SOC TIPS
CYBERSECURITY

Guia de Resposta a Incidentes de Segurança para LGPD

Um Framework Passo a Passo

Denny Roger
SOC Builder

SOC TIPS
CYBERSECURITY

Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece um novo padrão para a proteção de dados no Brasil, exigindo que as organizações adotem medidas eficazes para proteger as informações pessoais e garantir a privacidade dos usuários.

Diante disso, é fundamental que as empresas desenvolvam um plano robusto de resposta a incidentes de segurança que esteja em conformidade com a LGPD. Este guia apresenta um framework passo a passo que orienta as organizações sobre como alinhar suas atividades de resposta a incidentes com os requisitos da LGPD.

SOC TIPS
CYBERSECURITY

PASSO 1: PREPARAÇÃO E CONSCIENTIZAÇÃO

Abril 2024

Objetivo: Estabelecer uma base sólida de conhecimento e recursos para lidar com incidentes de segurança.

- **Formação de Equipe:** Crie uma equipe de resposta a incidentes composta por membros de diferentes departamentos, incluindo TI, jurídico e comunicação.
- **Treinamento e Conscientização:** Realize treinamentos regulares sobre a LGPD e procedimentos de resposta a incidentes para todos os funcionários.
- **Ferramentas e Recursos:** Adquira e configure ferramentas de detecção e resposta a incidentes. Certifique-se de que elas estão aptas a identificar e mitigar rapidamente ameaças.

PASSO 2: IDENTIFICAÇÃO DO INCIDENTE

Objetivo: Detectar e identificar incidentes de segurança de maneira eficiente.

- **Monitoramento Contínuo**: Utilize sistemas de monitoramento para detectar atividades anormais que possam indicar um incidente.

- **Alertas de Segurança**: Implemente um sistema de alertas para notificar a equipe de resposta a incidentes assim que uma possível violação for detectada.

SOC TIPS
CYBERSECURITY

PASSO 3: AVALIAÇÃO DO IMPACTO

Objetivo: Avaliar a extensão e o impacto do incidente sobre os dados protegidos pela LGPD.

- **Classificação de Dados:** Identifique quais dados foram afetados e determine sua classificação conforme a LGPD (por exemplo, dados sensíveis).

- **Avaliação Legal:** Trabalhe com o departamento jurídico para entender as implicações legais do incidente.

Para avaliar a extensão e o impacto de um incidente de segurança sobre os dados protegidos pela LGPD de maneira eficaz, é crucial fazer as perguntas certas.

Aqui estão algumas questões detalhadas que podem ser usadas para orientar a análise durante os processos de Classificação de Dados e Avaliação Legal.

SOC TIPS CYBERSECURITY

1 Classificação de Dados

- **Quais tipos de dados foram afetados?**
- Identifique se os dados envolvem informações pessoais, dados sensíveis (como dados de saúde, dados biometricos, etc.), ou dados anonimizados.
- **Qual é a quantidade de dados comprometidos?**
- Determine se a violação afetou grandes volumes de dados ou se foi limitada a uma pequena quantidade de registros.
- **Os dados afetados estão atualizados ou são obsoletos?**
- Avalie se os dados comprometidos são recentes ou desatualizados, o que pode influenciar o impacto sobre os indivíduos.
- **Existem dados de menores de idade ou de outros grupos vulneráveis envolvidos?**
- Verifique se os dados incluem informações sobre menores ou outros grupos que requerem proteções adicionais.
- **Os dados afetados estavam criptografados ou de alguma forma protegidos?**
- Analise se medidas de segurança como criptografia foram comprometidas ou se ainda oferecem proteção aos dados.

Aqui estão algumas questões detalhadas que podem ser usadas para orientar a análise durante os processos de Classificação de Dados e Avaliação Legal.

SOC TIPS CYBERSECURITY

2 Avaliação Legal

1. **O incidente configura uma violação de dados pessoais segundo a LGPD?**
   - Determine se o incidente envolve uma violação de segurança que resulta na destruição, perda, alteração, divulgação ou acesso não autorizado a dados pessoais.
2. **Quais são as obrigações legais imediatas após a identificação do incidente?**
   - Identifique as necessidades de notificação tanto para a Autoridade Nacional de Proteção de Dados (ANPD) quanto para os titulares dos dados.
3. **Existem requisitos específicos de notificação em função do tipo ou do volume de dados afetados?**
   - Verifique se o volume ou o tipo de dado afetado implica obrigações específicas de notificação ou outras ações legais.
4. **Quais são as potenciais consequências legais ou sanções associadas ao incidente?**
   - Avalie as possíveis multas, sanções e outras repercussões legais que podem ser aplicadas em decorrência do incidente.
5. **Há necessidade de envolvimento de outras autoridades ou órgãos regulatórios?**
   - Considere se o incidente requer o envolvimento de outras entidades reguladoras.

PASSO 4: CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Objetivo: Minimizar os danos, remover a ameaça e restaurar os serviços.

- **Contenção Imediata:** Implemente medidas para limitar a extensão do incidente.
- **Erradicação da Ameaça:** Elimine a fonte do incidente e quaisquer componentes maliciosos no sistema.
- **Recuperação:** Restaure os sistemas e dados afetados a partir de backups seguros.

SOC TIPS
CYBERSECURITY

PASSO 5: NOTIFICAÇÃO DE INCIDENTES

Objetivo: Cumprir com as obrigações de notificação da LGPD.

- **Determinação da Necessidade de Notificação:** Avalie se o incidente requer notificação às autoridades e aos titulares dos dados.
- **Comunicação Eficaz:** Prepare e envie notificações que sejam claras e informativas, respeitando os prazos legais.

SOC TIPS CYBERSECURITY

PASSO 6: AVALIAÇÃO PÓS-INCIDENTE E MELHORIA CONTÍNUA

Abril 2024

Objetivo: Aprender com o incidente e melhorar os processos de segurança.

- **Análise Pós-Incidente:** Conduza uma análise detalhada para entender as causas do incidente e avaliar a resposta dada.
- **Atualização de Políticas e Procedimentos:** Atualize políticas e procedimentos com base nas lições aprendidas.
- **Melhoria Contínua:** Implemente mudanças para fortalecer a segurança e a conformidade com a LGPD.

SOC TIPS
CYBERSECURITY

BENEFÍCIOS DO FRAMEWORK DE RESPOSTA A INCIDENTES DE SEGURANÇA CONFORME A LGPD

1. Conformidade Regulatória

- Cumprimento da Legislação: O framework garante que as organizações estejam em conformidade com a LGPD, evitando penalidades e sanções.
- Melhor Gestão de Obrigações Legais: Facilita a identificação e o cumprimento das obrigações legais, como notificações a tempo e a maneira correta para a ANPD e os titulares dos dados.

2. Gestão de Riscos Aperfeiçoada

- Minimização de Danos: Permite uma resposta rápida e eficiente a incidentes, minimizando os danos financeiros e de reputação.
- Redução de Vulnerabilidades: A análise pós-incidente ajuda a identificar e corrigir vulnerabilidades, reduzindo a probabilidade de futuras violações.

3. Fortalecimento da Segurança dos Dados

- Proteção de Informações Sensíveis: Implementação de práticas robustas de segurança para proteger dados contra acessos não autorizados e perdas.
- Confiança dos Usuários: Aumenta a confiança dos clientes e parceiros na capacidade da organização de proteger seus dados.

4. Resiliência Organizacional

- Capacidade de Recuperação: Melhora a capacidade de recuperação da organização após um incidente, garantindo a continuidade dos negócios.
- Adaptação e Flexibilidade: O framework fornece uma base que pode ser adaptada conforme novas tecnologias e ameaças emergem.

5. Alinhamento Estratégico

- Suporte à Estratégia de Negócios: A proteção eficaz de dados pessoais suporta a estratégia de negócios e promove uma cultura organizacional de segurança e privacidade.

SOC TIPS
CYBERSECURITY

DENNY ROGER

FOUNDER & SOC BUILDER

+ de 55.000 ativos protegidos e monitorados, + de 21.000 usuários protegidos e + de 3 milhões ataques cibernéticos detectados e contidos em 2023.

- Carreira desenvolvida em instituições financeiras e consultorias como Santander, Telefónica, Accenture e EY.
- Atuou como mentor dos alunos do curso de Defesa Cibernética da FIAP
- Foi Presidente da Associação Brasileira de Segurança da Informação.
- + 11 certificações internacionais em Coaching e PNL, incluindo:
  - PLCC - Professional Leader Coach Certification
  - PECC - Professional Executive Coaching
  - PBCC - Professional Business Coaching Certification

SOC TIPS
CYBERSECURITY

Somos "SOC Builders" e mentores de carreira na área de segurança cibernética

@soctips
www.linkedin.com/company/soctips/
www.linkedin.com/in/dennyroger/