



UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
09/01/2025	1.0	Plano de Resposta a Incidentes	Vertical de Segurança



SUMÁRIO

HISTÓRICO DE VERSÕES.....	2
1. INTRODUÇÃO.....	4
2. OBJETIVO E ESCOPO.....	5
2.1. OBJETIVO.....	5
2.2. ESCOPO.....	5
3. REFERÊNCIA LEGAL E DE BOAS PRÁTICAS.....	5
4. CONCEITOS E DEFINIÇÕES.....	5
5. COMUNICAÇÃO.....	7
5.1. INTERNA.....	7
5.2. EXTERNA.....	7
6. GOVERNANÇA E ESTRUTURA ORGANIZACIONAL.....	8
6.1. ESTRUTURA DE GOVERNANÇA PARA RESPOSTA A INCIDENTES.....	8
6.2. CSTI.....	9
6.3. CSIRT.....	9
6.4. Papéis Específicos.....	9
7. TIPOS E VETORES DE INCIDENTES.....	9
7.1. VETORES DE AMEAÇA COMUNS.....	9
7.2. TIPOS DE INCIDENTES DE SEGURANÇA.....	10
8. CLASSIFICAÇÃO E PRIORIZAÇÃO DE INCIDENTES.....	10
8.1. NÍVEIS DE PRIORIDADE.....	10
8.2. CRITÉRIOS DE AVALIAÇÃO DE IMPACTO.....	11
9. PROCESSO DE GESTÃO DE INCIDENTES (Ciclo de Vida).....	11
9.1. FASE 1: PLANEJAR E PREPARAR.....	12
9.2. FASE 2: DETECTAR, INVESTIGAR E COMUNICAR.....	13
9.3. FASE 3: CONTENÇÃO, COLETA DE EVIDÊNCIAS E REMEDIAÇÃO.....	13
9.4. FASE 4: RECUPERAÇÃO E RELATÓRIO.....	13
9.5. FASE 5: LIÇÕES APRENDIDAS E MELHORIA.....	14
10. MATRIZ RACI.....	14
11. TREINAMENTO E SIMULAÇÕES.....	15
12. ANEXOS NORMATIVOS.....	15

1. INTRODUÇÃO

Este documento tem como objetivo atender o controle 7 do Framework CIS controls Versão 8.1 que estabelece:



Controle 17: Gestão de respostas – Estabelecer um programa para desenvolver e manter uma capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para preparar, detectar e responder rapidamente a um ataque.

As medidas do Controle 17 que estão contempladas por esta política são 17.1, 17.2, 17.3, 17.4, 17.5 e 17.6.

Esta Política está alinhada ao arcabouço normativo institucional de segurança da informação, gestão de riscos, privacidade e governança de TIC da Unesp, em especial à Política de Segurança Cibernética instituída pela Portaria Unesp nº 12, de 05 de fevereiro de 2025, bem como às legislações estadual e federal aplicáveis.

Considerando a crescente digitalização dos processos administrativos, acadêmicos e de pesquisa, bem como a dependência institucional de serviços tecnológicos essenciais, a Unesp reconhece que provedores externos de TIC representam elementos críticos para a continuidade operacional, a segurança da informação, a proteção de dados pessoais e a mitigação de riscos institucionais.

Nesse contexto, esta Política define requisitos obrigatórios de segurança, conformidade, gestão de riscos, monitoramento, auditoria e responsabilização aplicáveis aos provedores de serviços de TIC, com o objetivo de assegurar que tais serviços estejam em conformidade com os princípios de confidencialidade, integridade, disponibilidade, autenticidade, governança e responsabilidade, conforme estabelecido nas normas internas da Universidade.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no art.46. da Lei Geral de Proteção de Dados, sancionada em 14 de agosto de 2018:

“Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

2. OBJETIVO E ESCOPO

2.1. OBJETIVO

Garantir que a Unesp detecte, responda e se recupere de incidentes de segurança com rapidez e eficiência, preservando a continuidade do ensino, da pesquisa e da extensão, além dos serviços administrativos.

Este plano busca reduzir impacto, proteger dados e sistemas (confidencialidade, integridade e disponibilidade), cumprir as normas internas e externas (incluindo a Portaria Unesp nº 12/2025 e a LGPD) e resguardar a reputação e o valor público da Universidade.

2.2. ESCOPO

Aplica-se a todos os recursos de TIC da Unesp, conectados ou não à unespNET, incluindo sistemas, serviços, aplicações, equipamentos e dados institucionais.

Abrange toda a comunidade acadêmica (docentes, discentes, servidores, pesquisadores, estagiários, voluntários) e terceiros autorizados.

3. REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Seção
<i>Center for Internet Security - CIS</i>	<i>Critical Security Control 17: Gestão de respostas a incidentes</i>
<i>International Organization for Standardization – ISO 27035</i>	<i>Orientações sobre o gerenciamento de incidentes de segurança da informação</i>
<i>International Organization for Standardization – ISO 27002:2022</i>	Itens 5.26, 5.27, 5.28 e 5.29
<i>Guia do Framework de Privacidade e Segurança da Informação 2.0</i>	CONTROLE 17: Gestão de incidentes

4. CONCEITOS E DEFINIÇÕES

Para garantir um entendimento consistente e claro dos termos, as seguintes definições são estabelecidas:

- **CSTI:** Comitê Superior de Tecnologia da Informação.
- **CTINF:** Coordenadoria de Tecnologia da Informação.

- **GTICC:** Grupo Técnico de Infraestrutura Computacional e Comunicações.
- **Encarregado:** Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados (ANPD). Também é referenciado no mercado e na área de tecnologia de informação como data protection officer em função da denominação adotada na GPDR (general protection data regulation) da União Europeia.
- **Vertical de Segurança:** Instância operacional da CTInf.
- **CSIRT:** (Equipe de Resposta a Incidentes de Segurança em Computadores): Equipe de Resposta a Incidentes responsável pela execução técnica e operacional da resposta.
- **Ativo de Informação:** Ativos com potencial para armazenar ou processar dados. Para os fins deste documento, os ativos corporativos incluem dispositivos de usuário final, dispositivos de rede, dispositivos não computacionais/Internet das Coisas (IoT) e servidores em ambientes virtuais, baseados em nuvem e físicos.
- **Evento de Segurança:** Ocorrência suspeita em um sistema, serviço ou rede que indica uma possível violação de política de segurança.
- **Incidente Cibernético:** ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso; pode ser ainda caracterizado por evento que possibilite o acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de acesso à informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **Indicador de Comprometimento (IoC):** Um dado forense (como um hash de arquivo ou endereço IP) que pode ser usado para detectar atividade maliciosa.



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”

- **MTTD (Mean Time to Detect):** O tempo médio para detectar um incidente.
- **MTTC (Mean Time to Contain):** O tempo médio para conter um incidente.
- **MTTR (Mean Time to Recover):** O tempo médio para restaurar os sistemas e serviços afetados.
- **PII (Personally Identifiable Information):** Informações que podem ser usadas para identificar uma pessoa.

5. COMUNICAÇÃO

5.1. INTERNA

CSIRT: security@unesp.br

GTICC: gticc@unesp.br

GTDSI: gtdsi@unesp.br

DevOps: devops.ndsi@unesp.br

Jurídico: aj@unesp.br / (11) 5627-0306

Encarregado: dpo@unesp.br / Profª Cláudia Maria - Ouvidoria de Serviços Públicos

Docentes, Discentes e Servidores: Listas Dinâmicas Google / [ACI](#)

5.2. EXTERNA

CERT.BR: <https://www.cert.br/>

FORNECEDOR FIREWALL: noc@ziva.com.br / (11) 3365-0415 e (11) 3365-0410

FORNECEDOR INTERNET: 24x7@ansp.br / (11) 3136-2785

SOC-RNP: atendimento@rnp.br / 0800 722 0216.

5.3. Matriz de Comunicação

Define os destinatários e os prazos de notificação para cada nível de incidente.

Tipo de Incidente	Prazo Notificação	Destinatários
P1 - Crítico	Imediato (<30min)	CSTI, Encarregado, GTICC, CSIRT, Jurídico.
P2 - Alto	até 2 horas	Encarregado, GTICC, CSIRT.
P3 - Médio	até 8 horas	GTICC, CSIRT.
P4 - Baixo	até 24 horas	CSIRT

5.4. Comunicação Externa

- Com Clientes: A comunicação deve ser transparente e factual, apenas se os serviços ou dados dos clientes forem diretamente afetados.
- Com Reguladores: Notificações obrigatórias em prazos definidos (ex: LGPD em até 72 horas para a ANPD se houver alto risco aos titulares).
- Com a Mídia: Apenas através da assessoria oficial, com aprovação do CSTI.
- Com a Polícia: Apenas em casos de suspeita de crime cibernético.

6. GOVERNANÇA E ESTRUTURA ORGANIZACIONAL

6.1. ESTRUTURA DE GOVERNANÇA PARA RESPOSTA A INCIDENTES

A efetividade da resposta a incidentes depende de uma governança clara, que assegure a definição formal de papéis, responsabilidades e fluxos de decisão. Cada servidor envolvido deve compreender suas atribuições, evitando sobreposição de funções e lacunas no tratamento do incidente. A governança deve garantir comunicação tempestiva, coordenação integrada entre as áreas técnicas e administrativas, além da observância às normas institucionais e legais vigentes.

6.2. CSTI

É o órgão máximo de governança, responsável por decisões estratégicas na área de TI.

- **Responsabilidades:** Aprovação de políticas e recursos, tomada de decisões estratégicas em incidentes críticos, aprovação de comunicações externas relevantes, e alinhamento com os objetivos de negócio.
- **Composição:** <https://www2.unesp.br/portal#!/csti/csti/composicao/>

6.3. CSIRT

O CSIRT da UNESP é a equipe técnica responsável por responder a incidentes de segurança cibernética.

- **Responsabilidades:** Investigação técnica, contenção imediata, erradicação, recuperação segura de sistemas e dados, e preservação de evidências.

6.4. Papéis Específicos

- **Coordenador:** Gerencia o incidente do início ao fim, coordena as atividades entre a IMT e a IRT, e mantém um registro cronológico das ações.
- **Analistas:** Triage inicial de eventos, análise técnica de logs e evidências, e implementação de medidas de contenção. Responsável pela preservação da cadeia de custódia e pela análise forense digital especializada.
- **Comunicação:** Elabora mensagens internas e externas em alinhamento com a estratégia da organização.
- **Jurídico/Compliance:** Avalia obrigações legais, gerencia a comunicação com autoridades e avalia riscos regulatórios.

7. TIPOS E VETORES DE INCIDENTES

7.1. VETORES DE AMEAÇA COMUNS

Os vetores são os métodos que os atacantes usam para explorar vulnerabilidades.

- **Mídia Externa/Removível:** Ataques de pendrives infectados.
- **Ataque de Força Bruta:** Uso de métodos de força bruta para comprometer sistemas (ex:

DDoS).

- Web e Email: Ataques realizados a partir de sites ou mensagens de e-mail (ex: phishing).
- Perda ou Roubo de Equipamento: Perda de laptops, smartphones ou tokens.
- Interdição na Cadeia de Suprimentos: Ataques em hardware ou software em trânsito do fornecedor.
- Uso Indevido: Violação da Política de Uso Aceitável por um usuário autorizado.

7.2. TIPOS DE INCIDENTES DE SEGURANÇA

Os incidentes incluem, mas não se limitam a:

- **Ataques de Malware:** Vírus, worms, ransomware.
- **Vazamento de Dados:** Exposição de informações confidenciais ou pessoais.
- **Acesso Não Autorizado:** Tentativas de acesso ou exploração de vulnerabilidades.
- **Indisponibilidade de Sistemas:** Interrupção de serviços causada por ataques (DoS, DDoS) ou falhas.
- **Falhas de Segurança:** Em processos ou controles.
- **Violações de Política:** Uso de software não autorizado, senhas fracas.

8. CLASSIFICAÇÃO E PRIORIZAÇÃO DE INCIDENTES

A classificação determina a urgência e os recursos necessários para a resposta.

8.1. NÍVEIS DE PRIORIDADE

- **CRÍTICO (P1) - Resposta Imediata:**
 - Impacto: Paralisação de sistemas de missão crítica, vazamento massivo de dados sensíveis (>10.000 registros), ataque de ransomware, impacto financeiro, risco à vida ou à segurança física.
 - Tempo de Resposta: Imediato (<30 minutos).
- **ALTO (P2) - Resposta em 2 horas:**
 - Impacto: Comprometimento limitado a sistemas importantes (mas não essenciais), vazamento de dados não sensíveis, malware detectado em múltiplos dispositivos sem movimento lateral confirmado.

- Tempo de Resposta: até 2 horas.
- MÉDIO (P3) - Resposta em 8 horas:
 - Impacto: Malware isolado em uma estação de trabalho, vulnerabilidade crítica descoberta sem exploração confirmada, violações de políticas internas sem impacto imediato.
 - Tempo de Resposta: até 8 horas.
- BAIXO (P4) - Resposta em 24 horas:
 - Impacto: Alerta de SIEM ou antivírus sem confirmação de incidente, eventos suspeitos que exigem investigação, uso não autorizado de software sem risco evidente.
 - Tempo de Resposta: até 24 horas.

8.2. CRITÉRIOS DE AVALIAÇÃO DE IMPACTO

A avaliação considera múltiplos fatores para determinar a classificação:

- Impacto Financeiro e Operacional: Perdas diretas (vendas interrompidas) e indiretas (horas de trabalho improdutivas).
- Sensibilidade dos Dados Comprometidos: Classificação dos dados (pessoais, financeiros, estratégicos) e volume de registros expostos.
- Exposição Pública ou Midiática: Potencial de dano à reputação da marca ou cobertura na imprensa.
- Obrigações Regulatórias: Necessidade de notificar autoridades (ex: LGPD, NIS2).
- Número de Usuários/Clientes Afetados: Quantidade de usuários internos ou clientes que não conseguem acessar serviços.
- Tempo de Indisponibilidade: Tempo que os sistemas críticos ficaram fora do ar, com thresholds definidos.

9. PROCESSO DE GESTÃO DE INCIDENTES (Ciclo de Vida)

O processo de gestão de incidentes segue um ciclo estruturado, alinhado à ISO/IEC 27035 e ao NIST Cybersecurity Framework, garantindo padronização e melhoria contínua.



Fonte: Elaboração própria da Vertical de Segurança, adaptado da ISO/IEC 27035:2023.

9.1. FASE 1: PLANEJAR E PREPARAR

Esta fase é a base de todo o processo e deve ser contínua.

- Planejamento: Desenvolver e manter planos de resposta específicos por tipo de incidente (playbooks), estabelecer critérios de classificação e definir canais de comunicação.
- Preparação: Treinar equipes regularmente, realizar exercícios de simulação, manter o inventário de ativos críticos atualizado, listar contatos dos integrantes da equipe de CSIRT.

9.2. FASE 2: DETECTAR, INVESTIGAR E COMUNICAR

Identificar a ocorrência de Incidentes de Segurança.

- Detecção: A detecção pode vir de sistemas automatizados (SIEM, SOC), relatórios de usuários, ou notificações de terceiros.
- Notificação Inicial: Notificar o ponto de contato único imediatamente, fornecendo a data/hora, descrição, sistemas afetados e ações preliminares.
- Análise e Classificação: Confirmar se o evento é um incidente, avaliar o escopo e determinar o impacto potencial usando os critérios de classificação.
- Preservação Inicial de Evidências: Não desligar sistemas afetados sem orientação e preservar logs relevantes, iniciando a cadeia de custódia formal.
- **Em caso de crime:**
 - Procurar a Delegacia de Polícia mais próxima ou registrar um Boletim de Ocorrência Eletrônico através do site da [Delegacia Eletrônica](#) na opção OUTROS CRIMES.

9.3. FASE 3: CONTENÇÃO, COLETA DE EVIDÊNCIAS E REMEDIAÇÃO

- Contenção: Ações imediatas para limitar o dano, como isolar dispositivos, bloquear acessos não autorizados e suspender serviços específicos.
- Coleta e Preservação de Evidências: Manter um registro detalhado de como toda a evidência foi coletada, incluindo quem a manuseia e o horário.
- Plano de Ação de Remediação: Criar um plano para resolver o incidente após a contenção, considerando recursos necessários e prazos.

9.4. FASE 4: RECUPERAÇÃO E RELATÓRIO

- Recuperação: Restaurar sistemas a partir de backups validados, garantir a integridade dos dados e testar a funcionalidade.
- Validação de Backups Limpos: Os backups usados para restauração devem ser verificados para garantir que estejam livres de malware e que sua integridade seja

validada através de checksums ou hashes.

- Monitoramento Pós-Recuperação: Monitoramento intensivo nos sistemas restaurados para garantir que não haja atividade suspeita.

9.5. FASE 5: LIÇÕES APRENDIDAS E MELHORIA

- Análise Pós-Incidente: Realizar uma reunião (em até 30 dias após a recuperação) para analisar a causa raiz, a eficácia da resposta e os tempos de detecção e resposta (MTTD, MTTC, MTTR).
- Plano de Ação Corretiva: Criar um plano de ação para implementar melhorias identificadas, como a correção de controles deficientes e a atualização de procedimentos.
- Atualização do SGSI: As lições aprendidas são incorporadas ao Sistema de Gestão de Segurança da Informação.

10. MATRIZ RACI

Atividade	CSIRT	CSTI	GTICC	Jurídico	Encarregado
Detecção	R	I	R	I	I
Contenção	R	A	C	I	I
Coleta de Evidências	R	I	C	C	I
Remediação	R	A	R	I	I
Recuperação	R	A	R	I	I
Comunicação	C	A	C	R	R
Análise Pós-Incidente	R	A	C	C	C



11. TREINAMENTO E SIMULAÇÕES

- Programa de Capacitação Estratificado: Treinamento específico para a liderança executiva (gestão de crise), equipes de resposta (habilidades técnicas) e áreas de negócio (reconhecimento e reporte).
- Exercícios de Simulação: Realização de tabletop exercises (trimestralmente para a IMT/IRT) e simulações técnicas (mensalmente para a IRT) para validar procedimentos e treinar equipes sob pressão.

12. ANEXOS NORMATIVOS

- Playbook por tipo de incidente
- [Fluxograma do Processo de Resposta a Incidentes](#)
- [Modelo de relatório de Resposta a Incidentes](#)