EDMOND

Um novo ciclo para ir além

Plano de Resposta a Incidente de Segurança em Dados Pessoais

SUMÁRIO

Objetivo

A **EDMOND SOLUÇÕES E TECNOLOGIA S.A**. (“Edmond” ou “Companhia”) realiza tratamento de dados pessoais como Operadora e como Controladora, nos termos da Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (“LGPD”), buscando atender à finalidade da prestação dos seus serviços, execução de contrato, para o cumprimento de obrigação legal ou regulatório e legítimo interesse do Controlador.

O plano de resposta a incidentes de segurança da informação indica como a Edmond irá proceder às situações de ameaça aos padrões e práticas de segurança que possam acarretar risco ou dano relevante aos titulares de dados.

A resposta da Edmond deve ser ágil e eficiente, resguardando evidências que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência.

EDMOND

01. Incidente de segurança da informação envolvendo dados pessoais

1 Incidente de segurança da informação envolvendo dados pessoais

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 acesso não autorizado a Dados Pessoais tratados pela Edmond. Os Incidentes podem ser de vários tipos, como por exemplo:

1. **Vazamento de Dados Pessoais:** Incidente no qual Dados Pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais;

2. **Negação de Serviço:** 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;

3. **Acesso Não Autorizado:** 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;

4. **Uso Inapropriado:** Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da Edmond.

EDMOND

02. Papéis e Responsabilidades

2 Papéis e Responsabilidades

Encarregado: O Encarregado pelo Tratamento de Dados Pessoais (DPO) terá seus canais de comunicação divulgados ao público, através da Política de Privacidade, e será também o responsável por monitorar/receber os avisos de incidentes de segurança. Ele também é o responsável por documentar as atividades da equipe, especialmente as tarefas de identificação e resolução do incidente. Por fim, o Encarregado também será o Comunicador/Notificador e fará parte do Comitê de Gestão de Crise, quando o incidente envolver dados pessoais.

Comitê de Gestão de Crise: Grupo de colaboradores designados pelo (a) Diretor (a) Presidente. Fazem parte do Comitê de Gestão de Crise, necessariamente, Diretor Comercial, o Head de Tecnologia, Head Operações e Compliance, podendo ainda fazer parte outros integrantes da Gerência de Tecnologia da Informação. O Encarregado fará parte da Comissão de Gestão de Crise quando o incidente envolver dados pessoais.

Comunicador/Notificador: pessoa responsável por notificar o incidente aos órgãos reguladores.

Head responsável/CTO: responsável pela Política de Segurança da Informação e Cibernética e pela coleta e análise de todas as evidências do incidente. Determina a causa raiz, direciona os outros analistas de segurança e coordena a recuperação rápida dos sistemas e serviços;

EDMOND

03. Identificação do Incidente e Avaliação

3 Identificação do Incidente e Avaliação

A suspeita de incidente de segurança da informação deverá ser reportada ao Encarregado via e-mail privacidade@edmond.com.br da forma mais ágil possível.

O **Comitê de Gestão de Crise**, em conjunto com o Head Jurídico, avaliará se o incidente reportado pode acarretar risco ou dano à Edmond, aos seus clientes ou aos titulares de dados pessoais, a extensão do risco e do potencial dano, através da análise e verificação da natureza e origem do incidente, se ocorreu via vazamento de dados ou divulgação indevida de dados, online ou offline. A criticidade do incidente poderá ser definida com as seguintes classificações:

O **Comitê de Gestão de Crise** avaliará os potenciais impactos e a urgência da resolução do incidente, elabora plano de ação e solicita atuação imediata do Departamento de Tecnologia da Informação.

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 da Controladora.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Controladora.
Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, dados Pessoais sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais identificáveis (ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (ex.: histórico de atividades, preferências).
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

EDMOND

04. Resolução e medidas adotadas para diminuição de danos e riscos

4 Resolução e medidas adotadas para diminuição de dados e riscos

O Head responsável procura identificar a causa do incidente (que podem ser serviços expostos na internet ou, acessos e e-mails de criminosos digitais, por exemplo), endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, buscando soluções técnicas; identifica sistema afetado e inicia medidas de contenção a fim de isolar o sistema afetado e diminuir os danos ocasionados. Exemplos de medidas de contenção podem ser desligar o sistema ou suas funcionalidades, interromper acessos, alterar ou bloquear senhas, realizar backups, entre outros.

Os sistemas serão restaurados após solucionados os problemas, bem como os backups.

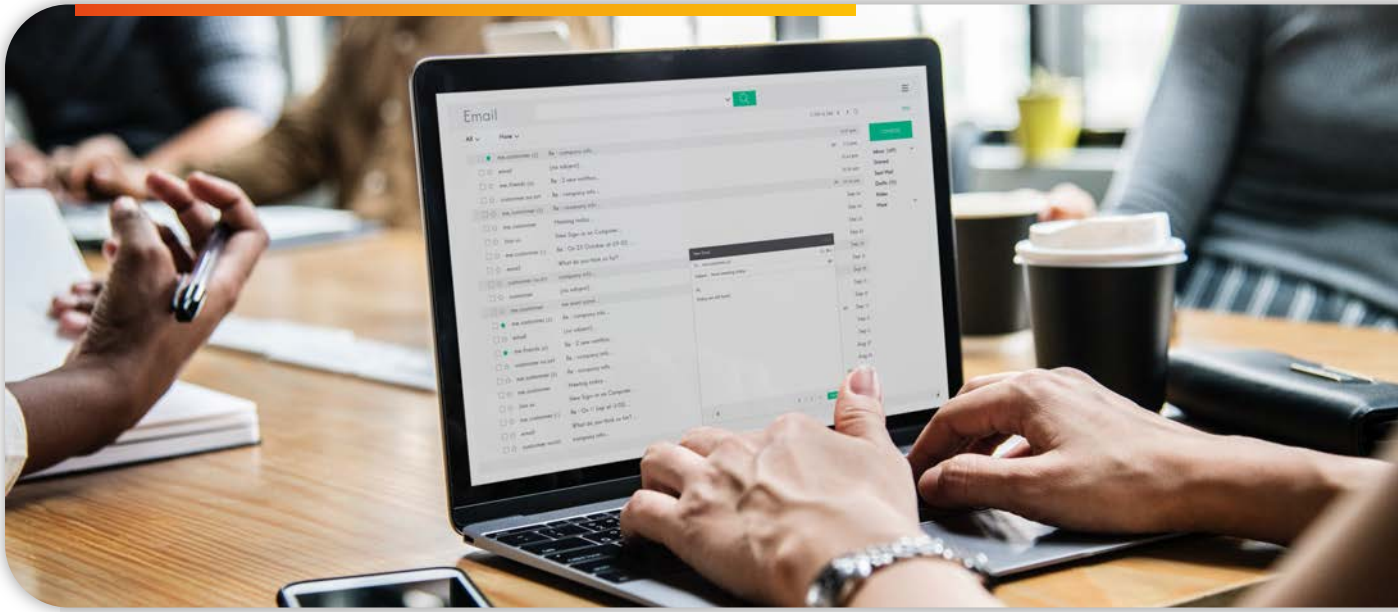
EDMOND

05. Documentação e Aprendizados

5 Documentação e Aprendizados

Após contido o incidente, o Comitê de Gestão de Crise fará reunião com o Departamento de Tecnologia da Informação, a fim de discutir os erros e falhas identificados e propor melhorias.

- *Informações do incidente;*
- *Classe do incidente (acesso não autorizado, vírus, uso não autorizado de dispositivo, malware, instalação de software não autorizado, entre outros);*
- *Ativo onde ocorreu o incidente (servidor web, banco de dados, dispositivo de colaborador, entre outros);*
- *Localização geográfica do incidente;*
- *Momento;*
- *Titulares de dados pessoais afetados, se houver;*
- *Dados relacionados ao incidente;*
- *Ações tomadas pela Edmond para resolução do incidente;*
- *Evidências coletadas e local onde as evidências do incidente estão armazenadas; e,*
- *Conclusões.*



Anualmente, a Edmond elaborará relatório anual, a ser enviado ao BCB, que deverá conter, dentre outros assuntos:

- *Resumo das implementações do plano de ação;*
- *Resumo dos resultados obtidos;*
- *Incidentes relevantes; e,*
- *Resultado dos testes de continuidade*

EDMOND

06. Notificações e Comunicações

6 Notificações e Comunicações

O Encarregado atua como canal de comunicação entre o controlador, os titulares dos dados, a Autoridade Nacional de Proteção de Dados (ANPD) e demais autoridades competentes.

O Encarregado, quando o incidente envolver dados pessoais, deverá comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, e o Diretor Responsável que compõe o Comitê de Gestão de Crise, deverá comunicar o incidente ao Banco Central do Brasil ("BCB"), respeitando os critérios definidos por esses, no prazo máximo de 72 (setenta e duas) horas da identificação do incidente. **Tal comunicação conterá, no mínimo:**

- *Descrição da natureza dos dados afetados;*
- *Informações sobre os titulares envolvidos;*
- *Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;*
- *Riscos relacionados ao incidente;*
- *Motivos da demora, no caso de a comunicação não ter sido imediata; e*
- *Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.*

EDMOND

07. Legislação Aplicável

- *Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018);*
- *Marco Civil da Internet, (Lei 12.965/2014);*
- *Resolução BCB nº 85, de 8 de abril de 2021.*

EDMOND

08. Considerações Finais

A segurança da informação deve ser entendida como parte fundamental da cultura interna da Edmond, ou seja, qualquer incidente de segurança será considerado e tratado como se fosse um agente atuando contra a ética e os bons costumes regidos pela instituição.

O presente documento deverá ser interpretado ao lado da Política de Segurança da Informação e Cyber da Edmond.

EDMOND

09. Vigência e Controle de Versões

Este Plano de Resposta a Incidentes de Segurança da Informações entra em vigor a partir da data de sua publicação e disponibilização e será periodicamente revisado e atualizado pelo Head responsável, com a frequência mínima de uma vez a cada 12 (doze) meses.

EDMOND

Um novo ciclo para ir além

Muito Obrigado!

company/edmond-tech

edmond.tech

edmond.tech

Edmond Soluções e Tecnologia S.A.

Av. Andrômeda, 885 - sala 2901 - Green Valley Alphaville

Barueri - SP - CEP - 06473-000

Tel.: + 55 11 5199-0983

Site: edmond.com.br

E-mail: contato@edmond.com.br