1. **Introdução**
	1. Este documento define as diretrizes para responder eventos ou incidentes de segurança que estejam impactando ou possam vir a impactar ativos/serviços de informação ou recursos computacionais da NOME DA EMPRESA.
2. **Propósito**
	1. Estabelecer diretrizes para garantir a resposta e tratamento adequados a incidentes de segurança da informação que possam impactar ativos/serviços de informação ou recursos computacionais da NOME DA EMPRESA.
3. **Escopo**
	1. Esta norma obedece ao escopo definido na Política Geral de Segurança da Informação.
4. **Diretrizes**
	1. **Incidentes de segurança da informação**
		1. Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação ou recursos computacionais da NOME DA EMPRESA serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados;
		2. Incidentes de segurança devem ser priorizados com base na criticidade dos ativos/serviços de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista;
		3. Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados a área de segurança da informação;
		4. A área de segurança da informação deverá determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas como, por exemplo, membros do time de resposta a incidentes de segurança da informação;
		5. Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente corporativo, de forma a garantir a contenção do incidente;
		6. A extensão dos danos do incidente de segurança deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados;
		7. Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.
	2. **Time de resposta a incidentes de segurança da informação**
		1. O time de resposta a incidentes de segurança da informação da NOME DA EMPRESA deverá ser composto por, no mínimo, representantes das seguintes áreas:
			1. Gerência de tecnologia da informação;
			2. Gerência de segurança da informação;
			3. Gerência de recursos humanos;
			4. Gerência de comunicações;
			5. Gerência jurídica.
		2. Conforme a natureza do incidente, colaboradores de qualquer setor da NOME DA EMPRESA podem ser convocados a participar do time de resposta a incidentes de segurança da informação.
	3. **Disseminação de informação sobre incidentes de segurança da informação**
		1. Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas a NOME DA EMPRESA sem aprovação expressa e formal da diretoria.
5. **Classificação de Tipos de Incidente**
	1. **Vazamento de Dados Pessoais**: É o Incidente no qual Dados Pessoais são indevidamente expostos e disponibilizados, para um número indeterminado de pessoas, no Brasil ou em qualquer país;
	2. **Negação de Serviço**: É o Incidente no qual o acesso a um sistema que armazene Dados 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 a um sistema que possua Dados 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.
6. **Priorização do Incidente e Procedimentos de Resposta**
	1. 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** | **Sensibilidade de dados pessoais afetados** |
| Gravidade | Descrição | Gravidade | Descrição |
| Alta | Volume de dados pessoais afetado superior a 10% da base de dados controlada pela empresa | 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 |
| Média | Volume de dados pessoais afetado inferior a 10% e superior 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 | Volume de dados pessoais afetado inferior a 2% da base de dados controlada pela empresa | 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) |

* 1. 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.
	2. **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, através de relatório técnico; 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.
		1. **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.
		2. **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, através de relatório técnico;
			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.
		3. DESCREVER PROCEDIMENTOS ESPECÍFICOS PARA OUTROS TIPOS DE INCIDENTES CONFORME AS PARTICULARIDADES DA SUA ESRUTURA
	3. Fluxo de resposta a incidentes



1. **Papéis e Responsabilidades**
	1. **GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO**
		1. É responsabilidade da GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO:
			1. Atuar como responsável por ocorrências e eventos de segurança e garantir a existência de recursos identificar, escalar, mitigar, conter, e erradicar incidentes de segurança, bem como ações efetivas para recuperar o estado anterior de ativos/serviços de informação ou recursos computacionais afetados pelo incidente;
			2. Comunicar prontamente o time de resposta a incidentes de segurança da informação da NOME DA EMPRESA sobre eventos e incidentes de segurança.
	2. **TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**
		1. É responsabilidade do TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO:
			1. Apoiar a equipe de segurança da informação no tratamento de ocorrências e incidentes de segurança da informação, fornecendo orientação e direcionamento estratégico dentro da área de especialidade de cada um dos participantes do time de resposta a incidentes de segurança da informação;
			2. Aconselhar a diretoria da NOME DA EMPRESA sobre quais informações sobre eventos e incidentes de segurança da informação podem ser divulgadas para públicos internos e externos.
	3. **COMUNICAÇÃO**
		1. É responsabilidade da GERÊNCIA DE COMUNICAÇÃO:
			1. Aprovar qualquer tipo de comunicação ou disseminação total ou parcial de informações sobre ocorrências e incidentes de segurança da informação para qualquer parte ou público a quem possa interessar.
2. **Sanções e Punições**
	1. Sanções e punições serão aplicadas conforme previsto na legislação vigente.
3. **Revisões**
	1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.
4. **Gestão da Norma**
	1. A norma **N-SI-001** é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da NOME DA EMPRESA.
	2. A presente norma foi aprovada no dia 27/01/2024

|  |  |  |
| --- | --- | --- |
|  |  |  |
| João da Silva – CTO |  | José dos Santos – CEO |