Plano de Gestão de Incidentes de Segurança da Informação e Privacidade

Versão 1.1 - 29/03/2021

1. INTRODUÇÃO 2
2. OBJETIVO 2
3. ABRANGÊNCIA 2
4. CONCEITOS E DEFINIÇÕES 2
5. ATORES 3
6. NOTIFICAÇÃO DE INCIDENTES 3
   6.1. INCIDENTES DE PRIVACIDADE DE DADOS 3
   6.2. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 4
7. PADRÕES DE NOTIFICAÇÃO 4
8. REGISTRO DO INCIDENTE 5
9. TRIAGEM DO INCIDENTE 5
10. CLASSIFICAÇÃO DO INCIDENTE 6
11. CRITICIDADE DO INCIDENTE 6
12. SITUAÇÃO DO INCIDENTE 6
13. PRESERVAÇÃO DE EVIDÊNCIAS 7
14. PROCESSO DE MITIGAÇÃO DO INCIDENTE 7
15. FECHAMENTO DO INCIDENTE 8
   15.1. RECOMENDAÇÕES E RESPOSTA AO INCIDENTE 8
   15.2. LIÇÕES APRENDIDAS 8
16. ARTEFATOS RELACIONADOS 9

1. INTRODUÇÃO

O processo de tratamento de incidentes de segurança e privacidade consiste na implementação de procedimentos e etapas bem definidas que conduzirão a equipe para a resolução de um incidente. O conjunto de etapas definidas permite determinar um fluxo lógico especificando ações a serem realizadas nas diferentes etapas do processo. **Este documento complementa a "Avaliação e Plano de Tratamento dos Riscos de TI"** (cigov.ufla.br/controle/gestao-de-riscos).

Portanto, este plano descreve um processo para responder às situações de emergência, ou evento de risco, que venham ocasionar em algum impacto aos ativos mantidos pela Universidade Federal de Lavras. Desta forma, o documento enaltece os passos necessários para uma resposta ágil e precisa, atendendo as exigências legais de comunicação e transparência para segurança da informação e privacidade.

2. OBJETIVO

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

3. ABRANGÊNCIA

Este plano abrange todos os recursos computacionais pertencentes, operados, mantidos e controlados pela UFLA.

4. CONCEITOS E DEFINIÇÕES

- **ataque:** Evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
- ***bot***: Código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;
- **GMT**: *Greenwich Mean Time*, ou Horário Médio de Greenwich, baseado no primeiro meridiano de Greenwich, que passa pelo Observatório Real, perto de Londres.
- **IP**: Protocolo da Internet (*Internet Protocol*), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- **log**: Processo de registro de eventos relevantes num sistema computacional;
- **porta**: Programa de computador específico ou processo específico servindo de ponto final de comunicação em um sistema operacional hospedeiro de um outro dispositivo.
- ***scripts***: conjunto de instruções para que uma função seja executada em determinado aplicativo;
- **SLA**: Acordo de Nível de Serviço (do inglês *Service Level Agreement*);
- ***spam***: Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
- ***spyware***: Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
- ***trojan***: Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;
- **vírus**: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
- ***worm***: Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

5. ATORES

- **Gestor da área de Segurança da Informação**: responsável pelas ações de segurança da informação e comunicações na organização.
- **Coordenador da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais**: responsável por gerenciar os membros e as atividades da equipe de resposta a incidentes.
- **Encarregado de Dados**: 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).
- **Ponto de contato**: responsável estratégico pela comunicação e ponto focal de contato da equipe de resposta a incidentes com outros setores da organização ou grupos externos.
- **Administrador de Infraestrutura Computacional**: profissional com conhecimento em sistemas operacionais e suas aplicações, responsável por instalar, configurar, suportar e manter servidores e outros sistemas.
- **Administrador de banco de dados**: responsável por gerenciar, instalar, configurar, atualizar e monitorar um banco de dados ou sistemas de banco de dados.
- **Administrador de redes de dados e comunicações**: responsável por projetar e manter uma rede de computadores em funcionamento, gerenciando a rede local e os recursos computacionais e ativos a ela relacionados, direta ou indiretamente.

6. NOTIFICAÇÃO DE INCIDENTES

6.1. INCIDENTES DE PRIVACIDADE DE DADOS

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

Encarregado pelo tratamento de dados pessoais da UFLA:
Reginaldo Ferreira de Souza
Telefone: (35) 2142-2176
E-mail: rfsouza@ufla.br

Endereço:
Prédio da Reitoria
Câmpus Universitário
Caixa Postal 3037
CEP 37200-900 - Lavras – MG

Para incidente 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).

6.2. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Quanto às notificações de incidentes de segurança da informação, serão utilizados dois meios de comunicação institucional: (1) o primeiro meio possibilita o registro da notificação por um informante externo, ou um informante interno à UFLA; (2) o segundo meio pode ser utilizado por uma pessoa com vínculo ativo com a UFLA.

1º - Canal para o informante externo, ou informante interno à UFLA:

Equipe Responsável: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) **Telefone:** +55(35)3829-1512 **E-mail:** etir@ufla.br **Site:** https://www.etir.ufla.br

2º - Canal para pessoa com vínculo ativo com a UFLA:

Serviço gerenciador de serviços de tecnologia da Informação (GLPI) **Endereço do sistema:** https://servicosti.ufla.br **Caminho no sistema**: "**Segurança da Informação**" >> "**Notificações de Problemas de Segurança**" >> "**Relatar Problemas de Segurança**"

7. PADRÕES DE NOTIFICAÇÃO

Ao se registrar uma notificação de incidente de segurança da informação e privacidade, devem-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;

8. REGISTRO DO INCIDENTE

Utilização do software de registro de chamadas de suporte técnico GLPI para registrar e catalogar o incidente (glpi.ufla.br). O incidente é documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

9. TRIAGEM DO INCIDENTE

O objetivo do processo de triagem é reunir informações sobre o incidente, avaliar a sua natureza, e classificá-lo como incidente para que, adiante, se inicie o processo de tratamento.

Fluxograma: "**Incidente não classificado**" >> "**Triagem do Incidente**" >> "**Classificar tipo de Incidente**" >> "**Definir Criticidade**" >> "**Alterar Situação do Incidente**" >> "**Incidente Classificado**".

10. CLASSIFICAÇÃO DO INCIDENTE

Classificar o incidente deixa claro o tipo de atendimento requerido e ajuda a definir sua criticidade.

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.

11. CRITICIDADE DO INCIDENTE

Definir uma ordem de atendimento dos incidentes e um SLA de acordo com a urgência de tratamento e o impacto nas áreas de negócio da UFLA. Determinar a classificação de criticidade do incidente de acordo com as classificações:

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.

12. 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. O fechamento pode ocorrer automaticamente ou por contato.

13. 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.

14. PROCESSO DE MITIGAÇÃO DO INCIDENTE

1. **Preparação:** gerenciar as ferramentas para análise de incidentes, incluindo o conhecimento de todo o ambiente utilizado;
    a. Implementar mecanismos de defesa e controle de ameaças;
    b. Desenvolver procedimentos para lidar com incidentes de forma eficiente;
    c. Obter recursos e equipe necessária para lidar com os problemas;
    d. Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.
2. **Detecção:** detectar o incidente, determinar o escopo e as partes envolvidas com o incidente;
    a. Identificar todos os sistemas e serviços afetados relacionados com o incidente;
    b. 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);
    c. Identificar a existência de outros eventos e alertas relacionados com o incidente em questão;
    d. Identificar que tipo de informação e processos podem ter sido afetados;
    e. Identificar os responsáveis pelo sistema comprometido, equipes de suporte e donos das informações.
3. **Contenção:** conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos.
    a. Desconectar o sistema comprometido ou isolar a rede afetada;
    b. Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque;
    c. Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso;
    d. Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas.
4. **Erradicação:** eliminar as causas do incidente, removendo todos os eventos relacionados.
    a. Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;
    b. 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.
5. **Recuperação:** restaurar o sistema ao seu estado normal.
    a. Caso exista Plano de Continuidade de Negócio dos serviços impactados, eles devem ser iniciados, conforme especificado no respectivo plano.
    b. Restaurar a integridade do sistema;
    c. Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas;
    d. Implementar medidas de segurança para evitar novos comprometimentos;
    e. Restauração do último e íntegro backup completo armazenado.
6. **Avaliação:** avaliar as ações realizadas para resolver o incidente, documentando detalhes, e discutir lições aprendidas.

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

15. FECHAMENTO DO INCIDENTE

15.1. RECOMENDAÇÕES E RESPOSTA AO INCIDENTE

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.

15.2. LIÇÕES APRENDIDAS

Consiste em se avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas. Devem-se relacionar e documentar no chamado do incidente as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões. A partir da mitigação do incidente e sua resolução, deve ser conduzido o apanhado de lições aprendidas, com outros atores se necessário, com o objetivo de discutir erros e dificuldades encontradas na mitigação do evento ocorrido, propor melhoria na infraestrutura computacional e para os processos de resposta a incidentes.

A área afetada deve ser comunicada das decisões tomadas para prevenção de incidentes da mesma natureza, caso se tenha consenso de implementar melhorias na infraestrutura de segurança.

16. ARTEFATOS RELACIONADOS

- Avaliação e Plano de Tratamento dos Riscos de TI: https://docs.google.com/spreadsheets/d/e/2PACX-1vTQlbn3JLQzfgMhW2STP51Ar-f7MK3zBwPO8H7o3f4X9KkT1pin-idAyvNxY56ZFkTAQdedLdQ2BEg6/pubhtml
- Política Geral de Proteção de Dados Pessoais da Universidade Federal de Lavras (publicada na Portaria Nº 1.896, de 23 de dezembro de 2020): https://sistemaslegados.ufla.br/documentos/arquivos/21_1896_23122020.pdf
- Política de Segurança da Informação e Comunicações da Universidade Federal de Lavras (publicada na portaria Nº 1.327, de 13 de novembro de 2019): https://sistemaslegados.ufla.br/documentos/arquivos/21_1327_13112019.pdf

SERPRO
Assinado digitalmente por:
ERASMO EVANGELISTA DE OLIVEIRA
Sua autenticidade pode ser confirmada no endereço :
<http://www.serpro.gov.br/assinador-digital>

ERASMO EVANGELISTA DE OLIVEIRA

Diretor de Gestão de Tecnologia da Informação