PS_GESI Gerenciar Incidentes de Segurança da Informação

Bizagi Modeler

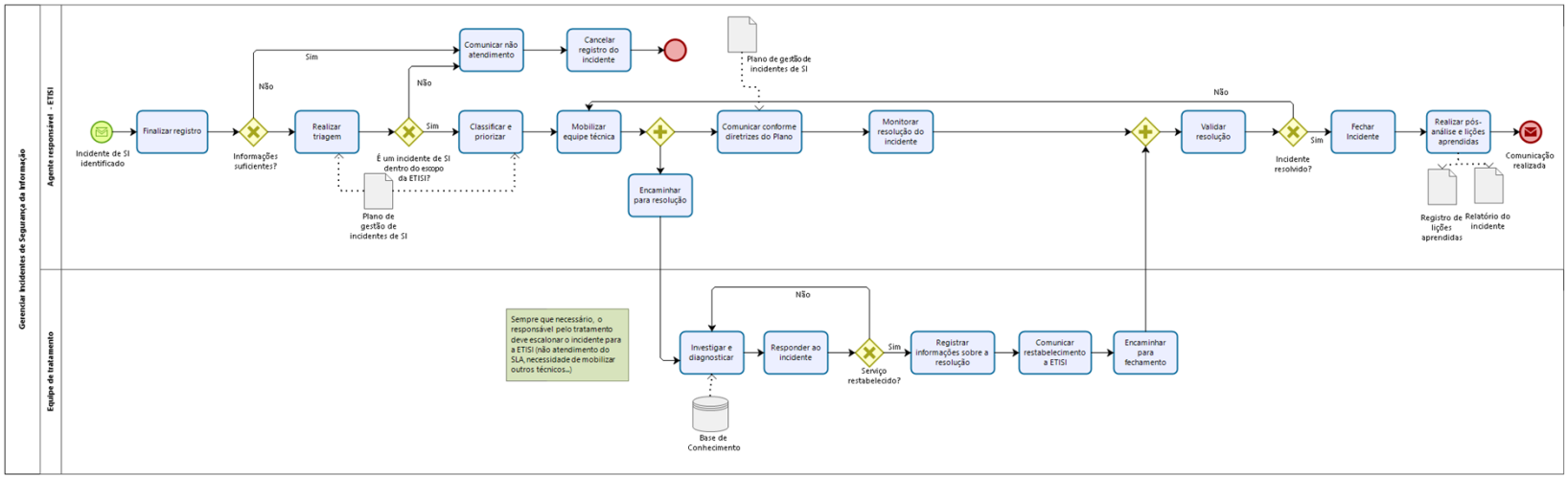
Índice

1 Gerenciar Incidentes de Segurança da Informação

Gerenciar Incidentes de Segurança da Informação

Autor: Daniel F. Arcoverde / Revisor: André S. S. Afonso
Versão: 30/07/2021
Descrição: Fluxo que descreve as atividades voltadas para o gerenciamento dos incidentes de segurança da informação.

UNIVERSIDADE FEDERAL DE PERNAMBUCO



Versão:

30/07/2021

Autor:

Daniel F. Arcoverde / Revisor: André S. S. Afonso

Descrição

Fluxo que descreve as atividades voltadas para o gerenciamento dos incidentes de segurança da informação.

1.1 Gerenciar Incidentes de Segurança da Informação

Finalidade

Promover o tratamento de incidentes de SI que afetem os ativos e sistemas de informação da UFPE, por meio de respostas padronizadas e eficazes.

Dono do processo

Coordenador de Segurança da Informação e Proteção de Dados

Termos e definições

Termo / Sigla	Definição
ETISI	Equipe de Tratamento de Incidentes de Segurança da Informação
SGIS	Sistema de Gestão de Incidentes de Segurança
CAIS	Centro de Atendimento de Incidente de Segurança
RNP	Rede Nacional de Pesquisas

Atores

Ator	Responsabilidade
Equipe de tratamento	Especialista responsável por receber, realizar a triagem, mobilizar e acompanhar a equipe de tratamento e responder às notificações e atividades relacionadas a incidentes de segurança da informação no ambiente da Universidade Federal de Pernambuco.
Agente responsável da	Especialista responsável por receber, realizar a triagem, mobilizar e acompanhar a equipe de tratamento e responder às notificações e atividades relacionadas a

ETISI	incidentes de segurança da informação no ambiente da Universidade Federal de Pernambuco.

Indicadores de desempenho

Tipo	Indicador	Descrição	Meta	Fórmula de cálculo	Periodicidade
Indicador de resultado (outcome)	Percentual de resolução de incidentes de SI identificados no SGIS.	Indicador que mede a capacidade em tratar e resolver os incidentes relacionados à Segurança da Informação na UFPE, registrados no SGIS, em um dado período de tempo.	Não definida	Número de incidentes de SI resolvidos no período / Número de incidentes de SI notificados no período. Fonte de coleta: SGIS	Mensal
Indicador de resultado (outcome)	Número de incidentes resolvidos no SGIS.	Indicador que mede o total de incidentes registrados como resolvidos no SGIS, em um dado período de tempo.	Não definida	Número de incidentes resolvidos no SGIS no período de tempo. Fonte de coleta: SGIS	Mensal
Indicador direcionador (driver)	Percentual de resolução de incidentes de SI registrados no OTRS	Indicador que mede a capacidade em tratar e resolver os incidentes relacionados à Segurança da Informação na UFPE, registrados no OTRS, em um dado período de	100%	Número de incidentes de SI resolvidos no período / Número total de incidentes de SI notificados no período.	Mensal

		tempo.			
Indicador direcionador (driver)	Número de incidentes notificados no SGIS	Indicador que mede o total de incidentes registrados como resolvidos no SGIS, em um dado período de tempo.	Não definida	Número de incidentes notificados no SGIS no período de tempo.	Mensal

Documentos reguladores

Documento / normativo	Descrição
Resolução Nº 01/2017 POSIC/UFPE	Política de Segurança da Informação e Comunicações
NC 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal
Plano de Gestão de Incidentes de Segurança da Informação	Plano de Gestão de Incidentes de Segurança da Informação

Equipe de elaboração

Integrantes
André Souto Soares Afonso
Daniel de França Arcoverde
Maria Betânia Martins da Silva
Pedro Correa de Araújo Neto

Xerxes Lins

1.1.1 Elementos do processo

1.1.1.1 *Incidente de SI identificado*

Descrição

O processo tem início com a identificação de um incidente de SI. O agente responsável pode tomar conhecimento sobre o evento de inúmeras formas.

1.1.1.2 *Finalizar registro*

Descrição

A ETISI, ao receber uma notificação, deverá verificar se as informações fornecidas estão completas e no padrão acordado. Caso, não, deverá entrar em contato com o relator do incidente para complementar as informações e finalizar o registro do incidente no sistema de gestão.

Caso os dados coletados não sejam suficientes para dar continuidade ao atendimento, a ETISI comunica ao relator sobre a não possibilidade do atendimento e cancela o registro da notificação.

Entrada

Notificação do incidente

Saída

Registro do Incidente

1.1.1.3 *Realizar triagem*

Descrição

Registrar o incidente de SI criando um chamado no OTRS
- Fila -> Segurança da Informação
- Proprietário -> Agente responsável pela ETISI
- Cliente interno -> Agente responsável pela ETISI

1.1.1.4 *Classificar e priorizar*

Descrição

A ETISI, após analisar os dados coletados no registro do incidente, realiza a classificação e a priorização do incidente de acordo com o modelo de classificação e a matriz de priorização de incidentes de SI, conforme definido no Plano de Gestão de Incidentes de Segurança da Informação.

1.1.1.5 ☐ *Mobilizar equipe técnica*

Descrição

A ETISI, de acordo com o escopo e tipo do incidente, define a equipe de tratamento e notifica os envolvidos que irão trabalhar cooperativamente no tratamento do incidente.

1.1.1.6 ☐ *Encaminhar para resolução*

Descrição

A ETISI escalona o chamado para a equipe de tratamento responsável pela resolução do incidente.

1.1.1.7 ☐ *Investigar e diagnosticar*

Descrição

Investigação e diagnóstico do que deu errado. Todas as atividades (incluindo detalhes de qualquer ação tomada para tentar resolver ou recriar o incidente) devem ser totalmente documentadas no registro do incidente para que o histórico completo de todas as atividades seja mantido durante todo o tempo.

A investigação inclui ações para:
- Estabelecer exatamente o que deu errado ou o que o usuário está solicitando
- Entender a ordem cronológica dos eventos
- Confirmar o impacto total do incidente, incluindo o número e a gama de usuários afetados
- Identificar algum evento que pode ter iniciado o incidente (ex. mudança recente, alguma ação do usuário, etc.?)
- Utilizar a base de conhecimento para procurar por ocorrências prévias do incidente, fazer pesquisas por erros conhecidos, registros de incidentes parecidos etc...)

1.1.1.8 ☐ *Responder ao incidente*

Descrição

A equipe de tratamento executará ações de acordo com o Plano de Respostas a Incidentes de SI para a contenção, erradicação e recuperação do incidente.

1.1.1.9 ☐ *Registrar informações sobre a resolução*

Descrição

Atualizar a base de conhecimento e outros documentos próprios para isso, documentando, neles, as informações sobre a resolução.

1.1.1.10 ☐ *Comunicar restabelecimento a ETISI*

Descrição

Informar a ETISI que o serviço foi restabelecido. Os usuários já podem voltar a usar o serviço normalmente.

1.1.1.11 ☐ *Encaminhar para fechamento*

Descrição

A equipe de tratamento encaminha o incidente para a ETISI onde será realizado o fechamento do mesmo.

1.1.1.12 ☐ *Validar resolução*

Descrição

O agente responsável da ETISI verifica se o incidente foi resolvido e se os serviços foram restabelecidos. Verifica também se todas as informações necessárias durante o tratamento foram devidamente registradas e se as evidências foram armazenadas nos locais indicados de acordo com a política de arquivamento (se houver).

1.1.1.13 ☐ *Fechar Incidente*

Descrição

A ETISI verifica se a classificação inicial corresponde ao que realmente foi tratado. Caso necessário, o incidente deve ser reclassificado. Após, fechar o registro do incidente, comunica a resolução aos envolvidos (quando necessário) e libera o registro para a pós-análise e lições aprendidas.

1.1.1.14 ☐ *Realizar pós-análise e lições aprendidas*

Descrição

A ETISI juntamente com os envolvidos com a resolução do incidentes deverá realizar uma pós-análise do incidente.

Ações de pós-análise visam:
• Avaliar os danos causados.
• Melhorar os procedimentos de resposta a incidentes.
• 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 incidentes de segurança.
• Ajudar a educar as partes envolvidas sobre as lições aprendidas.
• Instaurar queixa-crime, nos casos cabíveis.

Deve-se produzir ao final do incidente um breve relatório sobre o seu tratamento, registrando-o junto a ETISI-UFPE.

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

1.1.1.15 ☐ *Comunicar conforme diretrizes do Plano*

Descrição

Definir a periodicidade dos comunicados e reportar o andamento a clientes, equipe mobilizada e a CSIPD, quando necessário.

1.1.1.16 ☐ *Monitorar resolução do incidente*

Descrição

Verificar o andamento da resolução do incidente e produzir relatórios de acompanhamento, quando necessário.

1.1.1.17 ☐ *Comunicar não atendimento*

Descrição

Notificar o reclamante sobre a impossibilidade do atendimento, informando o motivo (informação insuficiente ou incidente fora do escopo de tratamento).

1.1.1.18 ☐ *Cancelar registro do incidente*

Descrição

Devido à impossibilidade do atendimento, a ETISI deve cancelar o registro do incidente.

1.1.1.19 *Comunicação realizada*

Descrição

O processo encerra com o envio de comunicação, sobre a resolução, às partes interessadas.