Plano de Gestão de Incidentes de Segurança da Informação

Diretoria de Governança e Gestão de TIC
Coordenação de Segurança da Informação e Proteção de Dados

Março/2021

UNIVERSIDADE FEDERAL DE PERNAMBUCO

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DE PERNAMBUCO
SUPERINTENDENCIA DE TECNOLOGIA DA INFORMAÇÃO – STI
DIRETORIA DE GOVERNANÇA E GESTÃO DE TIC - DGGTIC

Equipe de Colaboradores do Plano de Gestão de Incidentes de Segurança da Informação

André Souto Soares Afonso

Daniel da Cruz Brandão

Daniel Wanderley Vieira

Denisson Paulo de Albuquerque

Diego Augusto de Sena

Éber Luís de Melo Santos

Fernanda Rodrigues dos Santos D'Amorim

John Ewerton dos Santos Paiva

Maria Betânia Martins da Silva

Nestor Moreira Reis Neto

Paulo Shiosaki

Pedro Corrêa de Araújo Neto

Rosângela Saraiva Carvalho

Aprovação

Marco Aurélio Benedetti Rodrigues
Superintendente de Tecnologia da Informação - STI

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR (ES)	APROVADO POR
11/03/2021	1.11	O Plano de Gestão de Incidentes de Segurança da Informação apresenta o processo de gestão e o plano de tratamento de incidentes de segurança da informação, contendo papéis e responsabilidades, assim como, demais informações pertinentes ao processo.	Equipe de colaboradores do Plano de Gestão de Incidentes de Segurança da Informação	CSIPD DGGTIC DC DITIC DDS STI

Conteúdo

1 Objetivo

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 UFPE.

Os principais objetivos do tratamento de incidentes de SI são:

- Viabilizar que os recursos necessários estejam disponíveis para lidar com os incidentes, incluindo pessoas, tecnologia, entre outros.
- 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.
- Prover respostas sistemáticas e eficientes de modo que os serviços comprometidos sejam restaurados o mais rápido possível.
- Minimizar o possível impacto do incidente de SI em termos de vazamento de informações, corrupção e interrupção de serviços.
- Compartilhar experiências, quando apropriado.
- Prevenir ataques e danos futuros.
- Preservar informações para investigação, na medida do possível.

2 Escopo

O plano de gestão de incidentes de segurança da informação, a cargo da equipe de tratamento de Incidentes de Segurança da Informação (ETISI) está restrito a incidente de SI em ativos de tecnologia da informação da UFPE.

Estão fora do escopo eventos adversos como: desastres naturais, falha de hardware / software, falha na linha de dados, interrupção de energia. Estes eventos serão abordados pelo plano de continuidade de negócio.

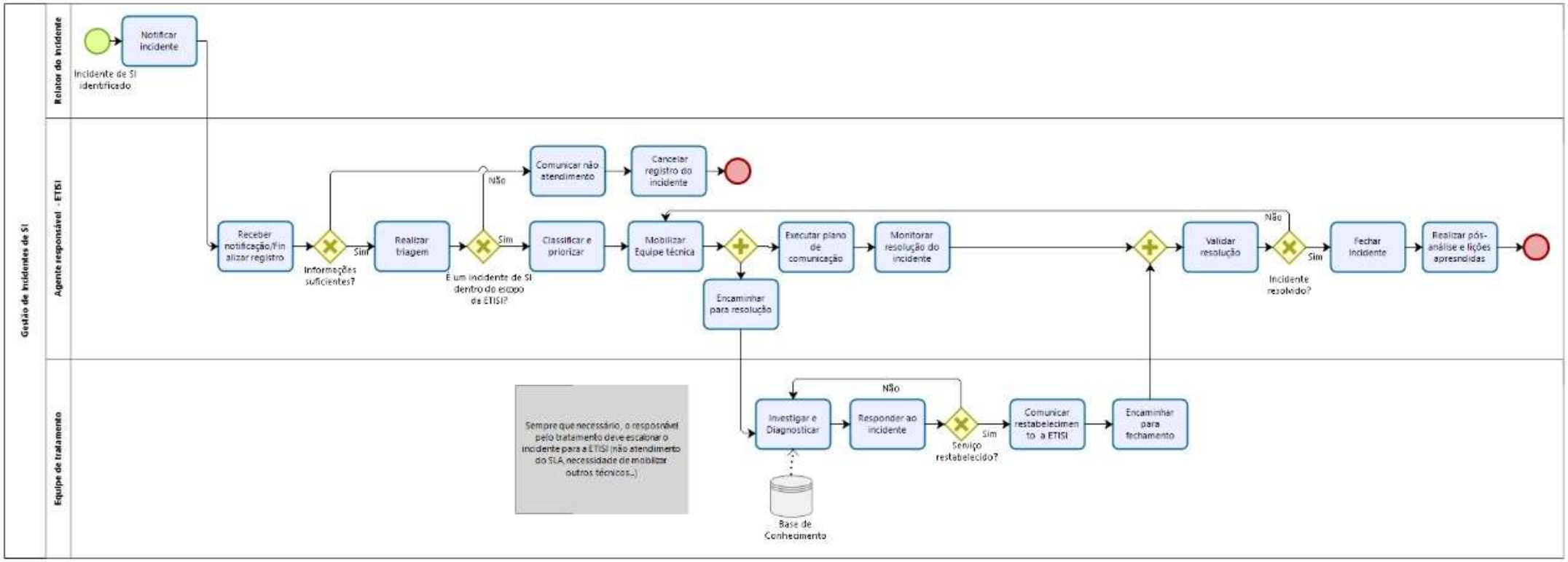
3 Papéis e Responsabilidades

- **Agente responsável da ETISI**: receber as notificações de incidentes de segurança, realizar a triagem, mobilizar a ETISI e acompanhar suas atividades na resolução do incidente, responder às notificações de incidentes de SI e demais atividades relacionadas a incidentes de SI no ambiente da Universidade Federal de Pernambuco.
- **Central de Serviços de TIC** (CSTIC): recebimento de notificações de incidentes de SI da comunidade acadêmica. <https://cstic.ufpe.br>.
- **Equipe de tratamento**: Grupo (multidisciplinar) criado com o objetivo de realizar o tratamento de um determinado incidente de SI. A este grupo é dada a responsabilidade por investigar e tratar o incidente de SI, executando ações de detecção, análise, contenção, erradicação, recuperação e avaliação crítica. Este grupo deve reportar ao agente responsável pela ETISI sobre as ações

executadas. No caso, de incidentes de SI ocorridos nos campi Caruaru e Vitória, CIn e HC, o grupo deve reportar ao respectivo representante da ETISI que comunicará ao agente responsável.

- **ETISI**: equipe responsável por coordenar os trabalhos no tratamento dos incidentes de SI.
- **NATI**: Núcleo de Apoio a Tecnologia da Informação, dar apoio no tratamento do incidente quando solicitado por algum membro da ETISI, fazendo, assim, parte da equipe de tratamento, no respectivo centro acadêmico ou órgão de atuação.
- **Relator do Incidente**: responsável pela notificação de um incidente de SI. Além dos próprios membros da ETISI, o relator do incidente pode ser:
    - **Comunidade acadêmica**: usuários dos serviços e ativos de informação da UFPE (Docentes, Técnico-administrativos, Discentes)
    - **NATI**: Núcleo de Apoio à Tecnologia da Informação formado por equipe especializada composta por servidores técnicos e bolsistas que têm como finalidade recuperar incidentes que demandem intervenção física de hardware e de software.
    - **Órgãos ou grupos externos**: órgãos/grupos de segurança da informação parceiros (CAIS/RNP, CERT e outras Equipes de Tratamento de Incidentes de segurança (ETIR's)).
    - **Reclamantes externos**: usuários que não fazem parte da comunidade acadêmica da UFPE, nem de órgãos ou grupos/equipes de segurança da informação.

4 Processo de tratamento



4.1 Notificação

Qualquer incidente de SI relativo aos ativos de informação da UFPE deve ser notificado à ETISI.

A ETISI receberá notificações internas, provenientes da comunidade acadêmica, de órgãos/grupos de segurança da informação parceiros (RNP, CERT e outras equipes de tratamento de incidentes de segurança (ETIR's)), assim como de reclamantes externos.

Saliente-se que as notificações devem conter evidências do incidente de SI que está sendo reportado, bem como, informações de contato do reclamante e dados adicionais que possibilitem melhor classificação e priorização do incidente.

Para notificar um incidente de SI, o relator deve utilizar um dos meios abaixo relacionados:

- **Usuários da comunidade acadêmica da UFPE**, **NATI** e **ETISI**: devem abrir chamado na Central de Serviços de TIC (**CSTIC**), as informações requisitadas no formulário de abertura de chamado devem ser devidamente preenchidas. Disponível em: <https://cstic.ufpe.br>.
- **Grupos de segurança ou reclamantes externos**, por:
  - Telefone: (81) 2126-7809
  - E-mail: etisi.nti@ufpe.br

No caso do **CAIS/RNP** - cabe a ETISI observar as notificações de incidentes de SI reportados no Sistema de Gestão de Incidentes de Segurança (SGIS) da Rede Nacional de Ensino e Pesquisa (RNP) ou habilitar e-mail para receber tais notificações.

4.2 Recebimento das notificações

A ETISI receberá todas as notificações de incidentes de segurança da informação.

Para o aceite da notificação deverá ser observado se todas as informações necessárias para o registro do incidente de SI foram devidamente preenchidas, a saber:

- Informações de contato do reclamante;
- Informações da origem do incidente;
- Informações do alvo do incidente;
- Descrição do incidente;
- Log's ou evidências.

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

4.3 Contactar relator do incidente

Caso alguma informação essencial para o tratamento do incidente não tenha sido preenchida no formulário de abertura do chamado, a ETISI deverá contatar o relator do incidente, de modo, a viabilizar o registro e consequente tratamento do incidente.

Quando as informações coletadas forem insuficientes, o incidente será, então, arquivado por impossibilidade de tratamento.

4.4 Finalizar o registro

Após todas as informações necessárias ao atendimento da ocorrência notificada terem sido coletadas, a ETISI finalizará o registro do incidente no sistema de chamados OTRS da CSTIC, dando prosseguimento da notificação para a triagem.

4.5 Triagem (Verificação)

Uma triagem (verificação) será realizada para confirmar se o evento reportado é um incidente de SI e se está dentro do escopo de tratamento da ETISI. O atendimento será negado caso o incidente não seja relativo a segurança da informação ou estiver fora do escopo da ETISI.

4.6 Classificação e priorização

Após o evento ser confirmado como de SI e dentro do escopo, a ETISI irá classificar e priorizar o incidente de SI de acordo com o esquema definido para tanto, tópico (5 Classificação Taxonomia) deste plano. A classificação e priorização do incidente serão feitas com base no relatório de registro do incidente. Logo, é deveras importante o preenchimento das informações quando da abertura do chamado, de forma a possibilitar a melhor classificação e priorização do incidente.

4.7 Plano de comunicação

O agente responsável pela ETISI reportará ao gestor de segurança da informação e comunicações sobre incidentes com prioridades 1 e 2, segundo as regras de priorização (Tópico 6), durante o processo de tratamento do incidente; para os demais casos deverá gerar um relatório com base nos registros do OTRS, trimestralmente.

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.

Quando houver indícios de ato ilícito, o agente responsável devera informar ao gestor de segurança da informação e comunicações, via e-mail, e encaminhar o chamado ao membro da ETISI da Superintendência de Segurança Institucional (SSI) para que o mesmo tome as providências cabíveis.

Trimestralmente, deverá ser gerado um relatório das lições aprendidas com os incidentes registrados no OTRS e encaminhado ao gestor de segurança.

4.8 Mobilização da equipe de tratamento (Grupo)

Os membros da ETISI estão distribuídos nas unidades organizacionais da UFPE, a saber: Superintendência de Tecnologia da Informação (STI), Centro de Informática (CIn), Hospital das Clinicas (HC), Centro Acadêmico de Vitória (CAV) e Centro Acadêmico do Agreste (CAA). Cada unidade citada atua operando um grupo de serviços, faixas de IP's e ativos específicos. Além das unidades citadas, a Superintendência de Segurança Institucional (SSI) também faz parte da ETISI. Observe-se que cada unidade é representada por um servidor titular e um suplente, no mínimo.

A depender do serviço/rede/ativo de TI afetado, o representante da ETISI, na unidade organizacional, para a qual o incidente foi reportado, acionará uma equipe de tratamento (grupo), de modo que as ações necessárias ao tratamento do incidente reportado sejam executadas. Saliente-se que a equipe de tratamento que atuará é formada a cada ocorrência, pois sua composição depende diretamente das áreas competentes a serem envolvidas para resolução do incidente em questão.

A ETISI poderá solicitar que um especialista de outra unidade atue junto à equipe de tratamento, caso esta não esteja apta para solucionar o incidente dentro do prazo acordado.

4.9 Investigação e diagnóstico

Esta é a fase de coleta e análise dos dados para a elaboração do diagnóstico do incidente. Para tanto, deve-se coletar dados de diversas fontes e utilizar técnicas de informação forense, quando necessário.

Inicia-se, então, a análise dos dados coletados, iniciando pelos mais relevantes. Saliente-se que as evidências coletadas devem ser armazenadas de forma segura.

4.10 Resposta ao incidente

A resposta ao incidente de SI envolve o desenvolvimento de procedimentos para avaliar e respondê-los a fim de restaurar os componentes e serviços do sistema afetados o mais breve possível.

Estratégias e procedimentos para responder a diferentes incidentes com diferentes recursos estão predeterminados no Manual de Tratamento de Incidentes e devem ser seguidos por todos os representantes das unidades organizacionais que compõem a equipe de tratamento.

Assim, a resposta ao incidente engloba três etapas subsequentes: Contenção, Erradicação e Recuperação, descritas a seguir:

4.10.1 Contenção

O primeiro estágio da resposta ao incidente é a contenção. Seu propósito é limitar o escopo, a magnitude e o impacto do incidente. As atividades, nesta etapa, podem incluir algumas ações, a saber:

- Realizar análise de impacto do incidente nos dados e sistemas de informação envolvidos para confirmar se os dados ou serviços foram danificados ou infectados.
- Proteger informações e sistemas críticos. Mover informações críticas para outras mídias, ou outros sistemas, que estão separados do sistema ou rede comprometida.
- Construir uma imagem do sistema comprometido para fins de investigação e como evidência para ação subsequente de acompanhamento.
- Verificar o comprometimento de quaisquer sistemas associados ao sistema comprometido por meio de serviços de rede ou outras relações de confiança.

4.10.2 Erradicação

Após a contenção, acontece a erradicação. Erradicar um incidente é remover sua causa raiz. Por exemplo, remover um *malware* de um sistema infectado.

Assim, de modo a evitar que informações importantes e necessárias sejam excluídas ou modificadas, recomenda-se que antes de remover qualquer arquivo ou parar/matar qualquer processo, deve-se coletar todos os arquivos de *log*, conexões e informações de status do processo, entre outras evidências que podem auxiliar na investigação do incidente.

4.10.3 Recuperação

A última etapa na resposta a incidentes de SI é a recuperação. Seu objetivo é restaurar o sistema, retornando ao seu funcionamento normal.

Saliente-se a importância, de antes de restabelecer o serviço/sistema, remover a fragilidade de segurança que causou o incidente em questão. Desta forma, as ameaças e riscos devem ser removidos antes do serviço/sistema ser restabelecido.

Deste modo, faz-se necessário, validar as correções com as áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade.

As tarefas que compõem esta etapa podem ser:

- Realizar reinstalação dos arquivos excluídos/danificados ou de todo o sistema, sempre que necessário, através de fonte confiável.
- Restabelecer os serviços por etapas, de maneira controlada, e na ordem demandada, por exemplo, os serviços mais essenciais ou aqueles que servem a maioria, podem retomar primeiro.
- Monitorar de forma a verificar se a operação de restauração foi bem-sucedida e que o sistema está de volta ao seu estado normal de operação.
- Desativar serviços desnecessários.

É relevante que a ETISI realize revisões periódicas para certificar que o incidente está sob controle, caso contrario, a equipe de tratamento não esteja conseguindo evoluir no tratamento, coordenar atividades de escalonamento.

4.11 Fechar incidente

O representante da ETISI, na unidade organizacional, para a qual o incidente foi reportado verificará se o incidente foi realmente resolvido. Caso não tenha sido resolvido, deverá ser escalonado novamente para a da equipe de tratamento (grupo).

No caso do incidente ter sido devidamente resolvido, o respectivo representante da ETISI deverá comunicar as partes envolvidas quanto a sua resolução. Também deve verificar se a classificação inicial está correta e, caso necessário, reclassificar o incidente. Após essas ações, ele deve arquivar os dados / evidências coletadas.

4.12 Pós-análise e lições aprendidas

A ETISI, juntamente, com a equipe de tratamento (grupo), na resolução do incidente deverá realizar uma pós-análise do incidente.

Uma pós-análise do incidente de SI deve ser realizada pela ETISI, juntamente, com a equipe de tratamento (grupo) que tratou o incidente, com vistas a:

- Avaliar os danos causados.
- Melhorar os procedimentos de resposta a incidentes SI.
- Melhorar as medidas de segurança para proteger sistemas/redes/ativos contra futuros ataques.
- Ajudar outras pessoas a se familiarizar com o processo de resposta a incidente de SI.

- Ajudar a educar as partes envolvidas sobre as lições aprendidas.
- Instaurar queixa-crime, nos casos cabíveis.

Ao final do incidente, deve-se produzir um relatório sobre o seu tratamento, registrando-o junto a ETISI.

Vale salientar que a realização de uma pós-análise do incidente deve estar relacionada com o nível de criticidade do incidente, podendo ser dispensada para incidentes menos críticos ou cujo tratamento já seja conhecido pela ETISI.

5 Classificação taxonomia

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

Classificação (Tipo)	Exemplos (Sub-Tipo)	Descrição
Conteúdo abusivo	SPAM	"E-mail em massa não solicitado", isso significa que o destinatário não concedeu permissão para que a mensagem seja enviada e que a mensagem foi enviada como parte de um grupo maior de mensagens, todas tendo o mesmo conteúdo.
	Denegrir imagem	Desclassificar ou discriminar alguém (por exemplo, *cyber stalking*, racismo e ameaças contra um ou mais indivíduos).
	Pedofilia / Sexual / Violência	Pornografia infantil, glorificação da violência.
Código malicioso	Vírus	Software que é incluído intencionalmente ou inserido em um sistema com um propósito prejudicial. Uma interação do usuário é normalmente necessária para ativar o código.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
	Ransomware	
Coleta de informações	Scanning	Ataques que enviam solicitações a um sistema para descobrir pontos fracos.
	Sniffing	Observar e registrar o tráfego de rede.
	Engenharia Social	Coletar informação de um ser humano por maneiras sociais.
Tentativa de intrusão	Explorar vulnerabilidades conhecida	Uma tentativa de comprometer um sistema ou de interromper qualquer serviço, explorando vulnerabilidades com um identificador padronizado, como o nome CVE (por exemplo, estouro de buffer, backdoor, script entre sites, etc.).
	Tentativa de login	Várias tentativas de login (adivinhação/ quebra de senhas, força bruta).
	Nova assinatura de ataque	Tentativa usando uma exploração desconhecida.

Intrusão	Comprometimento de conta privilegiada	Um comprometimento bem sucedido de um sistema ou aplicativo (serviço). Isso pode ser causado remotamente por uma vulnerabilidade conhecida ou nova, mas também através de uma conta não privilegiada, um acesso local não autorizado. Também inclui fazer parte de um botnet.
	Comprometimento de conta não privilegiada	
	Comprometimento de aplicação	
	Bot	
Disponibilidade	DoS	Por este tipo de ataque, um sistema é bombardeado com tantos pacotes que as operações são atrasadas ou o sistema trava.
	Ddos	
	Interrupção (não maliciosa)	Quando um sistema para, é interrompido de forma não maliciosa.
Segurança de conteúdo da informação	Acesso não autorizado da informação	Acesso não autorizado a uma informação restrita.
	Modificação não autorizada da informação	Modificação de um dado sem autorização necessária.
Fraude	Uso não autorizado de recursos	Uso de recursos para fins não autorizados, incluindo eventos com fins lucrativos (por exemplo, o uso de e-mail para participar de cartas de cadeia de lucro ilegais ou esquemas de pirâmide).
	Direito autoral	Oferecer ou instalar cópias de software comercial não licenciado ou outros materiais protegidos por direitos autorais.
	Phishing	Se passar por uma outra entidade, a fim de convencer o usuário a revelar uma credencial privada.
	Masquerade	Tipo de ataques em que uma entidade ilegitimamente assume a identidade de outra para se beneficiar dela.
Vulnerabilidade	Aberto por abusos	Resolvers abertos, impressoras vistas por todo o mundo, vulnerabilidade aparente do Nessus varreduras, assinaturas de vírus não atualizadas, etc.
Outra	Todos os incidentes que não cabem em uma das categorias acima, devem ser classificados nesta classe.	Se o número de incidentes nesta categoria aumenta, é um indicador de que o esquema de classificação deve ser revisado.

6 Regras de priorização

Pretende-se, em médio prazo que a priorização atribuída ao incidente de SI a ser tratado pela ETISI reflita os acordos de nível de serviço firmados entre a ETISI, as diretorias da STI e suas respectivas coordenações, e as equipes de tratamento dispostas no Cin, CAV, CAA e HC. Assim, deverá independer do nível de priorização definido na abertura da notificação do incidente pela CSTIC.

No momento, a priorização vem sendo definida na abertura do chamado pela CSTIC, podendo ser modificada pela ETISI.

Nesse modelo, os níveis de prioridade variam de um a cinco, sendo um o mais crítico e cinco o menos crítico.

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

IMPACTO	URGÊNCIA		
	BAIXA	MÉDIA	ALTA
ALTO	3	2	1
MÉDIO	4	3	2
BAIXO	5	4	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 na perda de prazos legais ou no funcionamento de atividades críticas administrativas ou acadêmicas da instituição; o incidente causa impacto negativo na imagem institucional; o incidente causa indisponibilidade em um ou mais equipamentos, serviços ou sistemas críticos da instituição; o incidente compromete o bom funcionamento dos serviços de TI e ocorre em momento crítico da instituição, por exemplo, período de matrícula de alunos, eventos, lançamento de notas, avaliação de órgãos financiadores etc.; o incidente impede o funcionamento de uma unidade organizacional; o incidente afeta usuários classificados como especiais pela STI (reitor, superintendentes, pró-reitores, entre outros).
- 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 UFPE;
- BAIXO: O incidente de SI pode ser tratado posteriormente, por necessidade do responsável; o serviço ou sistema afetado pelo incidente continua funcionando, porém em modo contingência; o incidente de SI 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 seguir, a classificação dos 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.

7 Revisão do documento

Este plano deverá ser revisado e atualizado a cada dois anos, a contar da sua vigência ou quando a ETISI considerar necessário.