Modelo de Plano de Resposta a Incidentes para Empresa XYW

1. Introdução

1.1 Objetivo do Plano:

Este Plano de Resposta a Incidentes foi desenvolvido pela Empresa XYW para estabelecer diretrizes e procedimentos para lidar com incidentes de segurança de dados. O objetivo é proteger os dados pessoais dos titulares, garantir conformidade com a LGPD e responder eficazmente a situações de emergência.

1.2 Escopo:

Este plano abrange todos os sistemas, redes e dados da Empresa XYW que contenham informações pessoais dos titulares. Ele se aplica a todos os funcionários, contratados e terceiros que tenham acesso aos dados da empresa.

2. Equipe de Resposta a Incidentes (IRT)

2.1 Membros da Equipe:

A Equipe de Resposta a Incidentes (IRT) da Empresa XYW é composta pelos seguintes membros:

- Encarregado de Proteção de Dados (DPO): João Silva
- Diretor de TI: Maria Santos
- Especialista em Segurança da Informação: Pedro Oliveira
- Especialista em Segurança Física: José Sergio
- Representante Jurídico: Ana Costa
- Responsável pelo Comunicação: Luísa Pereira

2.2 Responsabilidades:

- DPO: Coordenar a resposta a incidentes, garantir a conformidade com a LGPD e notificar as autoridades competentes.
- Diretor de TI: Supervisionar a contenção e recuperação de sistemas afetados.
- Especialista em Segurança da Informação: Conduzir a investigação forense e análise de incidentes.
- Especialista em Segurança Física: Conduzir medidas de segurança física.
- Representante Jurídico: Avaliar as implicações legais dos incidentes e coordenar a comunicação externa.
- Responsável pelo Comunicação: Preparar comunicados de imprensa, avisos públicos e atualizações para os clientes.

3. Procedimentos de Resposta a Incidentes

3.1 Detecção e Classificação:

- Monitoramento Contínuo: Utilizar ferramentas de monitoramento de rede, análise de logs e detecção de intrusão para identificar atividades suspeitas.
- Classificação de Incidentes: Classificar os incidentes de acordo com sua gravidade e impacto nos dados e operações da empresa.

3.2 Notificação Interna e Acionamento da Equipe:

- Acionamento da Equipe: Em caso de incidente identificado, o funcionário responsável deve imediatamente notificar o DPO ou a equipe de resposta a incidentes.
- Registro do Incidente: O incidente deve ser registrado em um registro de incidentes, incluindo detalhes como data, hora, tipo de incidente e sistemas afetados.

3.3 Contenção e Isolamento:

- Isolamento de Sistemas: Suspender o acesso aos sistemas afetados e isolar as áreas comprometidas para evitar a propagação do incidente.
- Coleta de Evidências: Preservar e coletar evidências digitais relevantes para a investigação forense.

3.4 Investigação e Análise Forense:

- Análise Detalhada: Realizar uma investigação forense para determinar as causas do incidente, métodos de invasão, dados afetados e impacto nos negócios.
- Documentação de Resultados: Registrar todas as descobertas da investigação em um relatório detalhado.

3.5 Comunicação Externa e Notificação:

- Notificação à ANPD: Em casos que possam resultar em risco ou dano relevante aos titulares, notificar a ANPD conforme exigido pela LGPD.
- Notificação aos Titulares: Notificar os titulares dos dados afetados sobre o incidente, seus dados comprometidos e as medidas de proteção disponíveis.

3.6 Recuperação e Resposta:

- Restauração de Serviços: Implementar planos de recuperação para restaurar sistemas afetados e garantir a continuidade dos serviços.
- Revisão de Políticas e Procedimentos: Identificar e corrigir as vulnerabilidades que permitiram o incidente, atualizando políticas de segurança e procedimentos operacionais.

4. Treinamento e Conscientização

4.1 Treinamento da Equipe:

Treinamento Regular: Fornecer treinamento contínuo para todos os funcionários sobre segurança da informação, políticas de proteção de dados e procedimentos de resposta a incidentes.

4.2 Conscientização dos Funcionários:

Campanhas de Sensibilização: Realizar campanhas regulares para aumentar a conscientização sobre a importância da segurança da informação e a responsabilidade de cada funcionário na proteção dos dados.

5. Revisão e Melhoria Contínua

5.1 Exercícios de Simulação:

Realizar exercícios de simulação regulares para testar a eficácia do plano de resposta a incidentes e a preparação da equipe.

5.2 Revisão e Atualização do Plano:

- Revisão Periódica: Revisar o plano regularmente para garantir sua eficácia e conformidade com as mudanças nas leis, regulamentos e ambientes de ameaças.
- Incorporação de Lições Aprendidas: Incorporar as lições aprendidas de incidentes anteriores para melhorar as práticas de segurança e resposta a incidentes.

Este Plano de Resposta a Incidentes da Empresa XYW foi elaborado para garantir uma resposta rápida, organizada e eficaz a incidentes de segurança de dados, protegendo assim os dados pessoais dos titulares, mantendo a conformidade com a LGPD e preservando a reputação e confiança da empresa. Este documento é um guia vivo e será revisado regularmente para garantir sua relevância e eficácia contínuas.

Assinaturas:

[Assinatura do Encarregado de Proteção de Dados (DPO)]

[Assinatura do Diretor de TI]

[Assinatura do Especialista em Segurança da Informação]

[Assinatura do Especialista em Segurança Física]

[Assinatura do Representante Jurídico]

[Assinatura do Responsável pelo Comunicação]

Data de Revisão: [Data da última revisão]