



UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura



DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD



RESUMEN EJECUTIVO

GUÍA PRÁCTICA PARA CSIRTs

JULIO – OCTUBRE 2026



CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía práctica para CSIRTs

Volumen 2: un modelo de negocio sustentable

Documento base: Organización de los Estados Americanos (OEA), 2023

Alcance: CSIRTs públicos, con énfasis en América Latina y el Caribe

Propósito: Síntesis estratégica para responsables de ciberseguridad y tomadores de decisiones

Síntesis ejecutiva

La principal conclusión de la guía es que un CSIRT sostenible no se construye alrededor de herramientas, sino de un mandato legítimo, una comunidad que confía en el equipo y una cartera de servicios que puede sostenerse en el tiempo.

La OEA propone entender al Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) como una capacidad institucional que integra gobernanza, personas, procesos, tecnología, comunicación y cooperación. Su función es prevenir, identificar, coordinar, responder y mitigar incidentes cibernéticos dentro de una comunidad definida. En el ámbito público, además de atender incidentes, el CSIRT puede contribuir a la resiliencia de los servicios esenciales, al desarrollo de políticas nacionales y a la coordinación entre organismos.

El documento advierte que numerosos CSIRTs de la región enfrentan problemas recurrentes: presupuestos inestables, alta rotación de especialistas, dependencia de personal prestado, adquisiciones lentas, deuda tecnológica y cambios de prioridades políticas. La respuesta recomendada es una construcción gradual: comenzar con pocos servicios, medir su valor, documentar procesos y ampliar capacidades únicamente cuando existan recursos, demanda y madurez suficientes.

Mensaje central: Pensar en grande, comenzar con poco y crecer con resultados verificables. La confianza es el activo que permite recibir reportes, coordinar acciones y asegurar apoyo político y presupuestario.

1. Razón de ser y alcance institucional

La digitalización ha convertido los incidentes cibernéticos en riesgos con efectos operativos, económicos y sociales. Un ataque puede interrumpir servicios de salud, energía, agua, transporte, identificación, finanzas o comunicaciones. Frente a este escenario, la existencia de un CSIRT permite sustituir respuestas improvisadas por una gestión formal, coordinada y repetible.

Valor estratégico

1. Estandariza la recepción, priorización, análisis, coordinación y cierre de incidentes.
2. Aumenta la visibilidad sobre vulnerabilidades, indicadores de compromiso (IoC), indicadores de ataque (IoA) y patrones de amenaza.
3. Facilita la cooperación con entidades nacionales, proveedores, otros CSIRTs y organismos internacionales.
4. Fortalece la preparación mediante alertas tempranas, ejercicios, capacitación y concientización.
5. Aporta evidencia para estrategias de ciberseguridad, políticas públicas y decisiones de inversión.

CSIRT nacional y CSIRT sectorial

Un CSIRT nacional funciona como punto de coordinación dentro y fuera del país. Centraliza el panorama situacional, articula respuestas en crisis de alcance nacional y conecta a sectores, autoridades y redes internacionales. Un CSIRT sectorial, en cambio, atiende una comunidad más delimitada -por ejemplo, salud, finanzas, defensa, academia o energía- y suele requerir conocimiento especializado sobre tecnologías, riesgos y obligaciones propias del sector.

Ambos modelos son complementarios. La arquitectura deseable combina coordinación continua, intercambio de información y delimitación clara de competencias. El CSIRT nacional necesita la visibilidad que proporcionan los equipos sectoriales; estos, a su vez, se benefician de la articulación, contactos y capacidad de escalamiento nacional e internacional.

Condiciones de legitimidad

La ubicación institucional no tiene una fórmula única. Puede depender de una presidencia, ministerio, secretaría, organismo de seguridad u otra entidad. La decisión debe considerar el mandato

jurídico, la capacidad de convocatoria, la autonomía operativa, el acceso a presupuesto, la protección de información y el apoyo político del más alto nivel. El mandato debe establecer comunidad atendida, alcance, servicios, responsabilidades y límites de actuación, con respeto de las normas aplicables y los derechos humanos.

Criterio de diseño: La posición orgánica es adecuada cuando permite coordinar con autoridad, actuar con agilidad, proteger la información y mantener una relación de confianza con las entidades atendidas.

2. Panorama regional y sostenibilidad

La experiencia de América Latina y el Caribe muestra una diversidad de modelos de creación y adscripción institucional. Los CSIRTs públicos han surgido mediante decretos, estrategias nacionales, planes de desarrollo, iniciativas legislativas, resoluciones y acuerdos ministeriales. La heterogeneidad confirma que la estructura debe adaptarse al ordenamiento jurídico, la organización estatal y el contexto político y sociocultural de cada país.

Principales riesgos de continuidad

La sostenibilidad se ve afectada por factores interdependientes. En materia de talento, el personal formado en un CSIRT se vuelve atractivo para el sector privado, lo que incrementa la rotación. En presupuesto, son frecuentes los equipos sin asignación fija, con perfiles salariales poco competitivos, personal comisionado y procesos de compra incompatibles con la velocidad de la amenaza. En tecnología, las migraciones, las licencias, el mantenimiento y la deuda técnica pueden comprometer la operación. A ello se suman cambios de gobierno y escenarios extraordinarios, como elecciones, conflictos sociales o eventos de gran escala.

Según los datos recopilados por CSIRTAmericas para la guía, un CSIRT público de la región tenía, en promedio, seis integrantes. La representación femenina alcanzaba 26 % del personal y 32 % de las posiciones de liderazgo. Estas cifras no constituyen un estándar de dimensionamiento, pero evidencian equipos pequeños y la necesidad de ampliar las vías de captación y desarrollo de talento.

Principios para asegurar continuidad

1. Definir servicios antes de dimensionar personas, herramientas y presupuesto. El tamaño del equipo depende de la cartera y del nivel de servicio comprometido.
2. Iniciar con la gestión de incidentes y capacidades básicas: sistema de tickets, correo, teléfono, sitio web y un mecanismo de alertas.
3. Evitar copiar servicios de otros equipos sin validar su utilidad local. La demanda de la comunidad debe orientar la expansión.
4. Contratar experiencia suficiente o cubrir brechas iniciales con asistencia especializada, sin convertir la tercerización en dependencia estructural.
5. Combinar software libre y soluciones comerciales según riesgos, costos de ciclo de vida, interoperabilidad y capacidad real de mantenimiento.
6. Reservar fondos para contingencias, renovación tecnológica, formación, desplazamientos, soporte especializado y crecimiento de servicios.

La confianza atraviesa todos estos elementos. Una entidad reportará oportunamente solo si percibe que el CSIRT la apoyará, mantendrá la confidencialidad y aportará valor. La autoridad formal habilita la actuación; la confianza la vuelve efectiva.

3.2 Propuesta de valor

La propuesta central es identificar, prevenir, responder y mitigar incidentes, acompañando a la comunidad con asistencia y asesoramiento. El valor se materializa, por ejemplo, al detectar credenciales expuestas, contener un ataque de denegación de servicio, analizar rastros de malware, coordinar la recuperación de un servicio o advertir sobre vulnerabilidades. Cada prestación debe estar alineada con el mandato, la misión y la madurez de la comunidad.

3.3 Canales

El CSIRT necesita canales accesibles y disponibles: sitio web, tickets, correo, teléfono, listas de distribución, alertas, redes sociales, conferencias, plataformas de intercambio como MISP y grupos de

mensajería. La automatización debe equilibrarse con interacción humana. En crisis públicas, una página de estado puede centralizar actualizaciones, reducir rumores y preservar la trazabilidad sin revelar información sensible.

La publicación del RFC 2350 es una buena práctica para comunicar políticas, procedimientos, servicios, formas de contacto y expectativas de cooperación. El lenguaje debe adaptarse al destinatario: simple para ciudadanía y medios; preciso, confiable y accionable para audiencias técnicas.

3.4 Relaciones con la comunidad

La relación se construye mediante soporte a incidentes, asesorías, formación, reuniones de trabajo y redes de contacto. Escuchar a la comunidad permite ajustar los servicios a necesidades reales. Un equipo que informa, acompaña y devuelve recomendaciones útiles convierte cada interacción en una oportunidad para fortalecer la confianza y elevar la madurez colectiva.

Prueba de valor: Un servicio es pertinente cuando resuelve una necesidad prioritaria, puede operarse con calidad y genera resultados que la comunidad reconoce.

4. Componentes operativos y financieros del CANVAS

4.1 Fuentes de financiamiento

El presupuesto público de la entidad anfitriona debe cubrir la operación ordinaria y al personal. Para proyectos de ampliación pueden evaluarse fondos de organismos internacionales, consultorías permitidas por el marco legal, cooperación con el sector privado, universidades, asociaciones civiles y Fuerzas Armadas. Estas alternativas complementan, pero no sustituyen, una base presupuestaria institucional estable.

4.2 Actividades y catálogo de servicios

El marco de FIRST agrupa capacidades en gestión de incidentes, vulnerabilidades, análisis situacional, transferencia de conocimientos y gestión de eventos de seguridad. La guía insiste en no ofrecer todo desde el inicio. La gestión de incidentes debe ser el núcleo; las alertas, campañas de concientización y entrenamientos son extensiones de alto impacto y relativa simplicidad. Antes de anunciar

un servicio deben definirse su alcance, horarios, criterios de priorización, dependencias y exclusiones. Prometer una atención 24/7 sin turnos, personal y procedimientos suficientes puede deteriorar la confianza y generar una falsa sensación de seguridad.

4.3 Recursos clave

1. Organizacionales: estructura, procedimientos, espacios, comunicaciones, servidores, movilidad y salas de coordinación.
2. Información accionable: datos relevantes, oportunos, precisos, íntegros y comprensibles que permitan decidir y actuar.
3. Herramientas: tickets, correo, telefonía, plataformas de análisis, detección, intercambio y respuesta, con costos de mantenimiento previstos.
4. Personas: perfiles técnicos, analíticos, jurídicos, de gestión y comunicación. El talento es el recurso crítico para prestar servicios y construir confianza.

4.4 Socios estratégicos

Los proveedores de Internet pueden apoyar en contención; las fuerzas del orden, en investigaciones; el Poder Legislativo, en marcos normativos; el Poder Judicial, en actuaciones que requieran evidencia o peritaje; las organizaciones internacionales, en coordinación, financiamiento y formación; las universidades, en talento e investigación; las empresas, en tecnología y capacitación; las asociaciones civiles, en cultura de seguridad; y otros CSIRTs, en intercambio de inteligencia y asistencia mutua. Las relaciones deben formalizarse cuando corresponda mediante acuerdos y mecanismos compatibles con la legislación.

4.5 Estructura de costos

El presupuesto debe diferenciar inversión de capital y gastos operativos. Debe incluir infraestructura, licencias y fuentes de inteligencia, salarios, guardias, formación, viajes, mantenimiento, soporte, membresías, consultorías, comunicación y contingencias. Toda expansión de servicios exige revisar nuevamente el CANVAS y el costo total de propiedad. La sostenibilidad se debilita cuando la capacidad depende de licencias o plataformas cuya renovación no puede garantizarse.

5. Claves para un CSIRT eficiente

Mandato, expectativas y procesos

El equipo debe mantenerse dentro de su mandato y canalizar solicitudes ajenas a su competencia. Al inicio conviene explicar a la alta dirección que la creación del CSIRT no elimina los incidentes; introduce una capacidad formal para gestionarlos. Procesos, responsabilidades, criterios de escalamiento y decisiones deben documentarse para sostener la operación y facilitar auditorías.

Talento y retención

En equipos pequeños, la asignación de roles múltiples y la rotación interna pueden ampliar capacidades, siempre que existan controles de segregación y continuidad. Las alianzas con universidades permiten crear una cantera de talento. La flexibilidad laboral, las trayectorias profesionales, la formación y el sentido de propósito ayudan a reducir la rotación. Quien recibe capacitación externa debe documentar y transferir lo aprendido para que el conocimiento permanezca en la organización.

Además de competencias técnicas, se requieren pensamiento crítico, análisis de riesgos, coordinación, negociación y comunicación pública. En incidentes con impacto ciudadano, la capacidad de explicar qué ocurre y qué debe hacer cada audiencia es parte de la respuesta.

Servicios y métricas

La cantidad de tickets no equivale a eficacia. Un mayor volumen puede reflejar visibilidad, pero también deficiencias recurrentes. La medición debe mostrar resultados: tiempos de reconocimiento y respuesta, severidad e impacto, porcentaje de casos dentro de niveles de servicio, recurrencia, uso de alertas, ejercicios realizados, adopción de recomendaciones, satisfacción y mejoras de madurez. Los indicadores deben servir para aprender y priorizar, no solo para reportar actividad.

Presupuesto y apoyo político

El presupuesto debe revisarse periódicamente y contemplar urgencias. La alta dirección necesita comprender que las amenazas, la tecnología y la demanda cambian. Para sostener el respaldo político, el CSIRT debe presentar resultados medibles, cuadros de

mando y evidencia de reducción de riesgo. La cooperación internacional puede ampliar capacidades, pero no debe reemplazar la responsabilidad institucional de financiar la operación esencial.

Comunicación y confianza

Se requiere un responsable y un plan de comunicación para incidentes de interés público. Los mensajes deben coordinarse con las autoridades competentes, proteger la confidencialidad y ofrecer orientación útil. Comunicar servicios, resultados y lecciones fortalece la relación con la comunidad y favorece que los incidentes se reporten temprano.

Riesgo crítico: Ofrecer más servicios de los que el equipo puede operar con calidad erosiona la confianza y compromete la sostenibilidad.

6. El CSIRT del futuro

El CSIRT evoluciona de un equipo reactivo y predominantemente técnico hacia una capacidad integral alineada con objetivos sociales, económicos y de transformación digital. El usuario final debe ocupar el centro del diseño de servicios, y la operación debe basarse en datos e información accionable.

Líneas de evolución estratégica

1. Coordinar plataformas nacionales de intercambio de indicadores y articular a CSIRTs sectoriales.
2. Diseñar servicios desde las necesidades y el contexto del usuario, explicando de manera comprensible su impacto y beneficio.
3. Incorporar análisis de datos e inteligencia accionable en la priorización, la respuesta y la medición de resiliencia.
4. Participar activamente en estrategias nacionales de ciberseguridad, gobernanza digital y políticas públicas.
5. Desarrollar capacidades de respuesta que incluyan a los distintos sectores y mejoren la coordinación nacional.
6. Aplicar metodologías ágiles que reduzcan tiempos de respuesta y aceleren el aprendizaje operativo.

7. Construir alianzas flexibles con proveedores, reguladores, autoridades y redes internacionales.
8. Intervenir tempranamente en el diseño de iniciativas y servicios digitales para identificar riesgos antes de su despliegue.
9. Fortalecer la retención y las trayectorias profesionales de los especialistas.
10. Aprovechar nuevas tecnologías y modelos de respuesta después de evaluar su utilidad, seguridad y sostenibilidad.
11. Consolidar comunicación interna, ejecutiva y pública como capacidad operativa.
12. Alcanzar liderazgo y reconocimiento mediante resultados, no únicamente por mandato formal.
13. Mantener procesos sólidos, trazables y auditables.

Esta evolución exige preservar un equilibrio: innovar sin crear dependencia tecnológica, compartir información sin vulnerar la confidencialidad, actuar con rapidez sin omitir controles y ampliar servicios sin exceder la capacidad operativa.

7. Recomendaciones ejecutivas para implementación

La guía puede traducirse en una hoja de ruta de decisiones progresivas. Las siguientes prioridades son una síntesis aplicada del contenido de la OEA y deben ajustarse al mandato, riesgos y recursos de cada institución.

Fase 1 - Definir y legitimar

1. Formalizar mandato, autoridad, comunidad atendida, límites de actuación y coordinación con otras entidades.
2. Aprobar propuesta de valor, servicios iniciales, criterios de severidad y canales oficiales; publicar la información operativa equivalente al RFC 2350.

Fase 2 - Operar con disciplina

3. Implementar tickets, correo, teléfono, sitio web, guardias y procedimientos de gestión de incidentes.

4. Definir roles, escalamiento, comunicaciones, protección de información, conservación de evidencia e indicadores de desempeño.

Fase 3 - Consolidar confianza y sostenibilidad

5. Mantener reuniones con la comunidad, ejercicios y programas de transferencia de conocimientos.
6. Asegurar financiamiento estable y formalizar alianzas con ISPs, fuerzas del orden, academia, sector privado, organismos internacionales y otros CSIRTs.

Fase 4 - Escalar con evidencia

7. Agregar servicios solo cuando exista demanda demostrada, capacidad operativa y financiamiento sostenible.
8. Revisar el CANVAS, el catálogo y el costo total de propiedad, y aportar datos operativos a las políticas de ciberseguridad y transformación digital.

Conclusión

La sostenibilidad de un CSIRT es, ante todo, un problema de gestión pública y gobernanza. La tecnología es indispensable, pero no compensa un mandato ambiguo, servicios sobredimensionados, talento inestable o ausencia de confianza. Un equipo eficaz crece de forma controlada, aprende de cada incidente, comunica su valor y coopera con el ecosistema. Su éxito se mide por su capacidad para reducir impactos, acelerar la recuperación y elevar la resiliencia.

La actuación debe respetar competencias institucionales, confidencialidad, normas aplicables y derechos humanos. Legitimidad, competencia técnica y confianza conforman la base del CSIRT del futuro.

Fuente

Organización de los Estados Americanos. (2023). *Guía práctica para CSIRTs. Volumen 2: Un modelo de negocio sustentable*. Programa de Ciberseguridad del CICTE/OEA.