PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

1. INTRODUÇÃO

Este Plano de Resposta a Incidentes de Segurança da Informação Envolvendo Dados Pessoais ("Plano de Resposta a Incidente" ou "PRI") estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável ("Dados Pessoais") que são tratados pela **Funerária Diersmann Ltda.** ("Empresa"), visando o combate dos riscos e a minimização de eventuais efeitos relacionados a incidentes desta natureza.

O presente PRI foi elaborado de acordo com a Lei 13.709/18 ("Lei Geral de Proteção de Dados Pessoais").

2. OBJETIVO

Este PRI tem como objetivo estabelecer as funções e responsabilidades das equipes da Empresa, bem como as medidas a serem tomadas por essas equipes para que a Empresa responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas, proteção de todas e quaisquer informações que possam viabilizar, direta ou indiretamente, a identificação de uma pessoa física ("Dados Pessoais") e privacidade dos seus titulares, possibilitando à Empresa manter a confiabilidade de suas marcas, produtos e serviços. Também estão compreendidas dentro do conceito de Dados Pessoais todas as informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informações referentes à saúde ou à vida sexual, dados genéticos ou biométricos e quaisquer dados que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza ("Dados Sensíveis").

O presente PRI se aplica em qualquer caso de incidentes envolvendo Dados Pessoais e deverá ser cumprida, em conjunto com as demais políticas da Empresa, por todas as áreas e colaboradores da Empresa, incluindo, sem limitação, os sócios, diretores, administradores, empregados e determinados prestadores de serviços e parceiros("Colaboradores") que, no âmbito das suas relações com a Empresa, possam vir a ter acesso às áreas, equipamentos, informações, redes e aos arquivos e dados de propriedade da Empresa.

Aplicam-se a este PRI, de forma complementar, as disposições da Política de Segurança da Informação, a fim de mitigar a ocorrência de incidentes de segurança da informação.

3. O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS?

Para fins do presente PRI, entende-se por "Incidente" toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje, ou seja, capaz de dar ensejo à destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizados a Dados Pessoais tratados pela Empresa.

Um Incidente pode ocorrer de forma maliciosa, ser o resultado de um erro humano ou, até mesmo, de falha nos sistemas que processam Dados Pessoais ou nos seus mecanismos de segurança. Isso pode incluir por exemplo, o furto de um documento, o envio de um e-mail contendo Dados Pessoais para destinatários indesejados, tentativas de invasão a sistemas da Empresa ou outras ações, culposas ou dolosas.

Os Incidentes podem ser de vários tipos, como por exemplo:

1. **Vazamento de Dados Pessoais.** É o Incidente no qual Dados Pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país;

2. **Negação de Serviço.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que armazene Dados Pessoais é prejudicado ou impossibilitado, de forma que a integridade dos Dados Pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso;

3. **Acesso Não Autorizado.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que possua Dados Pessoais é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida; e

4. **Uso Inapropriado.** É o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da Empresa, incluindo a Política de Privacidade e de Segurança da Informação.

4. PAPÉIS E RESPONSABILIDADES

Cada área da Empresa, sejam as áreas diretamente envolvidas na governança da Empresa ou não, tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descritas a seguir:

4.1. Obrigações de Todas as Áreas

1. comunicar imediatamente a Equipe de Resposta (conforme descrito abaixo), sobre a ocorrência ou a mera suspeita de um Incidente;

2. cumprir rigorosamente a Política de Segurança da Informação da Empresa, contribuindo para a mitigação de riscos; e

3. participar de treinamentos e programas de conscientização para mitigação de Incidentes.

4.2. Obrigações da Equipe de Resposta

A Equipe de Resposta a Incidentes da Empresa é o grupo de Colaboradores designado abaixo para atuar nas respostas a Incidentes:

Área/Departamento	Pessoa Responsável
TI	André Schossler
Pessoal	Francine Müller
Administrativo	Diana Joris

Financeiro	Jônatas Daroit
Gerencial	Régis Diersmann

Entre suas principais responsabilidades, destacamos:

1. atuar para detectar e corrigir os Incidentes;

2. alertar, comunicar e aconselhar os Colaboradores sobre Incidentes emergentes;

3. educar e conscientizar os Colaboradores sobre a detecção e resposta aos Incidentes; e

4. adotar demais medidas necessárias para prevenir Incidentes e minimizar o impacto de seus efeitos.

4.3. Obrigações de Outras Áreas

A Equipe de Resposta poderá acionar outros Colaboradores de outras áreas, dependendo do tipo e da gravidade do incidente. Neste caso, segue abaixo lista de áreas que podem ser envolvidas e suas responsabilidades ("Áreas Envolvidas"):

1. **Comitê de Proteção de Dados.** É a principal instância decisória sobre o tratamento de Dados Pessoais. Responde diretamente à Diretoria;

2. **Tecnologia e Sistemas da Informação.** Auxilia na resolução das questões técnicas relacionadas ao Incidente e na investigação da origem e das razões para ocorrência do Incidente;

3. **Jurídico.** Avalia a situação decorrente do Incidente e toma as medidas apropriadas quanto aos impactos jurídicos à Empresa ou a Colaboradores, clientes, parceiros comerciais ou titulares dos Dados Pessoais afetados;

4. **Relações Públicas.** Coordena as comunicações entre a Empresa e seus colaboradores, parceiros comerciais estratégicos, principais clientes, bem como o público em geral para mitigar eventuais riscos reputacionais e assegurar a continuidade dos negócios;

5. **Atendimento ao Consumidor.** Coordena a comunicação da Empresa com os seus clientes sobre o Incidente, incluindo o esclarecimento sobre o ocorrido e as ações tomadas para mitigar os efeitos e prevenir novos Incidentes semelhantes no futuro, sempre de acordo com as orientações das demais áreas; e

6. **Compliance.** Investiga as origens e as razões da ocorrência do Incidente, bem como avalia, junto aos gestores das áreas, a necessidade da aplicação de medidas disciplinares aos Colaboradores cujas condutas foram culposas ou intencionais na ocorrência de um Incidente.

5. DETECÇÃO DO INCIDENTE

Detectar um Incidente de forma rápida e eficiente é essencial para uma resolução bem-sucedida. São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma. Desta forma, **todos os Colaboradores** devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, *phishing*, *malware*, instabilidades sistêmicas etc.

Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, o Colaborador deverá comunicar imediatamente a Equipe de Resposta a Incidentes, por meio do e-mail [-], mantendo o seu supervisor sempre em cópia.

Na medida do possível, essa comunicação deverá conter (i) a hora e a data em que a suspeita do Incidente foi descoberta; (ii) o tipo de informações envolvidas; (iii) a causa e a extensão do Incidente; (iv) o contexto do ocorrido; bem como (v) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A COMUNICAÇÃO SOBRE A SUSPEITA DE UM INCIDENTE É VITAL PARA A EMPRESA. ASSIM, CASO O COLABORADOR SUSPEITE DE UM INCIDENTE E NÃO O COMUNIQUE, SANÇÕES DISCIPLINARES PODERÃO SER-LHE APLICADAS, A DEPENDER DA GRAVIDADE DO INCIDENTE E DA COMPROVAÇÃO DE EVENTUAL NEGLIGÊNCIA DO COLABORADOR.

5.1. Priorização do Incidente e Procedimentos para Resposta

Uma vez que o Incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à Empresa e aos titulares dos Dados Pessoais eventualmente afetados e a gravidade da ocorrência. O impacto do Incidente deve ser aferido da seguinte forma:

volume de Dados Pessoais expostos	Alto	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Médio	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Baixo	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**
		Baixa	Média	Alta
		sensibilidade dos Dados Pessoais afetados		

VOLUME DE DADOS PESSOAIS EXPOSTOS	
Criticidade	**Descrição**
Alto	volume de Dados Pessoais afetado superior a 10% da base de dados controlada pela Empresa

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS	
Criticidade	**Descrição**
Alta	Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito

Médio	volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados controlada pela Empresa
Baixo	volume de Dados Pessoais afetado inferior a 2% da base de dados controlada pela Empresa

Média	Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.)
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (e.g. IP)

De acordo com a matriz acima definida, a Equipe de Resposta a Incidentes deverá tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

1. tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente;

2. tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição da Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, conforme modelo anexo a este PRI; e

6. reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao Comitê de Proteção de Dados.

Média Gravidade

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

2. tomar as medidas imediatas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição para atender, com prioridade, a Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível, conforme modelo anexo a este PRI;

6. reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata documentada, que deverá ser apresentada ao Comitê de Proteção de Dados; e

7. realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os seus Colaboradores sobre o Incidente e medidas preventivas.

Alta Gravidade

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

2. imediatamente comunicar os diretores responsáveis pelas Áreas Envolvidas, os quais, em conjunto com outra pessoa de cada uma das respectivas Áreas Envolvidas, devem atuar de forma exclusiva no suporte à Equipe de Resposta e preferencialmente no mesmo local em que a Equipe de Resposta esteja trabalhando;

3. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, imediatamente, conforme modelo anexo a este PRI;

4. reunir-se, imediatamente, para avaliar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao Comitê de Proteção de Dados;

5. realizar, imediatamente, treinamento interno com todos os Colaboradores da Empresa para conscientizar sobre o Incidente e medidas preventivas; e

6. comunicar, imediatamente, os Colaboradores internos sobre medidas preventivas.

5.2. Comunicação do Incidente

Em cumprimento à legislação brasileira, Incidentes considerados relevantes devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD). A avaliação sobre quais Incidentes são materialmente relevantes cabe ao Comitê de Proteção de Dados, em conjunto com a Diretoria da Empresa.

Caso um Incidente seja identificado como relevante e a sua comunicação à ANPD seja determinada pelo Comitê de Proteção de Dados, o departamento Jurídico deverá, com suporte da Equipe de Resposta, elaborar a documentação aplicável à comunicação, contendo:

1. A descrição da natureza e da categoria dos Dados Pessoais afetados (ex. Dados sensíveis, dados de criança, dados cadastrais etc.);

2. As informações sobre os titulares dos Dados Pessoais envolvidos, a relação dos titulares dos Dados Pessoais afetados com a Empresa, o número de titulares afetados e o país de residência dos titulares dos Dados Pessoais afetados;

3. A indicação das medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais, observados os segredos comercial e industrial;

4. Os riscos relacionados ao Incidente;

5. Os motivos da demora, no caso de a comunicação não ter sido feita de forma imediata; e

6. As medidas que foram e as que serão adotadas para reverter ou mitigar os efeitos do Incidente.

Caso o Comitê de Proteção de Dados determine a comunicação sobre o Incidente aos titulares dos Dados Pessoais afetados, a área de [Relações Públicas, com suporte do Jurídico, do Atendimento ao Consumidor e da Equipe de Resposta], irá desenvolver a mensagem da comunicação, priorizando (i) os fatos ocorridos; (ii) as medidas já tomadas pela Empresa para minimizar o impacto dos efeitos; (iii) as eventuais medidas que possam ser tomadas pelos próprios titulares dos Dados Pessoais afetados para mitigar riscos; e (iv) os canais de contato para sanar dúvidas.

6. DISPOSIÇÕES FINAIS

Em caso de dúvidas, comentários e/ou sugestões relacionadas a este PRI, entre em contato com o DPO (encarregado) da Empresa, que está à disposição nos seguintes endereços de contato:

DPO (encarregado): André Luís Schossler