UNIVERSIDADE FEDERAL DO AMAZONAS

Plano de Gestão de Incidentes de Segurança da Informação

Manaus, maio de 2025

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DO AMAZONAS
Professor Doutor Sylvio Mário Puga Ferreira
Reitor

COMITÊ DE GOVERNANÇA DIGITAL
Professor Doutor Sylvio Mário Puga Ferreira
Reitor
David Lopes Neto
Pró-Reitor de Ensino de Graduação
Adriana Malheiro Alle Marie
Pró-Reitor de Pesquisa e Pós-Graduação
Almir Oliveira de Menezes
Pró-Reitor de Extensão
Maria Vanusa do Socorro de Souza Firmo
Pró-Reitor de Gestão de Pessoas
Maria da Glória Vitório Guimarães
Pró-Reitor de Planejamento e Desenvolvimento Institucional
Angela Neves Bulbol de Lima
Pró-Reitor de Administração e Finanças
Jorge Carlos Magno Silva de Lima
Diretor do Centro de Tecnologia da Informação e Comunicação
Nycolle Oliveira Souza Santos
Encarregada pelo Tratamento de Dados Pessoais
Dinorvan Fanhaimpork
Ouvidor
Azenilton Melo da Silva
Auditor

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Jorge Carlos Magno Silva de Lima
Diretor

COORDENAÇÃO DE SEGURANÇA DA INFORMAÇÃO
Márcia Regina Moraes de Paula
Coordenadora de Segurança da Informação

COORDENAÇÃO DE SERVIÇOS
Oldemar Diony Marinho Pereira Junior
Coordenador de Serviços

COORDENAÇÃO DE SISTEMAS
Diogo Soares Moreira
Coordenador de Sistemas

COORDENAÇÃO DE INFRAESTRUTURA
Thales Brandão de Lima
Coordenador de Infraestrutura

EQUIPE TÉCNICA DE ELABORAÇÃO
Lendel Monteiro
Márcia Regina Moraes de Paula
Pedro da Rocha Figueiredo

EQUIPE TÉCNICA DE REVISÃO
Gilberto Aires Libania
Lendel Monteiro
Márcia Regina Moraes de Paula
Pedro da Rocha Figueiredo
Robert Pessinga da Silva

Data	Versão	Descrição	Autor
20/03/2025	1.0	Plano de Gestão de Incidentes de Segurança da Informação.	Equipe Técnica de Elaboração
13/05/2025	2.0	Plano de Gestão de Incidentes de Segurança da Informação com as revisões da CTIC e sugestões do CGD.	Equipe Técnica de Revisão

Sumário

MINUTA DA RESOLUÇÃO

O **REITOR** da **UNIVERSIDADE FEDERAL DO AMAZONAS** e **PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL**, no uso de suas atribuições legais e regimentais,

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que "Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação" entre outros;

CONSIDERANDO o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos.

CONSIDERANDO a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal e por consequência trata da criação de Equipes de Tratamento e Resposta a Incidentes Cibernéticos no âmbito da Administração Pública Federal;

CONSIDERANDO a Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Norma Complementar 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, que estabelece as "Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal";

CONSIDERANDO a Portaria GSI/PR nº 120, de 21 de dezembro de 2022, que "Aprova o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal";

CONSIDERANDO a Portaria SGD/MGI Nº 852, de 28 de março de 2023, que "estabelece o Programa de Privacidade e Segurança da Informação (PPSI), no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP)";

CONSIDERANDO a Resolução CONSUNI nº 04 de 3 de abril de 2024, que instituiu a Política de Segurança da Informação e Comunicação (POSIC) da Universidade Federal do Amazonas (UFAM).

RESOLVE:

Art. 1° Instituir o Plano de Gestão de Incidentes de Segurança da Informação e regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da Universidade Federal do Amazonas (UFAM).

Art. 2° Esta Resolução entra em vigor na data de sua publicação.

ANEXO à RESOLUÇÃO

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA UNIVERSIDADE FEDERAL DO AMAZONAS

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1° O processo de Gestão de Incidentes de Segurança da Informação (SI) visa padronizar o tratamento de incidentes com respostas eficazes aos eventos de SI que afetem a disponibilidade, integridade, confidencialidade ou autenticidade associada aos ativos de Tecnologia da Informação (TI) e sistemas de informação e comunicações da UFAM. Seus principais objetivos são:

I - viabilizar que os recursos necessários estejam disponíveis para lidar com os incidentes, incluindo pessoas e tecnologia;
II - buscar que todas as partes responsáveis pelo tratamento de incidentes de segurança da informação tenham um entendimento claro sobre as tarefas que devem executar durante um incidente, seguindo os procedimentos predefinidos;
III - prover respostas sistemáticas e eficientes de modo que os serviços comprometidos sejam restaurados o mais rápido possível;
IV - minimizar o possível impacto do incidente de SI em termos de vazamento de informações, corrupção e interrupção de serviços;
V - compartilhar experiências, quando apropriado;
VI - prevenir ataques e danos futuros, e
VII - preservar informações para investigação, na medida do possível.

Art. 2° O Plano de Gestão de Incidentes de Segurança da Informação, a cargo da Equipe de Tratamento de Incidentes Cibernéticos (ETIR), está restrito a incidentes de SI em ativos de tecnologia da informação da UFAM.

Parágrafo único. Estão fora do escopo eventos adversos como desastres naturais, falha de hardware ou software, falha na linha de dados ou interrupção de energia.

CAPÍTULO II
CONCEITOS

Art. 3° Para efeitos deste normativo e em conformidade com o Glossário de Segurança da Informação do GSI/PR, aplicam-se as seguintes definições:

I - AGENTE RESPONSÁVEL PELA ETIR - servidor público, militar de carreira ou empregado público, ocupantes de cargo efetivo em órgão ou entidade da administração pública federal, direta ou indireta, incumbido de chefiar e gerenciar a equipe de prevenção, tratamento e resposta a incidentes cibernéticos (ETIR);

II - COMITÊ DE SEGURANÇA DA INFORMAÇÃO - grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal. Na Universidade Federal do Amazonas são atribuições do Comitê de Governança Digital;

III - COMUNIDADE OU PÚBLICO ALVO - conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IV - CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

V - DADO PESSOAL - informação relacionada à pessoa natural identificada ou identificável;

VI - ENCARREGADO - pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VII - EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

VIII - EVENTO DE SEGURANÇA - qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de

segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

IX - GESTOR DE SEGURANÇA DA INFORMAÇÃO - responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

X - GSI/PR - sigla de Gabinete de Segurança Institucional da Presidência da República;

XI - INCIDENTE DE SEGURANÇA - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XII - TRATAMENTO DE INCIDENTES CIBERNÉTICOS - consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias;

CAPÍTULO III
PAPÉIS E RESPONSABILIDADES

Art. 4° O Agente Responsável da ETIR tem a atribuição de gerenciar as atividades da ETIR, estabelecer os procedimentos operacionais, mobilizar e distribuir tarefas aos integrantes da ETIR, inclusive as de caráter proativo.

Art. 5° A ETIR é um grupo multidisciplinar criado com o objetivo de realizar o tratamento de um determinado incidente de SI.

§1º A ETIR é dada a responsabilidade por investigar e tratar o incidente de SI, executando ações de detecção, análise, contenção, erradicação, recuperação e avaliação crítica.

§2º Os membros da ETIR devem reportar ao Agente Responsável pela ETIR sobre as ações executadas.

Art. 6° Ao suporte CTIC (CSTIC) cabe o recebimento de notificações de incidentes de SI da comunidade acadêmica via sistema de abertura de chamados.

Art. 7° O relator do incidente é responsável pela notificação de um incidente de SI. Além dos próprios membros da ETIR, o relator do incidente pode ser:

I - comunidade acadêmica, isto é, usuários dos serviços e ativos de informação da UFAM (docentes, técnico-administrativos, discentes);

II - órgãos ou grupos externos de segurança da informação parceiros, tais como CTIR Gov, CAIS/RNP, CERT e outras ETIRs.

III - reclamantes externos, isto é, usuários que não fazem parte da comunidade acadêmica da UFAM, nem de órgãos ou grupos ou equipes de segurança da informação.

CAPÍTULO IV
PREPARAÇÃO

Art. 8° Para que o processo de resposta a incidentes ocorra da melhor forma possível, o Agente Responsável deverá conduzir as seguintes atividades:

I - verificar se as informações de contato para relatar incidentes estão corretas;

II - verificar se o processo para relatar incidentes está atualizado e disponível;

III - verificar se o processo de resposta a incidentes está atualizado e disponível;

IV - verificar a necessidade de atualização dos normativos internos associados ao processo de resposta a incidentes;

V - atualizar as funções e responsabilidades chave definidas para resposta a incidentes;

VI - conduzir exercícios de resposta a incidentes com toda equipe envolvida.

Parágrafo único. As atividades deverão ser realizadas de forma periódica ou sempre que consideradas necessárias pelo Agente Responsável

CAPÍTULO V
PROCESSO DE RESPOSTA À INCIDENTE

Art. 9° O processo de Gestão de Incidentes de Segurança da Informação possui suas atividades definidas nas Seções I a V do Capítulo V deste normativo e está descrito no ANEXO B.1 deste plano.

SEÇÃO I
NOTIFICAÇÃO E TRIAGEM

Art. 10. Qualquer incidente de SI relativo aos ativos de informação da UFAM deverá ser notificado à ETIR.

Art. 11. A ETIR receberá notificações oriundas dos relatores do incidente e deverá conter evidências do incidente de SI que está sendo reportado, informações de contato do reclamante e dados adicionais que possibilitem classificação e priorização adequadas do incidente.

Art. 12. As seguintes informações necessárias para o registro do incidente de SI devem ser informadas para o aceite da notificação:

I - informações de contato do reclamante;

II - informações da origem do incidente;

III - informações do alvo do incidente;
IV - descrição do incidente, e
V - logs ou evidências.

§1º Caso alguma dessas informações não esteja contida na notificação e mesmo assim seja possível prosseguir com seu tratamento, a ETIR a encaminhará para triagem.

§2º Caso alguma informação essencial para o tratamento do incidente não tenha sido informada, a ETIR deverá contatar o relator do incidente, de modo a viabilizar o registro e consequente tratamento do incidente. Caso as informações coletadas permaneçam insuficientes, o incidente será arquivado por impossibilidade de tratamento.

Art. 13. O relator do incidentes de SI deve utilizar um do seguintes meios para notificar o incidente de SI:

I - usuários da comunidade acadêmica da UFAM devem abrir chamado no portal de atendimento do CSTIC e as informações requisitadas no formulário de abertura de chamado devem ser devidamente preenchidas e identificadas como “Incidentes Cibernéticos”.
II - grupos de segurança ou reclamantes externos via contatos disponibilizados no site do CTIC.

Art. 14. A ETIR realizará triagem das notificações de incidente de modo a verificar se o evento reportado é um incidente de SI e se enquadra no escopo de tratamento da ETIR. Estando o evento dentro do escopo de atuação da ETIR, o agente deverá prosseguir com o registro.

SEÇÃO II
CLASSIFICAÇÃO E PRIORIZAÇÃO

Art. 15. A ETIR deve classificar e priorizar os incidentes de SI tendo como referência as informações registradas no relatório de incidente e deve seguir os critérios estabelecidos no ANEXO A.1 deste plano.

SEÇÃO III
PLANO DE COMUNICAÇÃO

Art. 16. O Agente Responsável pela ETIR reportará ao gestor de segurança da informação e comunicação sobre incidentes com prioridade alta segundo critérios estabelecidos no ANEXO B.1, durante o processo de tratamento do incidente.

Art. 17. No caso do incidente envolver outra(s) instituição(ões), o Agente Responsável, com a anuência do gestor de segurança da informação e comunicações, notificará a respectiva instituição, com vistas que as ações necessárias sejam tomadas.

Art. 18. Quando houver indícios de ato ilícito associado ao incidente, o Agente Responsável deverá informar ao gestor de segurança da informação para que o incidente seja reportado à devida autoridade.

Art. 19. Os incidentes que envolvam o comprometimento de dados pessoais devem ser informados ao Encarregado de Dados para avaliação, que determinará as medidas cabíveis, incluindo, se necessário, a comunicação à Autoridade Nacional de Proteção de Dados (ANPD).

Parágrafo único. Quando houver envolvimento de alunos, o incidente deve ser encaminhado para a PROEG nos casos de alunos de graduação, para a PROPESP nos casos de alunos de pós-graduação, e em caso de envolvimento de servidores, à PROGESP.

SEÇÃO III
MOBILIZAÇÃO DA EQUIPE DE TRATAMENTO

Art. 20. Os membros da ETIR estão distribuídos nas unidades organizacionais da UFAM, a saber:

I - Coordenação de Segurança da Informação (CSEGINFO);
II - Coordenação de Infraestrutura (COORDINFRA);
III - Coordenação de Sistemas (COORDISTE);
IV - Coordenação de Serviços de Tecnologia da Informação e Comunicação (CSTIC);

§1º Cada unidade organizacional deve ser representada por no mínimo dois servidores especialistas em suas respectivas áreas, sendo designado para cada titular um membro suplente.

§2º Os coordenadores de cada unidade deverão indicar os membros de sua coordenação participantes da ETIR.

§3º O Gestor de Segurança deverá indicar o Agente Responsável.

Art. 21. O percentual do esforço dedicado será negociado entre a supervisão de cada um dos membros e o Agente Responsável e deverá estar descrito no documento de nomeação dos membros da ETIR, resguardando-se um tempo mínimo de dedicação de 20% da carga horária para as atividades.

Parágrafo único. Em casos de incidentes de alta prioridade, deverá ser dada a devida atenção à sua resolução, independentemente do percentual mínimo estabelecido.

Art. 22. O membro servidor da ETIR para a qual a unidade organizacional foi reportada, poderá acionar outros servidores de sua unidade de modo que as ações necessárias ao tratamento do incidente reportado possam ser executadas.

Parágrafo único. A equipe responsável pelo tratamento do incidente será formada conforme a necessidade de cada ocorrência, sendo sua composição determinada pelas áreas competentes envolvidas na resolução do incidente.

Art. 23. Em casos excepcionais ou quando necessário, a ETIR poderá convocar a atuação de um especialista para auxiliar a equipe de tratamento de incidentes, conforme a natureza, prioridade e a complexidade do incidente.

Parágrafo único. O especialista convocado poderá ser representantes de outros setores da UFAM ou, quando necessário, um especialista externo solicitado.

Art. 24. A ETIR terá autonomia compartilhada e atuará em conjunto com os demais setores da UFAM responsáveis pela gestão de ativos de informação para auxiliar no processo de tomada de decisão durante um incidente.

§1º Os setores serão notificados e terão a responsabilidade de tomar as medidas necessárias para resolver os incidentes em sua área de atuação, devendo as orientações fornecidas, adotar as ações adequadas e informar à ETIR sobre as providências tomadas no tratamento dos incidentes, incluindo as medidas de prevenção adotadas para prevenir reincidência.

§2º A ETIR poderá participar ativamente do processo decisório, devendo recomendar procedimentos a serem executados ou medidas de recuperação durante um ataque.

§3º Os responsáveis pelos setores deverão seguir as orientações fornecidas, adotar as ações adequadas para solucionar o problema e informar à ETIR sobre as providências tomadas no tratamento dos incidentes, incluindo as medidas de prevenção adotadas para evitar reincidências.

SEÇÃO IV
RESPOSTA AO INCIDENTE

Art. 25. A resposta a incidente deverá seguir as seguintes etapas subsequentes:

I - Contenção: tem como propósito limitar o escopo, a magnitude e o impacto do incidente e inclui atividades como análise de impacto do incidente, proteção de informações e sistemas críticos, verificar o comprometimento de sistemas associados.

II - Erradicação: consiste na remoção da causa raiz do incidente e deve ser realizada observando as medidas apropriadas para garantir a preservação de informações relevantes.

III - Recuperação: tem como objetivo restaurar o sistema ao seu funcionamento normal. Deve-se remover a fragilidade de segurança que causou o incidente, além de restabelecer os serviços de forma controlada, priorizando os mais essenciais, monitorá-los para garantir que a restauração foi bem-sucedida.

Parágrafo único. A ETIR deve realizar revisões periódicas para assegurar que o incidente está sob controle. Caso a equipe de tratamento não consiga avançar na resolução do incidente, devem ser coordenadas atividades de escalonamento conforme os procedimentos estabelecidos.

Art. 26. Compete ao representante da ETIR verificar a efetiva resolução do incidente reportado. Caso persista, o incidente deve ser reenviado à equipe de tratamento para as providências necessárias.

Parágrafo único. Confirmada a resolução do incidente, o representante da ETIR deve comunicar sua conclusão às partes envolvidas revisar a classificação atribuída e, se necessário, reclassificá-lo, bem como assegurar o arquivamento dos dados e evidências coletadas.

SEÇÃO V
PÓS-ANÁLISE E LIÇÕES APRENDIDAS

Art. 27. A ETIR em conjunto com a equipe responsável pelo tratamento do incidente, deverá realizar uma pós-análise do incidente.

Parágrafo único. A realização da pós-análise deverá considerar o nível de criticidade do incidente, podendo ser dispensada em casos de menor impacto ou quando o procedimento de tratamento já for amplamente conhecido pela ETIR.

Art. 28. Nas ações de pós-análise, deverão ser realizadas as seguintes atividades:

I - avaliação dos danos causados pelo incidente;
II - aperfeiçoamento dos procedimentos de resposta a incidentes de SI;
III - fortalecimento das medidas de segurança para a proteção de sistemas, redes e ativos contra ataques futuros;
IV - contribuição para a disseminação de conhecimento sobre o processo de resposta a incidentes de SI;
V - promoção da capacitação das partes envolvidas por meio das lições aprendidas;
VI - instauração de queixa-crime, quando aplicável.

Art. 29. Após o encerramento do incidente, deverá ser elaborado um relatório documentando todas as ações tomadas durante o seu tratamento e registrá-lo junto à ETIR.

CAPÍTULO VI
DISPOSIÇÕES FINAIS

Art. 30. Em conformidade com a norma complementar 05/IN01/DSIC/GSIPR, o modelo de ETIR adotado deverá assim que possível, migrar

para o modelo centralizado no âmbito da instituição, sendo a ETIR composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes cibernéticos.

Art. 31. Este plano deverá ser revisado e atualizado a cada dois anos, a partir de sua vigência, ou sempre que a ETIR julgar necessário.

Art. 32. Os casos omissos serão analisados e deliberados por iniciativa da ETIR, do Gestor de Segurança da Informação ou do Comitê Governança Digital da Universidade Federal do Amazonas, observando-se a legislação em vigor.

ANEXO A.1 - CLASSIFICAÇÃO E PRIORIZAÇÃO DOS INCIDENTES

1. Classificação dos incidentes

Para fins deste plano, será considerada a seguinte previsão de classificação no tratamento de incidentes de segurança da informação da UFAM.

INCIDENTE	EQUIPES ENVOLVIDAS
Uso impróprio; -Uso de e-mail corporativo para spam ou promoção de negócios pessoais; -Instalação de softwares não autorizados; -Uso de pendrive de forma não autorizada; -Impressão não autorizada de documentos.	ETIR; CSTIC;
Vazamento de dados: -Exposição não autorizada de dados pessoais e informações privadas; -Credenciais roubadas ou comprometidas.	ETIR; Encarregado de Dados;
Tentativas de acesso não autorizado a sistemas ou dados, como por exemplo: -Tentar ou realizar acesso utilizando credenciais de terceiros; -Má utilização de um sistema; -Provocar falhas no sistema que impeça um acesso autorizado.	ETIR; CSTIC; COORDINFRA;
Ataques de negação de serviço: -Forçar um sistema a reinicializar ou consumir excessivamente recursos de forma que ele não possa mais fornecer seu serviço; -Obstruir mídia de comunicação entre os utilizadores de forma a não comunicarem-se adequadamente.	ETIR; COORDINFRA;
Vírus e outros códigos maliciosos;	ETIR; COORDINFRA; CSTIC;
Sequestro de dados (ransomware);	ETIR; COORDINFRA; CSTIC; Encarregado de Dados;

Desfiguração de sites;	ETIR; COORDSISTE;
Modificações em um sistema, sem conhecimento, instruções ou consentimento prévio do proprietário;	ETIR; COORDSISTE;
Coleta de Informações não autorizada; -Escaneamento não permitido da rede interna; -Sniffing; -Ataque de engenharia social -Phishing;	ETIR; COORDINFRA; CSTIC;
Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.	ETIR;
Outro; Todos os incidentes que não cabem em uma das categorias acima, devem ser classificados nesta classe.	ETIR;

2. Regras de priorização dos incidentes

A definição da prioridade dos incidentes de segurança da informação deve ser realizada pela ETIR com base em critérios técnicos e na análise do contexto de cada ocorrência. Sempre que julgar necessário, a ETIR poderá reavaliar e reclassificar a prioridade inicialmente atribuída por outras áreas, como a CSTIC, visando assegurar a adequada resposta ao incidente.

Os níveis de prioridade estão organizados em uma escala de 1 (um) a 5 (cinco), sendo 1 o mais crítico e 5 o menos crítico. A matriz a seguir estabelece os critérios para o cálculo da prioridade no tratamento dos incidentes de segurança da informação:

IMPACTO	**URGÊNCIA**		
	BAIXA	MÉDIA	ALTA
ALTO	3	2	1
MÉDIO	4	3	2

BAIXO	5	4	3

Impacto refere-se às consequências negativas que um incidente de segurança da informação pode causar à organização. A avaliação do impacto deve considerar o prejuízo às operações, à imagem institucional e aos serviços críticos, conforme a seguinte classificação:

- **Alto:**
  - Comprometimento de prazos legais ou interrupção de atividades administrativas ou acadêmicas críticas;
  - Danos à imagem institucional;
  - Indisponibilidade de um ou mais equipamentos, serviços ou sistemas classificados como críticos;
  - Afeta o funcionamento dos serviços de TI em períodos sensíveis, como matrícula de alunos, eventos institucionais, lançamento de notas, avaliações externas, entre outros.
- **Médio**:
  - Indisponibilidade parcial de sistemas, com manutenção das funções principais;
  - Interrupção das atividades de trabalho de um ou mais usuários;
  - Impacto sobre serviços institucionais ou prioritários da rede UFAM.

- **Baixo**:
  - Incidente pode ser tratado posteriormente, por necessidade do responsável;
  - Sistema ou serviço afetado permanece funcional, operando em modo de contingência;
  - Incidente não confirmado, identificado apenas como ameaça ou vulnerabilidade.

Urgência é definida pela necessidade de restabelecimento do serviço ou sistema em um prazo aceitável. Quanto menor o tempo tolerável para a recuperação, maior a urgência atribuída ao incidente. A seguir, a classificação dos níveis de urgência:

- **Alta:**
  - Restabelecimento deve ocorrer imediatamente ou no menor tempo possível, pois o impacto do incidente tende a se agravar com o

tempo.

- **Média:**
  - Restabelecimento necessário com brevidade, mas sem caráter emergencial imediato.
- **Baixa:**
  - O tratamento pode ser programado para uma data futura, sem comprometimento significativo das operações.

ANEXO B.1 - PROCESSO DE TRATAMENTO DE INCIDENTES