Plano de Comunicação de Incidentes

Plano de Comunicação de Incidentes

Tipo: Plano | PLNO-0004 | **Nº Revisão**: 2.0

Elaboração: SI | **Classificação**: Público

Sumário

1. Objetivo

O objetivo desse documento é ter um processo a ser seguido para a Comunicação entre a Plusoft e seus clientes sobre os incidentes.

O que comunicar: Descrição do Incidente

Quando comunicar: Assim que for identificado o incidente

Quem Comunicar: clientes envolvidos de acordo com a nossa base de dados cadastral

Quem será comunicado: contatos da base de dados cadastral

2. Diretrizes

O Regulamento de Comunicação de Incidentes de Segurança (Resolução n°15 de 2024 da ANPD) assegura responsabilidades e prestação de contas quanto a incidentes de segurança envolvendo dados visando os direitos dos titulares e possíveis prejuízos a interesses e direitos fundamentais dos titulares.

O RCIS prevê que a ANPD e o titular devem ser comunicados sobre incidentes de segurança que possam ocasionar risco relevante, que é definido de acordo com critérios específicos.

A Plusoft e suas associadas enquanto **OPERADORA** dos dados se compromete tanto com o registro adequado quanto a comunicação assertiva de incidentes de segurança aos seus Clientes, **CONTROLADORES** dos dados, que por sua vez tem a responsabilidade perante os **TITULARES** dos dados e à própria Agência Nacional de Proteção de Dados.

A Plusoft e suas associadas são controladoras dos dados de seus colaborares e ex-colaboradores, por isso, a comunicação de incidente envolvendo dados de **Departamento Pessoal e Human Experience** (Recursos Humanos), fazendo uso de linguagem simples e de fácil entendimento e sempre de forma direta e individualizada e devem anexar ao processo de comunicação a ANPD uma declaração de comunicação ao titulares.

A ANPD publica orientações com o objetivo de auxiliar os agentes de tratamento na avaliação do incidentes.

3. Critérios para Comunicação de Incidente de Segurança

Um incidentes pode acarretar risco ou dano relevante aos titulares quando puder afetar e significativamente interesses e direitos fundamentais e CUMULATIVAMENTE envolver pelo menos **um** dos seguintes critérios:

- dados pessoais sensíveis;
- dados de crianças, de adolescentes ou de idosos;
- dados financeiros;
- dados de autenticação em sistemas;

- dados protegidos por sigilo legal, judicial ou profissional;
- dados em larga escala

Um incidente passa a afetar significativamente interesses e direitos quanto, entre outras situações, a atividade de tratamento impede o exercício de direito ou utilização de um serviço; ocasiona danos materiais ou morais (discriminação, violação à integridade física, direito de imagem e à reputação, fraudes financeiras ou roubo de identidade.

Considera-se incidente com dados em larga escala quando abrange um número significativo de titulares. Considera-se também o volume de dados envolvidos, a duração, a frequência e a extensão geográfica de localização dos titulares.

---

4. Prazos

O Controlador dos dados tem 3 dias úteis para avisar os titulares e a ANPD. A Plusoft, quando na posição de Operadora, deve comunicar os controladores o mais rápido possível.

---

5. Canal da comunicação

Na posição de Operador: comunicação via email para os Controladores ou Clientes.

Na posição de Controlador: via Formulário no site da ANPD. Neste caso, o DPO deve estar munido de documento comprobatório de vínculo com o Controlador.

Não havendo possibilidade de comunicação individualizada, enquanto na posição de Controlador, a comunicação deve ser realizada por meio dos canais disponíveis como sites, aplicativos, mídias sociais, juntamente com a disponibilização de canais de atendimento aos titulares, disponível por pelo menos 3 meses, de forma a garantir conhecimento amplo.

---

6. Processo de comunicação a clientes controladores

A comunicação deverá conter as seguintes informações:

6.1 Detecção do incidente

> Tipo de Incidente: Integridade, disponibilidade, confidencialidade
> Natureza do Incidente: perda, roubo, cópia, vazamento.
> Categoria de dados envolvidos: pessoais, dados de atendimento. logs, dados sensíveis.
> Número de Titulares afetados, discriminando, se houver, o número de crianças, adolescentes e idosos.
> Medidas técnicas e de segurança utilizadas para proteção e adotadas antes do incidente.
> Riscos relacionados e identificação de possíveis impactos
> Motivo da demora na comunicação, se houve demora significativa.
> Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente
> Data e Hora da ocorrência: DD/MM/AAAA HH:MM
> Duração do incidente: HH:MM
> Contato do DPO e identificação por nome do responsável e do suplente.
> Descrição do Incidente, incluindo sua causa, se possível determinar.
> Volume total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.
> Estagio do Incidente: Identificado, Em Investigação, Monitorado, Resolvido
> Tempo até a próxima atualização:
> Prazo estimado para estabilização:

6.2 Encerramento do incidente

> Data e Horário da Estabilização
> Medidas técnicas e de segurança utilizadas para proteção e adotadas após o incidente, guardando segredos comerciais.
> Medidas que serão adotadas para reverter ou mitigar os efeitos do incidente
> Análise da causa raiz:

Se não tiver ainda a Análise final, será enviada uma breve descrição e depois será enviado um outro e-mail com o Detalhamento final.

---

7. Processo de comunicação a titulares

A comunicação deve fazer uso de linguagem simples e de fácil entendimento, de forma direta e individualizada, com as seguintes informações:

7.1 Detecção do incidente

> Tipo de Incidente: Integridade, disponibilidade, confidencialidade
> Natureza do Incidente: perda, roubo, cópia, vazamento.
> Categoria de dados envolvidos: pessoais, dados de atendimento. logs, dados sensíveis.
> Número de Titulares afetados, discriminando, se houver, o número de crianças, adolescentes e idosos.
> Medidas técnicas e de segurança utilizadas para proteção e adotadas antes do incidente.
> Riscos relacionados e identificação de possíveis impactos
> Motivo da demora na comunicação, se houve demora significativa.
> Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente
> Recomendações aptas a reverter ou mitigar os efeitos do incidente a serem tomadas pelo titular
> Data e Hora da ocorrência: DD/MM/AAAA HH:MM
> Duração do incidente: HH:MM
> Contato do DPO.

7.2 Encerramento do incidente

> Data e Horário da Estabilização
> Medidas técnicas e de segurança utilizadas para proteção e adotadas após o incidente, guardando segredos comerciais.
> Medidas que serão adotadas para reverter ou mitigar os efeitos do incidente
> Análise da causa raiz:

---

4. Histórico de revisões

Versão	Data	Autor	Comentários
1.0	10/09/2021	[redacted]	Criação do Documento
1.1	20/09/2021		Inclusão de Informações no item Objetivo.
1.2	21/09/2021		Revisão layout, ajuste de índice e numeração de tópicos
1.3	11/10/2022		Revisão 2022 e adequação as diretrizes da ANPD
1.4	27/02/2023		Adequação da origem dos dados de contato
1.5	25/09/2023		Revisão ISO 27001/2022
1.6	29/09/2023		Aprovação 2023
1.7	16/07/2024		Adequação a RCIS (Resolução n°15 de 2024 da ANPD)
1.8	27/08/2024		Adicionada a necessidade do DPO e Suplente estarem identificados.
1.9	11/09/2025		Revisão do documento.
2.0	03/10/2025	Comitê de SI	Aprovação 2025