Propuesta de Creación y Operación del CSIRT UTP-Veraguas (CSIRT-UTPV)

Propuesta de Creación y Operación del CSIRT UTP-Veraguas (CSIRT-UTPV)

Universidad Tecnológica de Panamá – Centro Regional de Veraguas

Versión 1.0 | Propietario: Coordinación CSIRT-UTPV

1. Propósito y alcance

Establecer un Equipo de Respuesta a Incidentes de Seguridad Informática para la UTP-Veraguas (CSIRT-UTPV), definiendo marco de actuación, servicios, funciones, procesos, métricas y coordinación con autoridades nacionales para prevenir, detectar, contener y recuperar incidentes.

2. Marco de referencia y cumplimiento

La propuesta se alinea con estándares y guías: NIST SP 800-61 Rev.3, Playbooks de CISA, TLP 2.0 y el CSIRT Services Framework v2.1 de FIRST; establece coordinación con CSIRT Panamá para incidentes graves o de interés nacional.

- NIST SP 800-61 Rev.3: recomendaciones actualizadas para gestionar incidentes (perfil CSF 2.0).
- CISA – Playbooks federales: procedimientos para respuesta a incidentes y a vulnerabilidades.
- TLP 2.0: clasificación para intercambio de información sensible.
- FIRST – CSIRT Services Framework v2.1: catálogo de servicios y funciones CSIRT.
- Ecosistema nacional: coordinación y reporte con CSIRT Panamá (incidentes@cert.pa, Tel. 520-2378).

3. Gobernanza y modelo operativo

- Patrocinio: Dirección/Coordinación de TI del Centro Regional de Veraguas.
- Propietario del proceso: Coordinación CSIRT-UTPV.
- Comité de Seguridad (ad hoc): Coordinación CSIRT, TI, Asesoría Legal, Académica y Comunicación.
- Difusión controlada: TLP 2.0 y principio de necesidad de saber.
- Políticas y runbooks: repositorio institucional con acceso restringido.

4. Catálogo de servicios

4.1 Reactivos (núcleo)

- Gestión de incidentes (recepción, análisis, contención, erradicación, recuperación, lecciones).
- Gestión de vulnerabilidades (tratamiento, priorización, parches).
- Análisis forense/digital (evidencias, malware, logs, imágenes).
- Alertas y avisos (IOC, campañas activas, CVE críticas).

4.2 Proactivos

- Monitoreo y caza de amenazas (telemetría de endpoints/IDS).
- Concienciación y capacitación (simulaciones de phishing, talleres).
- Asesoría de configuración segura (SO, MDM, MFA, backups).

- Divulgación responsable.

4.3 Gestión y calidad

- Evaluación de riesgos y controles; continuidad (BCP/DRP).
- Métricas y reporting; auditorías técnicas.
- Gestión de proveedores y herramientas (SOC, EDR, SIEM, ticketing).

5. Roles y estructura

Estructura funcional sugerida y asignaciones iniciales (sujetas a aprobación):

Rol del CSIRT	Misión del rol	Responsabilidades clave	Perfil / Habilidades	Responsable inicial
Coordinación CSIRT	Dirigir y gobernar la respuesta a incidentes	Priorizar incidentes; asignar recursos; enlace con autoridades y CSIRT Panamá; aprobar comunicaciones; validar cierre	Gestión de incidentes; liderazgo; comunicación ejecutiva; conocimiento normativo (TLP, políticas)	**Muriel Jaramillo**
Analista de Incidentes (Tier 1/2)	Triage y análisis inicial	Monitorear alertas; clasificar severidad; recolectar evidencias; contención inicial; escalar a especialistas	SIEM/EDR; redes básicas; sysadmin; scripting	**Por designar**
Especialista Forense / Malware	Preservar y analizar evidencias	Adquisición forense; análisis de artefactos; cadena de custodia; informes técnicos; apoyo a legal	Forense digital; análisis de malware; Autopsy/Volatility; buenas prácticas probatorias	**Gilberto Ramos**
Especialista de Redes / SOC	Defender infraestructura de red	IDS/IPS; NetFlow; reglas de firewall; detección y respuesta a intrusiones; soporte ante DDoS	Networking (TCP/IP, Wi-Fi); hardening; herramientas SOC	**Gilberto Ramos**
Gestor de Vulnerabilidades	Coordinar el ciclo de parches	Escaneo periódico; priorizar (CVSS); coordinar remediaciones; verificar y reportar estado	Gestión de vulnerabilidades; hardening; coordinación con TI	**Agustín Sánchez**
Responsable de Comunicación / TLP	Comunicaciones internas/externas controladas	Avisos a usuarios; etiquetado TLP 2.0; comunicados al Comité TIC; plantillas y cronogramas	Comunicación técnica; manejo de crisis; TLP 2.0	**Agustín Sánchez**
Admin. de Herramientas (SIEM/EDR/Ticketing)	Mantener la plataforma del CSIRT	Configuración e integraciones; control de accesos; respaldos; métricas y SLA	SecOps/DevOps; automatización; gestión de accesos	**Por designar**
Enlace Legal y Protección de Datos	Asegurar cumplimiento y asesoría legal	Revisión de actuaciones; privacidad y datos personales; notificaciones requeridas	Asesoría legal; normativa panameña de datos; gestión de riesgos legales	**Por designar**

- Coordinación CSIRT – Muriel Jaramillo: liderazgo, priorización, enlace con autoridades y CSIRT Panamá; comunicación ejecutiva.
- Analista Forense y Especialista en Redes – Gilberto Ramos: evidencias, cadena de custodia, monitoreo/IDS/IPS.
- Comunicación y Gestión de Vulnerabilidades – Agustín Sánchez: boletines, concienciación, coordinación de remediaciones.

Perfiles funcionales adicionales: analistas de incidentes (Tier 1/2), especialista malware/forense, especialista de redes/SOC, gestor de vulnerabilidades y responsable de comunicación/TLP.

6. Proceso de respuesta a incidentes

Flujo NIST SP 800-61 Rev.3:

1. Preparación
2. Detección y análisis
3. Contención, erradicación y recuperación
4. Post-incidente (lecciones y mejora)

7. Clasificación de severidad (inspirada en NCISS/CISA)

- Crítico: ransomware en servicios centrales; exfiltración amplia de PII; privilegios comprometidos con actividad.
- Alto: intrusión con potencial de movimiento lateral; exposición limitada; DoS sostenido.
- Medio: malware aislado; phishing con clics sin pérdida; degradación de servicio secundario.
- Bajo: escaneos/alertas sin compromiso; vulnerabilidades sin PoC explotable inmediata.

8. Playbooks abreviados

8.1 Phishing con credenciales

- Reset de credenciales y revocación de tokens/sesiones
- Búsqueda de IoC y revisión de accesos
- Notificación controlada (TLP)
- Prevención: filtros, DMARC/DKIM/SPF, MFA

8.2 Ransomware

- Aislar equipos/VLAN y bloquear C2
- Erradicar y rotar secretos
- Restaurar desde backups verificados
- Escalar a comité de crisis y CSIRT Panamá si aplica

8.3 DoS/DDoS

- Mitigación con proveedor/WAF/rate limiting
- Comunicación de estado

- Post-mortem y ajuste de capacidad

8.4 Vulnerabilidad crítica

- Inventario de exposición
- Parcheo/mitigaciones priorizadas
- Verificación de explotación y hardening

9. Comunicación y TLP 2.0

- Uso de TLP: CLEAR, GREEN, AMBER, AMBER+STRICT, RED
- Canales: incidentes@utp.edu.pa y teléfono de guardia
- Plantillas de avisos y aprobación por Coordinación CSIRT

10. Coordinación externa

- CSIRT Panamá – Tel. (+507) 520-2378; incidentes@cert.pa; uso de PGP/GnuPG recomendado
- Participación en comunidades de intercambio (FIRST/TF-CSIRT)

11. Fases de implementación y cronograma

- Fase 0 – Preparación (2–4 semanas)
- Fase 1 – Puesta en marcha (4–6 semanas)
- Fase 2 – Piloto operativo (4 semanas)
- Fase 3 – Mejora continua

12. Métricas y reporting

- MTTD/MTTR por severidad
- % incidentes contenidos < 24 h
- Tasa de parcheo (7/30 días) y reincidencia
- Informes ejecutivos trimestrales

13. Gestión de proveedores y herramientas

- Ticketing, SIEM, EDR, IDS/IPS, DLP, escáner de vulnerabilidades, SOAR
- Criterios: integración, cobertura, costo total, soporte, privacidad

14. Riesgos y mitigaciones

- Recursos limitados → acuerdos de servicio y priorización
- Dependencia tecnológica → pruebas de restauración y redundancias
- Errores de comunicación → TLP 2.0 y plantillas
- Rotación de personal → manuales y capacitación continua

Anexo A. Plantilla de Ficha de Incidente

- ID/Fecha
- Activo afectado/Descripción/Severidad

- Impacto/Evidencias
- Contención/Erradicación/Recuperación
- Estado
- Lecciones aprendidas

Referencias

[1] National Institute of Standards and Technology (NIST), "Computer Security Incident Handling Guide, SP 800-61 Rev.3," 2025. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/61/r3/final

[2] Cybersecurity and Infrastructure Security Agency (CISA), "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks," 2021. [Online]. Available: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks

[3] Cybersecurity and Infrastructure Security Agency (CISA), "Traffic Light Protocol (TLP) 2.0 User Guide," 2022. [Online]. Available: https://www.cisa.gov/resources-tools/resources/tlp-20-user-guide

[4] Forum of Incident Response and Security Teams (FIRST), "CSIRT Services Framework v2.1," 2019. [Online]. Available: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1

[5] Cybersecurity and Infrastructure Security Agency (CISA), "National Cyber Incident Scoring System (NCISS)," 2016. [Online]. Available: https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

[6] CSIRT Panamá, "Sitio oficial y contacto para reporte de incidentes," 2025. [Online]. Available: https://cert.pa/