e segurança de seus dados pessoais e lamentamos sinceramente qualquer inconveniente que isso possa causar. Se você tiver dúvidas ou precisar de mais informações, por favor, entre em contato conosco.

Atenciosamente,

Noname.

Resposta a questionamentos dos consumidores

Quando ocorrer um incidente de segurança que afete nossos consumidores, nossa equipe de atendimento ao cliente trabalhará rapidamente para garantir que os consumidores afetados sejam informados da situação e recebam as informações necessárias para proteger suas informações pessoais. Para ajudar nossos agentes de atendimento ao cliente a lidar com as perguntas e preocupações dos consumidores, elaboramos um script claro e preciso que possa ser usado para responder a perguntas comuns. Esse script será elaborado da seguinte forma:

1. Identificação das perguntas mais comuns: nossa equipe de atendimento ao cliente revisará as perguntas mais comuns que os consumidores fazem em relação ao incidente de segurança e identificará os principais tópicos que precisam ser abordados em um script.

2. Desenvolvimento do script: nossa equipe de segurança da informação e de atendimento ao cliente trabalharão juntas para desenvolver um script claro e preciso que aborde todas as perguntas e preocupações mais comuns dos consumidores. O script será redigido de maneira clara e simples, sem jargões técnicos, para garantir que seja facilmente compreensível pelos consumidores.

3. Revisão do script: após a elaboração inicial do script, nossa equipe de segurança da informação revisará e aprovará o script para garantir que todas as informações estejam corretas e atualizadas. Quaisquer alterações necessárias serão feitas nessa fase.

4. Treinamento dos agentes de atendimento ao cliente: após a aprovação do script, nossa equipe de atendimento ao cliente será treinada em como usar o script para responder a perguntas e preocupações dos consumidores de maneira clara e precisa. O treinamento incluirá uma revisão completa do script e prática em como lidar com as perguntas mais comuns dos consumidores.

5. Monitoramento contínuo: nossa equipe de atendimento ao cliente e de segurança da informação irá monitorar continuamente as perguntas e preocupações dos consumidores em relação ao incidente de segurança e fará ajustes no script, conforme necessário, para garantir que continue sendo relevante e útil.

Nosso objetivo é garantir que nossos consumidores recebam informações claras e precisas sobre a situação e saibam que estamos trabalhando para proteger suas informações pessoais. Estamos comprometidos em fornecer um excelente atendimento ao cliente em todos os momentos e garantir que nossos agentes estejam preparados para lidar com quaisquer perguntas ou preocupações dos consumidores.

Fato Relevante, Se Cabível

A publicação do fato relevante deve ser feita imediatamente após a confirmação da informação relevante, seguindo os prazos e procedimentos estabelecidos pelas regulamentações aplicáveis, garantindo a transparência e igualdade na divulgação das informações para todos os stakeholders. O fato relevante é publicado após o fechamento da bolsa de valores e deve ser assinado por um representante da empresa. Segue exemplo de nota a ser publicada:

A empresa NoName informa que implementou um processo de varredura da web para monitoramento da surface web e deep web, como parte de suas atividades de coleta de informações na internet. A varredura da web é realizada por meio de ferramentas de busca convencionais para a surface web e mecanismos de busca especializados para a deep web.

A Noname ressalta que a varredura da web é realizada de forma ética e legal, conforme as leis e regulamentos aplicáveis, e com respeito à privacidade e aos direitos de propriedade intelectual de terceiros. Asseguramos que todas as atividades de varredura da web são realizadas por profissionais experientes e dentro dos limites legais e éticos.

A implementação do processo de varredura da web visa auxiliar a empresa na coleta de informações relevantes sobre o mercado, concorrentes, produtos, notícias e outros tipos de conteúdo disponíveis publicamente, para subsidiar suas estratégias de negócio e tomada de decisões.

A empresa reforça seu compromisso com a conformidade legal e ética em todas as suas atividades, incluindo a varredura da web, e reitera que todas as informações coletadas são tratadas de acordo com suas políticas de privacidade e proteção de dados.

Essa divulgação de fato relevante tem caráter puramente informativo e visa proporcionar transparência sobre as atividades de varredura da web realizadas pela empresa.

11/04/2023

ASS: Henrico Bella

Relatório Forense do Incidente

Com satisfação, a Noname comunica que cumpriu com as obrigações previstas pela Lei Geral de Proteção de Dados (LGPD) ao responder ao Relatório Forense. Para tal, a empresa adotou as medidas necessárias e preencheu o Formulário de Comunicação de Incidente de Segurança com Dados Pessoais, o qual foi devidamente encaminhado à Autoridade Nacional de Proteção de Dados (ANPD).

Tendo em vista a relevância do tema, foi garantido um rigoroso cumprimento do processo, visando sempre a transparência e a segurança dos dados de nossos clientes e parceiros. Como comprovação do envio, segue anexo o documento devidamente preenchido e, a título de praticidade, disponibilizamos o link para download do mesmo. A Noname reitera seu compromisso com a proteção de dados pessoais e agradece a oportunidade de prestar esclarecimentos sobre o ocorrido.

Segue o Link do preenchimento do Relatório Forense pela Noname:

` Formulario-forense-resposta-Noname.pdf

Elaboração de notas reativas à imprensa

Quando ocorrer um incidente de segurança que afete nossos clientes e que possa gerar interesse na mídia, nossa equipe de comunicação trabalhará rapidamente para elaborar notas reativas à imprensa. Essas notas terão como objetivo fornecer informações precisas e atualizadas sobre o incidente, bem como transmitir a mensagem de que estamos trabalhando para solucionar o problema e proteger os dados de nossos clientes. Para elaborar essas notas, seguiremos as seguintes etapas:

1. Identificação das informações relevantes: nossa equipe de segurança da informação trabalhará em conjunto com a equipe de comunicação para identificar as informações relevantes sobre o incidente, incluindo a natureza do problema, as informações pessoais dos clientes afetados e as medidas tomadas para solucionar o problema.

2. Desenvolvimento das notas reativas à imprensa: nossa equipe de comunicação usará as informações relevantes identificadas na etapa anterior para elaborar notas reativas à imprensa. Essas notas serão escritas de forma clara e objetiva, evitando jargões técnicos e fornecendo informações claras e precisas sobre o incidente e as medidas tomadas para solucioná-lo.

3. Revisão das notas reativas à imprensa: após a elaboração inicial das notas reativas à imprensa, nossa equipe de segurança da informação revisará e aprovará as notas para garantir que todas as informações estejam corretas e atualizadas. Quaisquer alterações necessárias serão feitas nessa fase.

4. Distribuição das notas reativas à imprensa: as notas reativas à imprensa serão distribuídas à imprensa e publicadas em nossos canais oficiais de comunicação. Nossa equipe de comunicação trabalhará para garantir que as notas sejam publicadas rapidamente e que as informações sejam transmitidas de forma clara e objetiva.

5. Monitoramento contínuo: nossa equipe de comunicação e de segurança da informação irão monitorar continuamente a cobertura da mídia sobre o incidente e fará ajustes nas notas reativas à imprensa, conforme necessário, para garantir que continuem sendo relevantes e úteis.

Nosso objetivo é fornecer informações precisas e atualizadas sobre o incidente, garantir a transparência em relação ao que aconteceu e como estamos solucionando o problema, e transmitir a mensagem de que estamos comprometidos em proteger os dados de nossos clientes. Estamos preparados para lidar com crises e trabalharemos rapidamente para elaborar notas reativas à imprensa que transmitem essas informações de forma clara e objetiva.

Estratégia jurídica para contenção

Avaliação das leis e regulamentos aplicáveis: A equipe jurídica da empresa avalia as leis e regulamentos aplicáveis à Noname, incluindo leis trabalhistas, leis ambientais, de propriedade intelectual, fiscais, cumprimento das leis criminais, entre outras.

Identificação das possíveis violações: Com base na análise legal, a equipe jurídica localiza possíveis violações cometidas pela Noname. Isso pode incluir a falta de pagamento de horas extras aos funcionários, o descarte inadequado de resíduos tóxicos, a violação de patentes de terceiros, entre outras violações.

Reunião de evidências: Para apoiar as alegações de violações, a equipe jurídica da empresa deve reunir evidências relevantes, incluindo documentos, testemunhos, fotos, vídeos e outras informações que possam ajudar a comprovar as violações. É importante que as evidências sejam coletadas de forma legal e ética.

Entrada com ação legal: Com base nas leis e regulamentos aplicáveis e nas evidências coletadas, a equipe jurídica da empresa entra com uma ação legal contra a Noname Isso pode incluir uma ação trabalhista, uma ação ambiental, uma ação de propriedade intelectual, entre outras ações.

Negociação de um acordo: Em alguns casos, pode ser possível chegar a um acordo com a empresa para resolver as questões legais de forma amigável. Isso pode envolver o pagamento de indenizações, a implementação de mudanças nas práticas da empresa ou outras medidas. A equipe jurídica deve estar preparada para negociar de forma estratégica e proteger os interesses da empresa.

Monitoramento do cumprimento: Após a resolução das questões legais, é fundamental que a empresa monitore o cumprimento das obrigações pela Noname. Isso pode incluir a implementação de políticas e procedimentos para garantir a conformidade com as leis e regulamentos aplicáveis. O monitoramento é importante para garantir que a empresa continue a operar dentro da lei e proteger seus interesses.

Medidas Jurídicas para identificar o ofensor

Medidas jurídicas para identificar o ofensor incluem investigação policial, ordens judiciais, interrogatórios, análise de evidências, identificação por testemunhas, monitoramento de atividades online e cooperação com outras agências e países.

1. Investigação policial: A polícia é geralmente responsável por investigar crimes e pode usar várias técnicas de investigação, como coleta de evidências, entrevistas com testemunhas.

2. Ordens judiciais: Um juiz pode emitir ordens judiciais, como mandados de busca e apreensão, que permitem às autoridades buscar e apreender evidências ou monitorar atividades de comunicação para identificar o ofensor.

3. Interrogatórios e depoimentos: Através de interrogatórios, o acusado pode ser questionado a fim de obter informações sobre seu envolvimento no crime.

4. Análise de evidências: A análise de evidências coletadas na cena do crime, como impressões digitais, DNA, pegadas, entre outros, pode ser usada para identificar o ofensor.

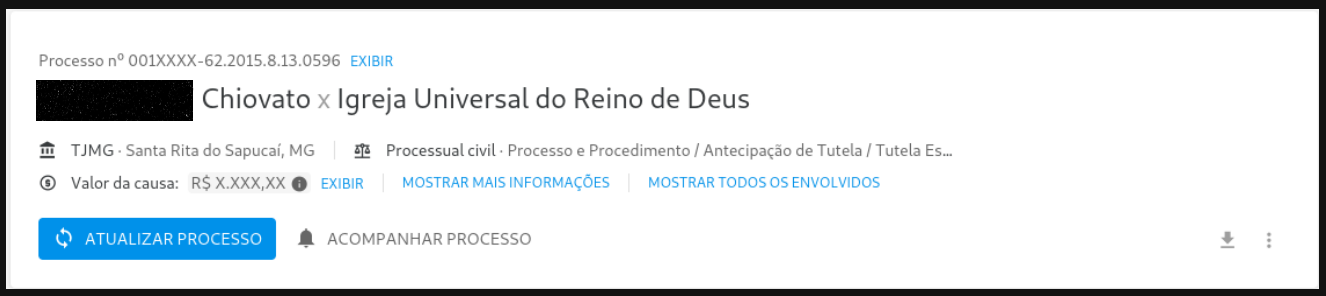
5. Identificação por testemunhas: Testemunhas oculares ou testemunhas que possam ter informações sobre a identidade do ofensor podem ser ouvidas em um tribunal e fornecer informações relevantes para sua identificação.

6. Monitoramento de atividades online: Em casos de crimes cibernéticos, as autoridades podem usar técnicas de monitoramento de atividades online, como rastreamento de endereços IP

7. Cooperação com outras agências e países: em casos que envolvam ações transnacionais, as autoridades podem cooperar com outras agências e países para obter informações e evidências para ajudar na solução do crime.

É importante ressaltar que a identificação do ofensor deve ser realizada dentro dos limites da lei, respeitando os direitos e garantias individuais do suspeito ou acusado, incluindo o direito ao devido processo legal, ao contraditório, à ampla defesa e à presunção de inocência até que se prove sua culpa.

Dúvidas?


Processo nº 001XXXX-62.2015.8.13.0596 EXIBIR
[redacted] Chiovato x Igreja Universal do Reino de Deus
TJMG · Santa Rita do Sapucaí, MG
Processual civil · Processo e Procedimento / Antecipação de Tutela / Tutela Es...
Valor da causa: R$ X.XXX,XX EXIBIR
MOSTRAR MAIS INFORMAÇÕES
MOSTRAR TODOS OS ENVOLVIDOS
ATUALIZAR PROCESSO
ACOMPANHAR PROCESSO