Plano de Gestão de Incidentes de Segurança da Informação e Privacidade

Versão 1.0
(Aprovado em reunião da ETIR-UFJ em 23/03/2026)

INTRODUÇÃO

O processo de tratamento de incidentes de segurança da informação e de privacidade consiste na implementação de procedimentos e etapas bem definidas que orientem as equipes na resolução de um incidente. Esse conjunto de etapas permite estabelecer um fluxo lógico, especificando as ações a serem executadas em cada fase do processo.

Este documento serve como referência específica para a resposta a incidentes de segurança e de privacidade, inclusive aqueles envolvendo dados pessoais. Assim, o plano descreve o processo para responder a situações de emergência, ou eventos de risco, que possam ocasionar impactos sobre os ativos de informação mantidos pela Universidade Federal de Jataí (UFJ).

Dessa forma, o documento destaca os passos necessários para uma resposta ágil e consistente, em conformidade com as exigências legais de comunicação e transparência relacionadas à segurança da informação e à proteção de dados pessoais.

Este Plano foi elaborado, inicialmente, pelo Encarregado pelo Tratamento de Dados Pessoais, alocado na Diretoria de Governança e Conformidade (**DGC**) da

Pró-Reitoria de Planejamento e Orçamento (**PROPLAN**) em parceria com a Secretaria de Tecnologia da Informação (**SeTI**). Além disso, passou por análise e validação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (**ETIR/UFJ**).

OBJETIVOS E ABRANGÊNCIA

O Plano de Gestão de Incidentes da Segurança da Informação e Privacidade (**PGISIP**) estabelece princípios, conceitos, diretrizes e responsabilidades sobre a gestão de incidentes de segurança da informação e privacidade na UFJ, orientando o funcionamento do processo, de forma que este seja tratado adequadamente, reduzindo ao máximo os impactos para o negócio.

Este plano tem como principais objetivos:

- Orientar a UFJ e a comunidade acadêmica nas respostas a incidentes que envolvam os ativos de Tecnologia da Informação (TI) da instituição, de forma documentada, formalizada e confiável, preservando evidências que possam ajudar a prevenir novos incidentes.;
- Dar transparência ao fluxo de procedimentos adotados e aos responsáveis pela atuação em caso de incidentes.;
- Desenvolver uma base de conhecimento institucional com fundamento nas lições aprendidas em cada ocorrência.

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pela UFJ. Para mais informações, consultar a Política de Segurança da Informação e Comunicação (POSIC) da UFJ.

CONCEITOS E DEFINIÇÕES

Segurança da Informação

Ataque: Evento ou conjunto de ações deliberadas, conduzidas por um agente interno ou externo, que exploram vulnerabilidades e fragilidades de controles de segurança da informação, com o objetivo de comprometer a confidencialidade, a integridade e/ou a disponibilidade dos ativos de informação, podendo resultar em acesso não autorizado, alteração, destruição ou indisponibilidade de informações e serviços.

Bot: Software malicioso que compromete um ativo de informação, permitindo seu controle remoto não autorizado por um agente de ameaça, geralmente para a execução coordenada de ataques ou outras atividades ilícitas.

GMT: Greenwich Mean Time (Horário Médio de Greenwich), baseado no meridiano de referência que passa pelo Observatório Real de Greenwich, próximo a Londres.

IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede ou na Internet.

Log: Registro estruturado de eventos relevantes em um sistema computacional, utilizado para auditoria, rastreabilidade e investigação de incidentes.

Porta: Identificador lógico associado a um programa ou processo específico, que atua como ponto final de comunicação em um sistema operacional hospedeiro.

Script: Conjunto de instruções executadas por um aplicativo, serviço ou interpretador, com o objetivo de automatizar tarefas ou processos.

SLA: Acordo de Nível de Serviço (Service Level Agreement), que define níveis mínimos de qualidade, disponibilidade e resposta de um serviço.

Spam: Mensagens eletrônicas não solicitadas, geralmente enviadas em massa, frequentemente com conteúdo publicitário ou fraudulento.

Spyware: Programa projetado para monitorar atividades de um sistema e enviar as informações coletadas para terceiros, sem o conhecimento ou consentimento do usuário.

Trojan (cavalo de troia): Programa que aparenta ter uma função legítima, mas executa também funções ocultas, normalmente maliciosas, sem o conhecimento do usuário.

Vírus: Código malicioso que se propaga ao inserir cópias de si mesmo em outros programas ou arquivos, dependendo da interação do usuário, com potencial de causar danos à integridade e à disponibilidade das informações.

Worm: Código malicioso capaz de se propagar automaticamente por redes ou sistemas, explorando vulnerabilidades, sem necessidade de intervenção do usuário, podendo causar degradação ou indisponibilidade de serviços.

Privacidade e LGPD

Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, e-mail, matrícula, telefone ou dados acadêmicos.

Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Titular de dados pessoais: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado (DPO): Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a ANPD.

Incidente de segurança com dados pessoais: Evento adverso confirmado ou sob suspeita relacionado à violação na segurança de dados pessoais, que pode acarretar risco ou dano relevante aos titulares (como acesso não autorizado, destruição, perda, alteração ou divulgação indevida).

ATORES E RESPONSABILIDADES

A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (**ETIR-UFJ**) é responsável pelas atividades relacionadas à gestão de incidentes de segurança da informação e privacidade.

Compete à ETIR-UFJ (PORTARIA UFJ No 672/2025, DE 08 DE JULHO DE 2025) atuar de forma preventiva e reativa para proteger a infraestrutura cibernética da UFJ. Assim, os principais atores envolvidos na gestão de incidentes de segurança e privacidade são:

- Gestor(a) da Segurança da Informação no âmbito do PPSI, definido como Agente Responsável, conforme previsto no item 4.1 da Norma Complementar (NC) 05/IN01/DSIC/GSIPR;
- Gestor(a) de Tecnologia da Informação no âmbito do PPSI, que ocupará a coordenação da ETIR em caso de afastamentos e impedimentos legais do membro designado no inciso I;
- Diretor(a) da Secretaria de Tecnologia da Informação (SeTI);
- Coordenação de Infraestrutura (SeTI);
- Coordenação de Desenvolvimento (SeTI);
- Coordenação de Suporte (SeTI);

- Encarregado(a) pelo Tratamento de Dados Pessoais, no âmbito da LGPD;
- **Usuários**, também atores importantes, pessoas que utilizam os dados e informações processados pela UFJ, com as seguintes responsabilidades:
    - a) utilizar os dados e informações prioritariamente para a realização das atividades desempenhadas, nos limites da ética, razoabilidade e legalidade;
    - b) notificar incidentes de segurança da informação; e
    - c) evitar se envolver em incidentes de segurança da informação.

NOTIFICAÇÃO DE INCIDENTES

Incidentes de Privacidade de Dados

O encarregado de dados da UFJ será o canal de comunicação para notificar incidentes de privacidade.

E-mail: lgpd@ufj.edu.br

Para incidentes com vazamento de dados pessoais, o Encarregado de Dados deve avaliar e fazer as comunicações, bem como informar e subsidiar os controladores ou operadores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a Autoridade Nacional de Proteção de Dados (ANPD).

Incidentes de Segurança da Informação

As notificações de incidentes de segurança da informação serão enviadas à ETIR.

E-mail: etir@ufj.edu.br

PADRÕES DE NOTIFICAÇÃO

Ao se registrar uma notificação de incidente de segurança da informação e privacidade, deve-se inserir as seguintes informações:

1. **Origem do incidente**: unidade, setor ou organização à qual dispositivo ou o processo que originou o incidente pertence;

2. **Contato da origem**: e-mail, telefone ou outro contato disponível do informante do incidente;
3. Registro do **tempo da ocorrência** do incidente: data e hora em formato GMT na qual o incidente foi identificado. Exemplo: “10:23, 20 de Março de 2021”;
4. Local **onde originou** o incidente: endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente;
5. **Recursos utilizados** pela origem do incidente: especificação do tipo do protocolo (IP, TCP, UDP, etc.) e portas, ou procedimentos operacionais, adotados na ação do incidente;
6. **Endereço do alvo**: endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acesso do serviço que foi o alvo do incidente;
7. **Protocolos e portas** alvos do incidente: especificação do tipo do protocolo (IP, TCP, UDP, etc.) e portas utilizados no destino do incidente;
8. **Serviços envolvidos**: especificação do serviço que foi alvo do incidente (http, ftp, smtp, etc.) e versões de sistemas utilizados;
9. **Descrição** do incidente: breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes;
10. **Logs ou evidências**: anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente;

Para o registro descrito acima, poderão ser utilizados:

1. Formulário específico para registrar o incidente (**https://etir.ufj.edu.br**). O incidente deverá ser documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas.
2. Quando for necessário manter o sigilo da fonte, sugere-se utilizar a plataforma Fala.BR (**https://falabr.cgu.gov.br**) como canal oficial de recebimento de manifestações que envolvam os direitos dos titulares de dados, caso o incidente envolva dados pessoais.
3. Para assegurar a confidencialidade no trânsito de evidências ou informações estritamente sensíveis durante o registro, sugere-se a possibilidade de envio de trechos de mensagens ou arquivos anexos criptografados, utilizando a chave pública PGP da ETIR.

TRIAGEM DO INCIDENTE

O objetivo do processo de triagem é reunir informações sobre o incidente, avaliar a sua natureza, classificar seu tipo e avaliar sua criticidade para que, apenas após esta etapa, se inicie o processo de tratamento.

Classificação do Incidente

Classificar o incidente quanto ao tipo, como uma das classes abaixo.

1. **Conteúdo abusivo**: spam, assédio, etc;

2. **Código malicioso**: bot, worm, vírus, trojan, spyware, scripts;

3. Prospecção por informações: varredura, sniffing, engenharia social;

4. **Tentativa de intrusão**: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;

5. **Intrusão**: Acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação;

6. **Indisponibilidade** de serviço ou informação: negação de Serviço, sabotagem;

7. **Segurança da informação**: acesso não-autorizado à informação, modificação não autorizada da informação;

8. **Fraude**: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;

9. **Outros**: incidente não categorizado.

Criticidade do Incidente

Determinar a classificação de criticidade do incidente de acordo com as classificações abaixo.

1. **Alto** (Impacto Grave) Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;

2. **Médio** (Impacto Significativo) Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;

3. **Baixo** (Impacto Mínimo) Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

Situação do Incidente

Definir uma situação para cada incidente, a fim de acompanhar o andamento do mesmo dentro do processo de tratamento.

1. **Aberto**: Nesse momento foi realizado apenas o registro das informações;

2. **Processando**: Quando o chamado é assumido por um técnico e está em tratamento;

3. **Pendente**: É preciso confirmar alguma informação com o solicitante antes de dar prosseguimento. Tentativas de contato devem ser realizadas e registradas;

4. **Pendente de Terceiros** (Transferido): Ocorre quando uma equipe solucionadora não tem ação no chamado e é repassado para outra coordenadoria ou equipe;

5. **Solucionado**: Indica que o procedimento técnico foi aplicado e aparentemente o chamado foi solucionado;

6. **Fechado**: Quando a solução do chamado foi confirmada pelo solicitante.

Preservação de Evidências

Antes de se iniciar as ações para restaurar as operações do ambiente, é necessária a preservação de provas para a identificação correta da causa raiz do incidente e, posteriormente, para a recuperação dos sistemas afetados.

PROCESSO DE MITIGAÇÃO DE INCIDENTES

Preparação

Gerenciar as ferramentas para análise de incidentes, incluindo o conhecimento de todo o ambiente utilizado:

- Implementar mecanismos de defesa e controle de ameaças;
- Desenvolver procedimentos para lidar com incidentes de forma eficiente;
- Obter recursos e equipe necessária para lidar com os problemas;
- Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.

Detecção

Detectar o incidente, determinar o escopo e as partes envolvidas com o incidente:

- Identificar todos os sistemas e serviços afetados relacionados com o incidente;
- Avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e impacto na reputação);
- Identificar a existência de outros eventos e alertas relacionados com o incidente em questão;
- Identificar que tipo de informação e processos podem ter sido afetados;
- Identificar os responsáveis pelo sistema comprometido, equipes de suporte e donos das informações.

Notificação

- Caberá à ETIR/UFJ notificar incidentes de segurança ao Centro Integrado de Segurança Cibernética do Governo Digital, seguindo os procedimentos definidos em https://www.gov.br/cisc/pt-br/incidente.
- Incidentes relacionados à privacidade, isto é, a dados pessoais, devem seguir os passos relacionados no tópico INCIDENTES COM DADOS PESSOAIS, abaixo.

Contenção

Conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos.

- Desconectar o sistema comprometido ou isolar a rede afetada;
- Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque;
- Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso;
- Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas.

Erradicação

Eliminar as causas do incidente, removendo todos os eventos relacionados.

- Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;
- Assegurar a remoção de todos os métodos de acesso utilizados pelo atacante: novas contas de acessos; backdoors e, se aplicável, acesso físico ao sistema comprometido, etc.

Recuperação

Restaurar o sistema ao seu estado normal.

- Caso exista Plano de Continuidade de Negócio dos serviços impactados, eles devem ser iniciados, conforme especificado no respectivo plano.
- Restaurar a integridade do sistema;
- Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas;
- Implementar medidas de segurança para evitar novos comprometimentos;
- Restauração do último e íntegro backup completo armazenado.

Avaliação

Avaliar as ações realizadas para resolver o incidente, documentando detalhes, e discutir lições aprendidas.

- Caracterizar o conjunto de lições aprendidas de modo a aprimorar os procedimentos e processos existentes;
- Identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe;
- Prover estatísticas e métricas relativas ao processo de resposta a incidentes;
- Obter informações que podem ser utilizadas em processos legais.

INCIDENTES COM DADOS PESSOAIS

Consta no art. 46 da LGPD que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, e tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

No caso de incidentes que envolvam dados pessoais e dados pessoais sensíveis, o presente Plano aponta, dentro do fluxo de tratamento de incidentes da ETIR/UFJ, as seguintes medidas como fundamentais:

- Preservar todas as evidências possíveis do incidente.
- Avaliar internamente o incidente e obter informações iniciais sobre:
    - i. o impacto do evento;
    - ii. a natureza, categoria e quantidade de titulares de dados pessoais afetados;
    - iii. a categoria e quantidade de dados afetados;
    - iv. as consequências do incidente para os titulares e para a UFJ, bem como criticidade e probabilidade.
- Comunicar à ETIR/UFJ em caso de incidentes na rede computacional.
- Comunicar ao Encarregado da UFJ a existência do incidente.
- Comunicar ao Controlador a existência do incidente, caso envolva dados pessoais.
- **Comunicar a ANPD e os titulares dos dados pessoais**
    - **Modelos de Comunicação nos Anexos 1 e 2**
    - **A comunicação à ANPD é feita utilizando-se o modelo de ofício constante no ANEXO 1. O canal oficial para este tipo de comunicação é através de peticionamento no SEI da ANPD. Na UFJ, o acesso a este sistema é mantido e realizado apenas pelo Encarregado pelo Tratamento de Dados Pessoais.**
    -
- Elaborar documentação com todas as informações coletadas, as ações realizadas para o tratamento efetivo do incidente e as considerações necessárias para promover a melhoria contínua no atendimento.

REFERÊNCIAS

POSIC-UFJ. Política de Segurança da Informação e Comunicação (POSIC) da UFJ. RESOLUÇÃO CONSUNI/UFJ Nº 025/2025, DE 03 DE DEZEMBRO DE 2025.

ETIR-UFJ. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos. PORTARIA UFJ No 672/2025, DE 08 DE JULHO DE 2025

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 23 de agosto de 2024.

BRASIL. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. Diário Oficial da União, Brasília, DF, 26 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024 Acesso em: 23 de agosto de 2024.

ANPD. Comunicação de incidente de segurança. Acessado em: 15 de dezembro de 2025. Disponível em : https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

UFLA. Plano de Gestão de Incidentes de Segurança da Informação e Privacidade, Versão 1.1 - 29/03/2021. Disponível em: https://dgti.ufla.br/pt/seguranca-informacao/normas-politicas-e-termos-si

FURG. Plano de Gestão de Incidentes Cibernéticos, Julho, 2024. Disponível em: https://segurancadainformacao.furg.br/

IFTO. Processo de Gestão de Incidentes de Segurança da Informação, 05/01/2024. Disponível em: https://portal.ifto.edu.br/acesso-a-informacao/seguranca-da-informacao/

SANTOS, Ingrid B. Guia sobre Comunicação de Incidente de Segurança (CIS), out de 2024. Disponível em: https://www.azevedosette.com.br/noticia/pt/guia-sobre-comunicacao-de-incidente-de-seguranca-cis/7639

ANEXO 1

Comunicação de incidente à ANPD (ofício)

Assunto: Comunicação de incidente de segurança com dados pessoais.

À
Autoridade Nacional de Proteção de Dados – ANPD
[A/C do órgão ou unidade competente]

Ref.: Comunicação de incidente de segurança com dados pessoais, nos termos do art. 48 da Lei nº 13.709/2018.

1. A **Universidade Federal de Jataí**, inscrita no CNPJ sob o nº 35.840.659/0001-30, por meio de seu Encarregado pelo Tratamento de Dados Pessoais, vem comunicar a ocorrência de incidente de segurança envolvendo dados pessoais, em cumprimento ao disposto na Lei nº 13.709/2018 e às normas complementares expedidas por essa Autoridade.

2. O incidente foi identificado em [data e hora], no **contexto** de [descrever, de forma sintética, o ambiente ou sistema afetado – por exemplo: sistema acadêmico, sistema de gestão de pessoas, serviço de e-mail institucional etc.].

3. De acordo com a **apuração inicial**, o incidente envolveu:
   a) Natureza dos dados pessoais afetados: [ex.: dados cadastrais, dados de contato, dados funcionais, dados acadêmicos, dados financeiros, dados sensíveis, se for o caso];
   b) Categoria dos titulares afetados: [ex.: estudantes, servidores docentes, servidores técnico-administrativos, terceirizados, candidatos em processos seletivos, participantes de pesquisa etc.];
   c) Volume estimado de titulares afetados: [informar número aproximado ou intervalo estimado];
   d) Abrangência do incidente: [ex.: acesso não autorizado, vazamento, indisponibilidade, alteração indevida de dados, perda de integridade etc.].

4. Até o momento, a universidade identificou os seguintes **riscos** e possíveis **impactos** aos titulares: [descrever, de forma objetiva, os riscos relevantes, tais como risco de fraude, exposição de dados sensíveis, discriminação, dano à imagem, violação de sigilo, uso indevido, vazamento de dados etc.].

5. Foram adotadas as seguintes **medidas técnicas e administrativas** para conter o incidente, mitigar seus efeitos e prevenir novas ocorrências:
   a) [ex.: isolamento do sistema afetado, bloqueio de credenciais, alteração de senhas, aplicação de correções, restauração de backups, reforço de controles de acesso, criptografia, antivírus, firewall, protocolos de autenticação, comunicação a áreas internas relevantes];
   b) [ex.: abertura de procedimento interno de apuração, notificação à área de segurança da informação, acionamento da auditoria interna, quando couber];
   c) [ex.: plano de comunicação aos titulares, reforço de orientações de segurança etc.].

6. Os **titulares** de dados pessoais afetados estão **sendo comunicados** por meio de [citar os canais utilizados – e-mail institucional, aviso no portal, mensagem em sistema, correspondência etc.], com informações sobre o incidente, seus possíveis impactos e orientações sobre medidas de proteção que podem adotar.

7. Para **maiores esclarecimentos** sobre o incidente e as medidas adotadas, a ANPD poderá contatar o Encarregado pelo Tratamento de Dados Pessoais desta universidade, por meio dos seguintes canais:
   - Nome: [NOME DO ENCARREGADO]
   - E-mail: lgpd@ufj.edu.br
   - Telefone: 64-3606-8386 (Whatsapp)
   - Endereço:
     - Diretoria de Processos e Governança de Dados - PROPLAN
     - Universidade Federal de Jataí - Câmpus Jatobá - Cidade Universitária, BR 364, km 195, nº 3800, CEP 75801-615

Termos em que,
Pede deferimento.

Jataí, [DIA] de [MÊS] de [ANO].

[NOME DO(A) REITOR(A) OU AUTORIDADE COMPETENTE]
Cargo: Reitor
Universidade Federal de Jataí

[NOME DO(A) ENCARREGADO(A) PELO TRATAMENTO DE DADOS PESSOAIS]
Encarregado(a) – Universidade Federal de Jataí

ANEXO 2

Comunicação de incidente aos titulares (aviso)

Assunto: Aviso sobre incidente de segurança envolvendo seus dados pessoais.

Prezado(a) [Nome do titular, se aplicável],

A **Universidade Federal de Jataí** informa que identificou, em [data], um incidente de segurança da informação que pode ter afetado dados pessoais sob sua titularidade.

1. O que ocorreu
   Em [data e, se for o caso, horário], foi detectado um incidente no [nome do sistema/serviço ou descrição geral], que resultou em [ex.: acesso não autorizado/possível exposição/indisponibilidade] de determinados dados pessoais.
2. Quais dados podem ter sido afetados
   Conforme a análise realizada até o momento, podem ter sido afetados os seguintes tipos de dados pessoais: [ex.: nome completo, CPF, e-mail, telefone, matrícula, dados acadêmicos, dados funcionais etc.].
   Não há, até o momento, evidências de comprometimento de [mencione, se for o caso, dados que não foram afetados, como senhas em texto aberto, dados financeiros, dados sensíveis etc., se for verdade].
3. Quais os possíveis impactos
   Em razão desse incidente, podem existir riscos como [ex.: recebimento de mensagens fraudulentas (phishing), tentativas de uso indevido de dados de contato ou outros impactos pertinentes].
   Até o presente momento, não há registro confirmado de uso indevido de seus dados pessoais decorrente deste incidente, mas a universidade permanece monitorando a situação.
4. Medidas adotadas pela universidade
   A universidade adotou as seguintes medidas para tratar o incidente e reduzir seus efeitos:

- [ex.: bloqueio imediato do acesso indevido e correção da vulnerabilidade identificada];
- [ex.: reforço dos controles de segurança da informação e revisão de procedimentos internos];
- [ex.: abertura de processo interno de apuração e comunicação à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável].

5. O que você pode fazer
   Recomenda-se que você:

- Altere imediatamente suas senhas de acesso;

- Monitore movimentações em contas vinculadas a dados pessoais;
- Preste atenção a comunicações suspeitas e tentativas de golpe;
- Desconfie de mensagens suspeitas que solicitem dados pessoais ou financeiros em nome da universidade;
- Não clique em links ou abra anexos de remetentes desconhecidos;
- Mantenha seus dispositivos atualizados e utilize soluções de segurança, como antivírus;
- Em caso de dúvidas ou se identificar uso indevido de seus dados, entre em contato imediatamente pelos canais abaixo.

6. Canal de contato para esclarecimentos
   Para obter mais informações sobre o incidente, os dados possivelmente afetados ou os seus direitos como titular de dados pessoais, entre em contato com o Encarregado pelo Tratamento de Dados Pessoais da universidade:
- E-mail: lgpd@ufj.edu.br
- Site/Canal institucional da LGPD: [URL da página LGPD da universidade]

A Universidade Federal de Jataí reforça seu compromisso com a proteção de dados pessoais e com a transparência na comunicação com seus titulares.

Atenciosamente,

[NOME DA AUTORIDADE RESPONSÁVEL PELO COMUNICADO]
Cargo: Encarregado pelo Tratamento de Dados Pessoais
Universidade Federal de Jataí