POLÍTICA DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. Objetivos

Assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de informação da UFSM.

2. Escopo

- Denúncia de host como origem de vírus;
- Denúncia de host como origem de spam;
- Denúncia de violação de direitos autorais;
- Denúncia de atividade maliciosa ou ilegal.

3. Base normativa

Esta política foi elaborada com base na ABNT NBR-ISO/IEC-27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos e na ABNT NBR-ISO/IEC-27002 – Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão de segurança da informação.

4. Procedimento

O procedimento padronizado para o tratamento de incidentes de segurança compreende as seguintes etapas:

- Recepção da denúncia ou alerta interno de atividade suspeita
- Medidas de contenção imediata do incidente
- Coleta de informações e evidências
- Análise das informações e evidências
- Notificação dos envolvidos
- Análise crítica e medidas corretivas

4.1 Recepção da denúncia ou alerta interno de atividade suspeita

Serão aceitas denúncias e a UFSM investigará e tomará ações corretivas sobre as denúncias realizadas pelo Centro de Atendimento a Incidentes de Segurança – CAIS da Rede Nacional de Pesquisa, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT-BR e seus colaboradores sobre atividade suspeita proveniente da rede UFSM.

Serão aceitas denúncias e a UFSM colaborará plenamente com a polícia e entidades legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede UFSM.

Serão investigados os alertas provenientes dos sistemas de monitoramento da rede UFSM, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com a **Política de uso aceitável da rede UFSM**.

Serão aceita denúncias de pessoas físicas ou entidades públicas ou privadas vítimas de atividade suspeita proveniente da rede UFSM, quando devidamente evidenciadas.

4.2 Medidas de contenção imediata do incidente

A contenção imediata do incidente se fará por meio de bloqueio de acesso do host envolvido à rede UFSM até o término da investigação.

4.3 Coleta de informações e evidências

Serão coletadas informações e evidências sobre as atividades denunciadas através dos logs dos diversos sistemas e serviços disponíveis na rede UFSM.

4.4 Análise das informações e evidências

Todas as informações e evidências serão analisadas para investigar o host que gerou o incidente denunciado. A identificação do host compreenderá a determinação do seu endereço IP e endereço MAC da interface de rede, nome, switch e porta de acesso, bem como prédio, departamento, sala e usuário, se possível.

O tipo de atividade será determinado pelas informações evidenciadas em logs de serviços. As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

4.5 Notificação dos envolvidos

Será encaminhada notificação por escrito da atividade denunciada ou sob investigação à direção do centro onde se situa o host envolvido. Cabe ao responsável pelos usuários da máquina alvo de investigação a determinação da origem da atividade, com sua adequada comprovação.

Como origem pode-se considerar:

- Atividade realizada pelo usuário;
- Atividade realizada por terceiro com autorização do usuário;
- Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Como evidência da origem da atividade pode-se considerar:

- Logs de acesso local ou remoto da máquina;
- Logs de detecção de vírus, spyware, malware, etc.;
- Outras informações que possam identificar claramente a origem da atividade.

O centro notificado deverá responder a notificação por escrito, com a comprovação da origem da atividade e as medidas administrativas tomadas para evitar reincidência do usuário.

4.6 Análise crítica e medidas corretivas

O CPD/UFSM avaliará a resposta do centro responsável e determinará as medidas corretivas no host identificado. Nos casos comprovados de invasão, o host permanecerá bloqueado até a implantação das medidas corretivas apresentadas. Nos casos de atividade maliciosa de usuário, o host permanecerá bloqueado por 30 dias, sem prejuízo das medidas administrativas tomadas pelo centro responsável.

Em caso de reincidência de atividade mal-intencionada no host identificado, o mesmo permanecerá bloqueado por 90 dias, sem prejuízo do processo de tratamento de incidentes definido neste documento.

Se ocorrer nova reincidência após o bloqueio de 90 dias, o host perderá definitivamente o acesso direto externo, passando a receber endereço IP da rede interna e acessando a internet indiretamente através de Proxy.

5. Contato para denúncia

O CPD/UFSM seguirá as orientações e colaborará com as atividades do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP) em relação ao uso e divulgação de conteúdo na Internet. Para mais informações sobre o CAIS e suas políticas específicas consultar **http://www.rnp.br/cais**.

Qualquer reclamação em relação à utilização ilícita ou questões de segurança do sistema ou da rede, uso indevido de correio eletrônico, spamming, violação de direitos autorais

ou qualquer atividade em desacordo com esta política devem ser enviadas a **abuse@ufsm.br** com a devida comprovação da atividade.

6. Disposições finais

O CPD/UFSM reserva o direito de revisar esta política periodicamente para adaptá-la às necessidades mais atuais de segurança de sistemas de informação.