Plano de Gestão de Incidentes de Segurança da Informação e Comunicação

O COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA UFV, no uso de suas atribuições legais e regimentais, resolve aprovar Plano de Gestão de Incidentes de Segurança da Informação e Comunicação da Universidade Federal de Viçosa (UFV):

1. Apresentação

A Universidade Federal de Viçosa (UFV), por meio da ETIR/UFV, estabelece este Plano de Gestão de Incidentes em redes computacionais para orientar a identificação, análise, resposta e recuperação diante de eventos que afetem ativos, serviços e informações institucionais.

O Plano alinha-se às políticas internas e à legislação brasileira de segurança e proteção de dados, adotando princípios de finalidade, necessidade, prevenção e segurança. Define procedimentos padronizados para: identificar, receber e classificar notificações; priorizar e conter incidentes; erradicar causas; recuperar serviços; registrar evidências; e comunicar partes interessadas. Este alinhamento principiológico adota a Segurança e Privacidade desde a Concepção (Security and Privacy by Design) como pilares da resposta. O tratamento de incidentes na UFV pauta-se pela busca da resiliência, garantindo que as ações de remediação sejam proporcionais ao risco, transparentes aos órgãos de controle e focadas na preservação dos direitos fundamentais dos titulares de dados e na continuidade do bem comum.

O Plano fundamenta-se na Política Nacional de Segurança da Informação (Decreto nº 9.637/2018) e na Portaria SGD/MGI nº 9.511/2025 (PPSI 2.0), integrando-se à Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) conforme o Decreto nº 10.748/2021. Observa estritamente a Lei nº 13.709/2018 (LGPD), assegurando que o tratamento de incidentes ocorra em plena harmonia com o Programa de Governança em Privacidade da UFV (PGPriv) e as Normas Complementares do GSI/PR, notadamente as NC 05, 08 e 21.

Estabelece, ainda, objetivos institucionais: reduzir impacto e recorrência, fortalecer a cultura de segurança e aprimorar continuamente o processo de resposta. Por fim, delimita escopo e responsabilidades, atribuindo à ETIR a coordenação das ações e aos setores envolvidos a cooperação necessária com base em criticidade e impacto.

2. Objetivos

2.1 Objetivo geral

Este plano de gestão de incidentes de segurança da informação visa garantir o tratamento e resposta eficazes aos eventos de segurança da informação que afetam a disponibilidade, integridade, confidencialidade ou autenticidades associadas aos ativos e sistemas de informação e comunicações da UFV. Além disso, o plano tem por objetivo definir funções e responsabilidades, documentar as ações e medidas necessárias para o tratamento de incidentes de forma rápida e eficiente, limitando seu impacto, e, assim, protegendo os ativos e as informações.

2.2 Objetivos específicos

- Orientar respostas padronizadas e céleres, com registro formal e proteção de evidências, assegurando a melhoria contínua e prevenção de novos incidentes.
- Dar transparência ao fluxo de procedimentos e responsáveis durante o tratamento do incidente.
- Consolidar lições aprendidas em uma base de conhecimento institucional.
- Assegurar conformidade legal e regulatória, incluindo comunicações exigidas à ANPD, quando aplicável.

3. Papéis e Responsabilidades

- **Gestor de Segurança da Informação e Comunicação (GSIC):** responsável por coordenar as ações de segurança da informação e comunicações na organização.
- **Equipe de Tratamento de Incidentes em Redes (ETIR-UFV):** Responsável por receber, analisar, tratar ou apoiar o tratamento e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no ambiente da Universidade Federal de Viçosa.
- **Encarregado:** atua como canal de comunicação entre a UFV, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).
- **Administrador de rede ou de sistema:** responsável por investigar e tratar os incidentes de segurança, executando ações de análise e detecção do

incidente, contenção, erradicação, recuperação e avaliação crítica, reportando-se à ETIR-UFV sobre ações executadas e atualizando-a sobre mudanças nos contatos de redes ou sistemas.

- **Diretoria de Tecnologia da Informação DTI:** Responsável pela administração da TI da Universidade Federal de Viçosa.
- **Diretoria de Comunicação Institucional DCI:** Responsável pela comunicação com a comunidade acadêmica.

Fluxo e Matriz de Responsabilidades e Papéis (RACI) – Notificação em vazamento de credenciais:

Ação	**ETIR**	**GSIC e DTI**	**Encarregado**	**Comunicação (DCI)**
Avisos **técnicos** a donos de sistemas	R/A	C	C	I
Comunicado **institucional** interno (prazos, determinações)	C	R/A	I	I
CIS à ANPD e **titulares** (LGPD art. 48)	C	C	R/A	C
Notificação ao **CTIR Gov/REGIC**	R/A	C	I	I
Nota pública / imprensa	C	C	C	R/A
Tratamento	R	I	C	I

Legenda: **R**=Responsável, **A**=Aprovador, **C**=Consultado, **I**=Informado.

4. Processo de Tratamento de Incidentes de Segurança da Informação

O processo de tratamento de incidentes de segurança da UFV possui diversas fases e cada uma dessas fases possui um conjunto de entradas e saídas, ações e papéis, cuja execução ocorre sobre responsabilidade da Equipe de Tratamento de Incidentes de Redes da UFV (ETIR-UFV) com base no fluxo da Figura 1.

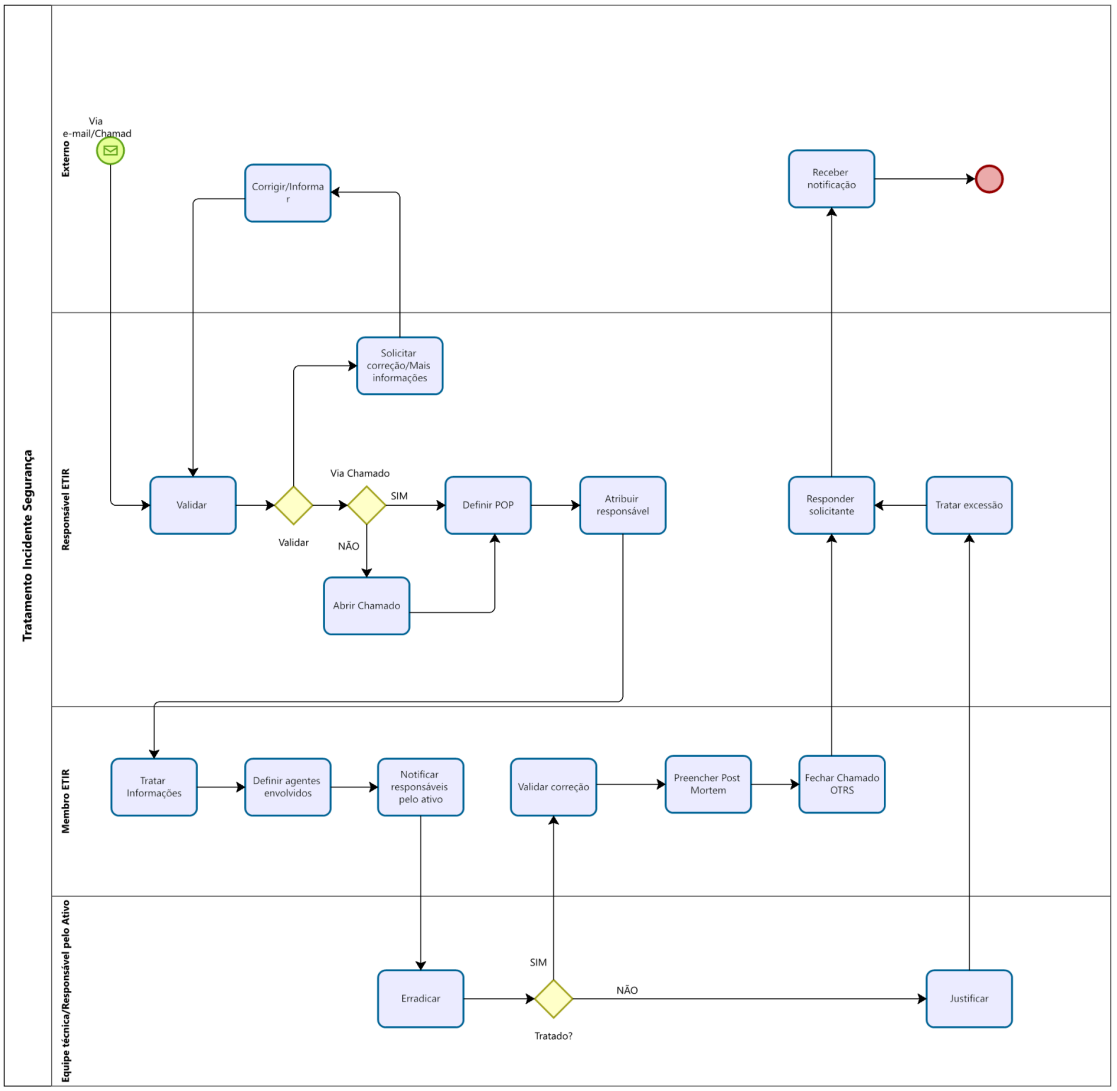

Fig 1: Fluxo de tratamento de incidentes de segurança da ETIR-UFV

O fluxo de tratamento de incidentes de segurança apresentado acima será detalhado a seguir:

4.1 Identificação

A identificação é o processo no qual a ETIR toma conhecimento de um determinado incidente. Dar-se-á por um ou mais dos meios listados abaixo:

4.1.1 Recebimento de notificações:

Serão considerados os seguintes meios para o recebimento de notificações de incidentes de segurança relacionados a UFV:

- Sistema de Chamados da DTI: https://chamado.dti.ufv.br/

- e-mail: etir@ufv.br
- web: www1.dti.ufv.br/etir-ufv

As notificações devem conter evidências do incidente de segurança sendo reportado, bem como informações de contato do reclamante e dados adicionais que possibilitem melhor classificação e priorização do incidente.

4.1.2 Sistemas IPS, IDS e firewalls de aplicação

Ferramentas automatizadas, como o Alienvault, NMAP e Scripts shell. Esses sistemas geram relatórios, alertas e registros em log que permitem a identificação tanto de incidentes como de vulnerabilidades que possam levar a incidentes. Além disso, eles podem gerar dicas e procedimentos para mitigação e correção dos problemas encontrados.

4.1.3 Notificações de terceiros (RNP/SGIS, CTIR.Gov, CERT.br)

As notificações ficam registradas em banco de dados e são enviadas por e-mail às ETIRs. Há procedimentos de resposta para a notificação de correção e pedidos de ajuda.

4.1.4 Verificação pessoal

A verificação pessoal ocorre quando um usuário detecta o incidente sem o uso de ferramentas automatizadas. Nesse caso, o problema deve ser relatado a ETIR e devidamente registrado no sistema de chamados da DTI.

4.2 Validação e Triagem

O objetivo do processo de triagem é reunir informações sobre o incidente, avaliar a sua natureza, identificar o escopo do incidente e validar as informações nele contidas para que, mais adiante, seja possível tomar decisões sobre como tratá-lo.

O primeiro passo no processo de validação e triagem é avaliar se as seguintes informações estão presentes na notificação do incidente:

- Informações de contato do reclamante
- Informações de origem do incidente
- Informações do alvo do incidente
- Descrição do incidente

Caso uma informação essencial para o tratamento do incidente não esteja presente, o agente responsável deverá retorná-lo ao reclamante para que possa obter mais informações. Caso não seja possível prosseguir com o

tratamento e o reclamante não possa fornecer mais informações, o incidente será então fechado por impossibilidade de tratamento.

Caso o incidente tenha sido notificado por e-mail ou outro meio de comunicação que não seja o sistema de chamado da DTI, será criado um chamado no sistema.

O escopo determinará se o incidente está relacionado com ativos internos da equipe de TI da instituição ou é de responsabilidade de terceiros, inclusive se o incidente é de responsabilidade de outra instituição.

4.3 Classificação e Priorização

4.3.1 Categorias de Incidentes – Taxonomia

Os incidentes deverão ser classificados. A classificação visa compreender o método utilizado por um atacante para a realização de alguma atividade maliciosa. A classificação poderá seguir a tabela abaixo, aplicando-se a mesma inclusive quando envolver dados pessoais:

Incidente	Descrição
Comprometimento de sistema	Incidente genérico de comprometimento de um sistema computacional.
Copyright (direitos autorais)	Uso não autorizado de material protegido por direitos autorais. Vulgarmente conhecido como “pirataria”.
Desfiguração de páginas (web-defacement)	Alteração não autorizada de páginas em um site.
Destruição de dados	Exclusão ou corrupção de dados de um sistema computacional.
dos	Negação de Serviço. Perturbação temporária no acesso normal a um sistema ou rede computacional.
Phishing	Fraudes Eletrônicas. Similar ao Spam, mas com o objetivo de levar o receptor a clicar em URL que leve a site malicioso, baixar e instalar algum malware ou a fornecer informações sensíveis.
Vazamento	Qualquer tipo de vazamento (intencional ou não) de informação sensível ou classificada.

malware	Uso, disseminação ou divulgação de software malicioso, deliberadamente desenvolvido com fins de ataque a sistemas computacionais. Exemplo: vírus, trojans, ransomware, etc.
Sequestro de Dados	Uso de alguma técnica que efetue o travamento de dados, impossibilitando seu usuário de acessá-los. Pode envolver pedido de resgate. Exemplo: ataques de ransomware.

Com base na classificação o próximo passo no processo é a definição do Procedimento Operacional Padrão (POP). Para cada tipo de incidente existe um POP apropriado.

4.3.2 Criticidade

Os níveis de criticidade para tratamento de incidentes de segurança pelo ETIR-UFV são independentes dos níveis de criticidade definidos para tratamento de requisições e incidentes da central de serviços de TI da UFV, refletindo os acordos de nível de serviço da ETIR com a equipe de administradores e redes da instituição e não com seus usuários diretamente. Dessa forma, os acordos de níveis de serviço de TI estabelecidos com os usuários devem ser respeitados. Essa observação é particularmente importante para CSIRT com modelo de dedicação compartilhada.

Os níveis de criticidade, no entanto, possuem correlação com o modelo da atribuição de prioridades do Plano de Gestão de Incidentes e Requisições da DTI/UFV, aqui simplificados. Nesse modelo, os níveis de criticidade variam de um a cinco, sendo um o menos crítico e o cinco mais crítico.

Portanto, a matriz abaixo é utilizada para realizar o cálculo da criticidade ou prioridade para tratamento de incidentes de segurança:

Impacto	Urgência		
	Baixa	Média	Alta
Alto	3	4	5
Médio	2	3	4
Baixo	1	2	3

O impacto dos incidentes de segurança é definido em função de ocorrências ou consequências negativas para a organização, conforme listado a seguir:

• **ALTO:** O incidente implica perda de prazos legais ou no funcionamento de atividades críticas Administrativas ou Acadêmicas da organização; o incidente causa impacto negativo na imagem institucional da organização; o incidente causa indisponibilidade em um ou mais equipamentos, serviços ou sistemas críticos da organização; o incidente compromete o bom funcionamento de serviços de TI e ocorre em momentos críticos da organização, como período de matrícula de alunos, inscrição em processos seletivos, eventos, lançamento de notas, avaliação de órgãos financiadores etc; o incidente impede o funcionamento de uma unidade organizacional.

• **MÉDIO:** o incidente provoca a indisponibilidade de parte do sistema, porém suas funções principais estão operacionais; a falha impede o trabalho do dia a dia de um ou mais usuários; o incidente implica impactos institucionais ou serviços prioritários da rede UFV;

• **BAIXO:** o incidente de segurança não pode ser tratado imediatamente, por necessidade do responsável; o serviço ou sistema afetado pelo incidente continua funcionando, porém em modo contingência; o incidente de segurança não foi confirmado, tratando-se apenas de uma vulnerabilidade ou ameaça.

A urgência é determinada pela necessidade de restabelecimento dos serviços ou do sistema dentro de determinado prazo. Quanto menor for o tempo aceitável ou tolerável para restauração ou recuperação do incidente em questão, maior será a urgência. A listagem a seguir classifica os níveis

de urgência em função de um fator determinante:

• **ALTA**: O equipamento, sistema ou serviço precisa ser restabelecido imediatamente ou o mais rápido possível; o dano ou o impacto causado pela falha aumenta significativamente com o tempo;

• **MÉDIA**: O equipamento, sistema ou serviço precisa ser restabelecido assim que possível;

• **BAIXA**: O tratamento do incidente poderá ser agendado para data específica, a posteriori.

Segue abaixo os prazos e acordos de nível de serviço para iniciar o tratamento de incidentes de segurança da informação da UFV, de acordo com o nível de prioridade:

Prioridade	Tempo Máximo para Início do Tratamento
1	Em até 24hs ou em data posterior específica ou programada.
2	Em até 12hs
3	Em até 8hs
4	Em até 4hs
5	Em até 2hs

4.3.3 Status

Os status que podem ser atribuídos a um incidente de segurança registrado são listados na tabela a seguir:

Status	Descrição
Novo	Incidente recém-recebido, aguardando primeiro atendimento
Processando	Incidente sendo tratado, seja pela equipe interna ou por terceiros
Planejado	Incidente sendo tratado porém com atividade planejada para execução futura
Pendente	Incidente sendo tratado, encaminhado para responsável e aguardando resposta
Fechado - Resolvido	Incidente cujo tratamento foi concluído com sucesso
Fechado - Cancelado	Incidente foi cancelado porque se trata de falso positivo, porque não faz mais sentido prosseguir com tratamento etc.
Fechado - Sem resposta	Incidente cujo tratamento esgotou as tentativas de interação ou prazos para resposta

4.5 Tratamento do Incidente

O tratamento de incidentes de segurança consiste em um conjunto de ações a serem executadas de acordo com cada ativo de informação da organização. Abaixo serão apresentadas as ações de forma geral, sendo necessária a definição de procedimentos operacionais padrão (POP) específicos para cada serviço. As ações de tratamento de incidentes são, portanto:

• **Detecção e Análise:** consiste em realizar a análise e detecção do incidente, determinando a sua natureza e extensão, além de prover detalhes dos sistemas comprometidos. Deve-se contemplar: sistemas e serviços afetados, impacto e risco, eventos correlatos e responsáveis. A correlação do incidente com eventos passados pode ajudar a identificar semelhanças e possíveis soluções. Nessa etapa, a equipe de segurança pode identificar as áreas da organização que atuarão em conjunto com a ETIR para contribuir com informações úteis durante o processo. Por fim, inicia-se a execução de um Plano de Investigação de Incidentes de Segurança;

• **Contenção:** nessa etapa o responsável pelo tratamento do evento deverá executar um Plano de Contenção de Incidentes de Segurança, limitando ou atenuando os danos causados;

• **Preservação de evidências:** antes de se iniciar as ações para restaurar o ambiente, é necessária a preservação de provas e evidências para a identificação correta da causa raiz do incidente e ações futuras;

• **Recuperação:** consiste em recuperar o sistema ou rede em questão, retornando ao seu estado normal de operação através de um Plano de Recuperação de Incidentes de Segurança. Deve-se restaurar a integridade do sistema e garantir sua disponibilidade. Em alguns casos, é possível partir para a etapa de Erradicação ou Mitigação sem necessidade de Recuperação, porém deve-se garantir as propriedades integridade e disponibilidade anteriormente mencionadas;

• **Erradicação ou Mitigação:** nessa etapa o responsável pelo tratamento do evento deverá executar um Plano de Correção, Mitigação ou Erradicação do incidente, eliminando sua causa raiz. É importante remover a fragilidade de segurança utilizada para causar o incidente em questão. Idealmente, todas as ameaças e riscos devem ser removidos do sistema ou da rede antes que seja restabelecido online. É importante também validar as correções com as áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade;

• **Avaliação:** consiste em avaliar o incidente, caracterizando um conjunto de lições aprendidas, prover relatórios, identificar características do incidente para treinar a equipe no tratamento de novos eventos e, quando cabível, levantar informações a serem usadas em processos legais. Deve-se produzir ao final

do incidente um relatório sobre o seu tratamento, registrando-o junto à ETIR-UFV;

Os documentos complementares mencionados nesta norma, quando ainda não formalmente elaborados, aprovados ou publicados, deverão ser desenvolvidos oportunamente pelas unidades competentes, observadas as diretrizes aqui estabelecidas.

4.6 Escalonamento do Incidente

Quando um incidente de segurança não for resolvido dentro do tempo máximo para solução acordado em seu respectivo SLA, deverá ser executada uma ação de escalonamento daquele incidente, tanto internamente na ETIR, quanto entre outros setores da organização e parceiros externos, quando cabível. Serão considerados os dois tipos de escalonamento convencionados no ITIL:

- Escalonamento Funcional (horizontal), que trata da passagem do incidente de segurança que não foi resolvido por determinada equipe ou responsável para uma outra equipe ou responsável mais especializado;
- Escalonamento Hierárquico (vertical), para casos de incidentes de segurança graves que precisam notificar superiores imediatos na cadeia de comando do setor da organização, a fim de agilizar o tratamento do incidente.

4.7 Fechamento e Resposta ao Incidente

No fechamento de um incidente de segurança, a equipe de tratamento de incidentes deverá, quando cabível, validar se as ações de tratamento do incidente foram executadas (conforme Seção 4.5) e se o incidente em questão foi ou não resolvido.

Para incidentes cujo escopo de tratamento envolve organizações externas ao escopo do ETIR, o incidente de segurança poderá ser fechado após um período de quinze dias úteis sem resposta ou após três tentativas de contato sem sucesso. Para incidentes dentro do escopo da ETIR, a equipe deve tratar ou cobrar o tratamento do incidente até que seja resolvido ou, no mínimo, tenha sido tratado até uma fase cujo impacto seja aceitável pela instituição.

Havendo recomendações a serem feitas aos usuários, administradores de sistemas ou a outras equipes de segurança, estas devem ser feitas no processo de fechamento do incidente.

Por fim, deve-se preencher o relatório PostMortem com as informações necessárias e anexar ao chamado do incidente.

4.8 Lições Aprendidas

Esta fase do tratamento de incidentes consiste em avaliar todo o processo de tratamento do incidente e verificar a eficácia das soluções adotadas. Devem-se relacionar e documentar no tíquete do incidente as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões.

Deve-se, ainda, realizar ou promover a realização de reuniões de lições aprendidas dos incidentes tratados, culminando na produção de documentos de recomendações ou ações futuras na organização para evitar novas ocorrências do incidente ou viabilizar seu tratamento.

Vale salientar que a realização de tais reuniões podem estar relacionado com o nível de criticidade do incidente, podendo ser dispensada para incidentes menos críticos ou cujo tratamento já seja conhecido pela ETIR-UFV.

5 Disposições Finais

A ETIR-UFV poderá atualizar ou adaptar esse documento a qualquer tempo que julgar necessário, a fim de mantê-lo consistente com as demandas e diretrizes da área de segurança da informação e comunicações.

6 Histórico de revisões

Rev.	Data	Descrição	Itens Revisados	Autor