SECUTITY.UFRJ.BR

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

DIRETORIA DE SEGURANÇA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

UFRJ TIC
Superintendência de Tecnologia da Informação e Comunicação

Segurança da Informação UFRJ

Universidade Federal do Rio de Janeiro – UFRJ

Denise Pires de Carvalho

Reitora

Superintendência de Tecnologia da Informação e Comunicação

Augusto Cesar Gadelha Vieira

Superintendente

Diretoria de Segurança da Informação - SegTIC

Felipe Ribas Coutinho

Diretor

Equipe SegTIC

Aline Nery

Daniel Leonardo

Gabriel Rodrigues Caldas de Aquino

Lilian Chagas

Patricia do Amaral Gurgel

Robert Sachsse

Roberta Bordalo

Zeus Olenchuk

Sumário

1. Apresentação

A Diretoria de Segurança da Informação (SegTIC), subordinada à Superintendência de Tecnologia da Informação e Comunicação (STIC), tem como missão atuar na detecção, resolução, prevenção e redução da ocorrência de incidentes de segurança da informação na Universidade Federal do Rio de Janeiro, proporcionando um ambiente cada vez mais confiável, disponível e íntegro.

Para assegurar sua missão é fundamental que se faça a gestão dos incidentes de forma adequada, eficiente e eficaz, a fim de proteger a informação contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

2. Objetivo

O objetivo do plano é apresentar o processo de Tratamento e Resposta a Incidentes da Segurança da Informação executado pela SegTIC, alinhado com a portaria nº 7.252, publicada no Boletim da UFRJ - Extraordinário - 3ª parte, sob o nº 30, de 31 de julho de 2018. A portaria institui e regulamenta o funcionamento do Time de Resposta, Orientação e Tratamento de Incidentes (TROTI), na rede computacional da Universidade Federal do Rio de Janeiro (UFRJ).

Neste documento, estão contempladas as diretrizes para gerenciamento de incidentes em redes computacionais, estabelecidas pela Norma Complementar nº 08/IN01/DSIC/GSIPR, publicada no Diário Oficial da União, em 23/08/2010, bem como estão contempladas as ações necessárias ao atendimento de incidentes de segurança envolvendo dados pessoais, conforme

previsto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD). Além das boas práticas recomendadas pela European Union Agency for Cybersecurity (ENISA).

3. Conceitos e definições

Neste documento serão adotados os conceitos e definições descritos na portaria nº 93, de 26 de setembro de 2019, publicada no Diário Oficial da União.

4. Processo de Tratamento de Incidentes da Segurança da Informação

O processo de Tratamento e Resposta de Incidentes da Segurança da Informação tem o objetivo de atender as notificações de incidentes de segurança da informação detectados na UFRJ.

Havendo ocorrência ou suspeita de incidente de segurança da informação, a SegTIC deverá ser comunicada imediatamente, através dos Canais de Comunicação:

a. Por envio de e-mail: abuse@ufrj.br; atendimento@tic.ufrj.br; ri@tic.ufrj.br;

b. Pela página eletrônica da SegTIC: security.ufrj.br;

c. Por abertura de chamado através do Sistema de Gerenciamento de Chamados (osTicket): suporte.tic.ufrj.br;

As comunicações de incidente deverão conter informações de identificação do usuário, salvo as reportadas de forma anônima, que podem ser feitas somente através da página eletrônica da SegTIC. É fundamental que seja feita uma descrição detalhada da ocorrência, para melhor atender ao chamado.

A STIC disponibiliza os diagramas de processos de negócio de suas diretorias em sua página eletrônica. Para visualizar este e outros processos da SegTIC, acesse: https://tic.ufrj.br/processos/.

5. Ciclo de Vida do Incidente de Segurança da Informação

O processo de Tratamento e Resposta a Incidente de Segurança da Informação segue as etapas definidas na tabela Etapas do Ciclo de Vida do Incidente de Segurança da Informação (Tabela 01).

Informamos que, a descrição das atividades apontadas, podem ser encontradas no diagrama do processo. Conheça em: https://tic.ufrj.br//stic-modProc/SegTIC/TrataIncidSegInfo/index.html#list

ETAPAS DO CICLO DE VIDA DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO		
ETAPA	**DEFINIÇÃO**	**ATIVIDADES DO PROCESSO**
Notificação ou Detecção	Define os Canais de Comunicação (reativo) ou Meios de Monitoramento (proativo) pelos quais recebe-se as notificações dos incidentes	

Registro	Descreve como o incidente é registrado e a sua forma de rastreamento.	
Triagem e classificação	Descreve os requisitos para validação do incidente. Decisão rápida baseada em informações limitadas. O objetivo da triagem é categorizar, priorizar e atribuir um evento de informação ao pessoal apropriado. Define as identificações por tipo (tabela Taxonomia) e criticidade (SLA configurada) do Ticket. São levados em consideração os recursos afetados e o impacto às atividades críticas da Universidade. É capaz de identificar quais incidentes devem ser imediatamente atendidos ou não, inserindo-os em "Lista" apropriada. É finalizado com Incidente sendo encaminhado para tratamento.	- Validar Notificação - Categorizar Incidente - Verificar Necessidade de Alerta -Verificar Necessidade de Comunicação a Encarregada de Dados - Priorizar Incidente
Resolução	Define as ações que serão executadas para a mitigação e solução do incidente e o retorno à normalidade. É o tratamento em si.	- Verificar Criticidade - Analisar Informações - Solicitar Evidências - Verificar Viabilidade de Atendimento - Verificar Origem Incidente - Identificação de Responsável Técnico - Notificar Responsável

		Técnico - Conferir Resposta - Verificar Reincidência do Incidente - Analisar Resultado do Tratamento - Analisar Situação do Incidente - Identificar Tipo de Bloqueio - Solicitar Bloqueio IP Origem - Realizar Bloqueio E-mail - Verificar Retorno do Responsável - Validar Solução do Responsável - Avaliar Chamado - Identificar Solução - Aplicar Solução - Validar Solução - Verificar Situação do IP - Solicitar Desbloqueio
Fechamento	Define procedimentos para finalização do tratamento do incidente, quais ações devem ser realizadas ao se fechar o chamado, quem deve ser informado e quais informações devem estar contidas na resposta.	- Encerrar Notificação

Tabela 01: Etapas do Ciclo de Vida do Incidente de Segurança da Informação

6. Tipos de Incidentes

Todos os incidentes de segurança devem ser classificados conforme tabela de Taxonomia para a Classificação do Incidente (Tabela 02).

TAXONOMIA PARA A CLASSIFICAÇÃO DO INCIDENTE (BASEADO METODOLOGIA (ENISA))		
Categoria	**Tipo**	**Descrição ou Característica do Evento**
Conteúdo Abusivo	Spam	Envio de e-mails não solicitados pelo destinatário.
	Assédio / Discriminação	Envio de e-mails ou acesso a conteúdos relacionados à difamação, assédio, discriminação, entre outros proibidos por lei.
	Difamação	
	Pornografia	
	Pedofilia	
Código Malicioso	Bot	Códigos maliciosos infectando sistemas, disponíveis para downloads, anexos a e-mails ou recebendo comandos.
	Worm	
	Vírus	
	Trojan	
	Spyware	
	Scripts	
Pesquisa de Informações	Varredura	Envio de solicitações a sistemas para descobrir vulnerabilidades, configurações ou serviços. Abrange processos de testes não solicitados (scans em rede de dados).
	Escuta não autorizada	Monitorar ou gravar tráfego de rede sem autorização (sniffing).
	Phishing	Obter informações sigilosas de pessoas se utilizando de manipulação, confiança e/ou boa fé.

Tentativa de Intrusão/Invasão	Tentativa de exploração de vulnerabilidades	Tentativas de comprometimento ou acesso a sistemas através de ataques que explorem vulnerabilidades (ex.: XSS, buffer overflow etc).
	Tentativa de login	Tentativas de acesso não-autorizado a contas de usuários em serviços ou mecanismos de autenticação, usando força bruta ou não.
Intrusão/Invasão	Comprometimento de conta do usuário	Intrusão efetiva, comprometendo sistema, componente ou rede, através de uma conta de usuário.
	Exploração de vulnerabilidade	Intrusão efetiva explorando uma vulnerabilidade num sistema, componente ou rede.
Indisponibilidade	Negação de Serviço	Tentativas ou sucesso na indisponibilização de serviços ou informações, esgotando a capacidade de processamento e resposta dos recursos de hardware, software ou rede.
	Sabotagem	Ação premeditada para danificar um sistema, interromper um processo, alterar ou eliminar informação na UFRJ.
Segurança da Informação	Acesso não autorizado	Ataques cuja finalidade é o acesso ou modificação não-autorizada de informação, sem envolver o comprometimento de sistemas (invasão, força bruta, indisponibilidade).
	Modificação não autorizada	
	Acesso à Darknet / DeepWeb	Acesso indevido à Darknet / Deepweb
Fraude	Violação de direitos autorais	Compartilhar conteúdo protegido por direitos de autor e direitos conexos
	Fingir ou falsificar identidade da UFRJ	Ataque onde a identidade da UFRJ é assumida ilegitimamente para obter qualquer tipo de informação, recurso ou vantagem.
	Uso de recursos de forma não autorizada	Utilização de recursos de forma não autorizada (correntes de e-mail, servidores de jogos etc)
Vulnerabilidades	DNS Recursivo Aberto	Serviço publicamente acessível.
Outros	Incidentes não categorizados	Incidentes não listados.

Tabela 02: Taxonomia para a Classificação do Incidente

7. Priorização do Incidente

Após a classificação do incidente, é definida a criticidade conforme tabela Nível de Criticidade (Tabela 03). Tais níveis definem a ordem de atendimento das notificações.

NÍVEL DE CRITICIDADE			
Nível	**Criticidade**	**Descrição**	**Acordo de Nível de Serviço - ANS**
1	Baixa	Incidentes com baixo impacto para a UFRJ, que possuem atuação restrita.	7 dias dias úteis, cada dia 8 horas úteis. (Prioridade Baixa)
2	Média	São eventos ou incidentes generalizados, mas com um pequeno impacto.	5 dias dias úteis, cada dia 8 horas úteis. (Prioridade Moderada)
3	Alta	Incidentes restritos a uma unidade com alto impacto nas operações da UFRJ.	3 dias dias úteis, cada dia 8 horas úteis. (Prioritário)
4	Muita Alta	Incidentes com impacto crítico ou que afetam múltiplas unidades da UFRJ. São eventos que requerem uma grande intervenção da SegTIC e com atuação de alta prioridade. Requer bloqueio de IP	1 dia útil, 8 horas úteis. (Prioritário)

Tabela 03: Nível de Criticidade

8. Análise Crítica

As boas práticas na literatura sugerem o controle das ações, no tocante a mensurar a efetiva atuação da prática. Dados estatísticos sobre incidentes de segurança contribuem para identificar oportunidades de melhorias nos processos de trabalho ou, até mesmo, novas ações de contenção e prevenção a incidentes.

Ciente desta premissa, a SegTIC gera relatórios com o total de atendimentos, periodicamente e de forma categorizada. Tais relatórios, podem ser acessados em: https://www.security.ufrj.br/nossos-numeros/

9. Referências

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 08, de 23 de agosto de 2010. Brasília, DF, GSI/PR, 2008. Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=24/08/2010&jornal=1&pagina=1&totalArquivos=144. Acesso em: 10 de maio de 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Portaria Nº 93 GSI/PR, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação. Disponível em: www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 10 de maio de 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 07 de julho de 2022.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (cert.br). Disponível em: www.cert.br . Acesso em: 10 de maio de 2021.

ENISA. Good practice guide for incident management. European Network and Information. Disponível em: www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. Acesso em: 10 de maio de 2021.

Histórico de Revisão

Revisão	Data	Descrição	Item Revisado	Autor
01	24/05/2021	Criação do Documento		Lilian Chagas Roberta Bordalo Patricia do Amaral Gurgel
02	27/05/2021	Validação		Felipe Ribas
03	16/06/2021	Atualização	Links que direcionam aos processos da SegTIC e ao processo de Tratamento de Incidente de SI	Lilian Chagas
04	28/09/2021	Atualização	Link que direciona para os gráficos de análise crítica	Lilian Chagas
05	01/07/2022	Atualização	Incluída a referência à LGPD e atividade Comunicar Encarrega de Dados no item: 5. Ciclo de Vida do Incidente de Segurança da Informação	Lilian Chagas
06	01/07/2022	Validação		Patrícia do Amaral Gurgel Roberta Bordalo