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

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Buenas prácticas para establecer un CSIRT nacional

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Buenas prácticas para establecer un CSIRT nacional

Síntesis estratégica para la toma de decisiones

Documento base: Organización de los Estados Americanos (OEA), abril de 2016
Ámbito: Creación y puesta en funcionamiento de un CSIRT de alcance nacional
Enfoque: Gobernanza, marco legal, servicios, talento, infraestructura y operación

Síntesis ejecutiva

La creación de un CSIRT nacional debe gestionarse como un proyecto institucional, no como una adquisición tecnológica. Su viabilidad depende de un mandato claro, autoridad jurídica, financiamiento sostenido, personal competente y confianza entre los actores que deben reportar y coordinar incidentes.

La guía de la OEA organiza el establecimiento del equipo en tres fases: planificación, ejecución y cierre. La planificación define misión, visión, ubicación institucional, marco legal, comunidad atendida, servicios, estructura, recursos, presupuesto y cronograma. La ejecución convierte esas decisiones en capacidades concretas mediante contratación, formación, instalaciones, arquitectura tecnológica y políticas operativas. El cierre verifica que los productos estén completos, documenta lecciones aprendidas y obtiene la aprobación formal del patrocinador.

El CSIRT nacional se concibe como punto de contacto y coordinación para incidentes de alcance estatal, incluido el enlace con equipos extranjeros y redes internacionales. No reemplaza a los responsables de seguridad de cada organización ni a los CSIRTs sectoriales; los articula, facilita el intercambio de información y actúa como instancia de apoyo cuando un incidente excede capacidades o jurisdicciones particulares.

Decisión clave: Antes de comprar herramientas o contratar personal, el país debe acordar para quién trabajará el CSIRT, qué autoridad tendrá, qué servicios podrá prestar y cómo se financiará después de la inversión inicial.

1. Función estratégica de un CSIRT nacional

Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) es una organización cuyo propósito principal es prestar servicios de gestión y respuesta a incidentes a una comunidad definida. Aunque el manejo de incidentes constituye su núcleo, la evolución del riesgo digital exige capacidades preventivas, analíticas, de comunicación, formación y coordinación. En consecuencia, el CSIRT debe integrarse al sistema nacional de gestión de riesgos y no operar como una unidad técnica aislada.

Valor para el Estado

- Centraliza la recepción, clasificación, análisis y coordinación de incidentes que afectan a entidades públicas, sectores críticos o intereses nacionales.
- Proporciona una visión común de amenazas, vulnerabilidades, campañas y patrones de ataque, reduciendo respuestas fragmentadas.
- Establece canales de cooperación con proveedores, autoridades, academia, sector privado, otros CSIRTs y organizaciones internacionales.
- Genera alertas, recomendaciones, ejercicios y programas de concientización que elevan la preparación de la comunidad objetivo.
- Aporta información técnica para decisiones de política pública, inversión, continuidad y protección de infraestructuras críticas.

Relación con otros equipos

El ecosistema puede incluir CSIRTs gubernamentales, académicos, militares, comerciales, sectoriales, de proveedores o de infraestructuras críticas. La coexistencia es deseable si las competencias están delimitadas. El equipo nacional debe conocer qué entidades ya reciben apoyo especializado, establecer procedimientos de escalamiento y evitar duplicidades. Su función coordinadora cobra especial importancia en crisis multisectoriales, incidentes transfronterizos y situaciones en las que ningún otro equipo tiene jurisdicción clara.

Principio de adaptación

La guía no propone una estructura universal. Cada país debe adaptar el modelo a su realidad política, cultural, jurídica, geográfica y presupuestaria. La madurez institucional se construye de forma progresiva: primero se formaliza el propósito y la capacidad básica de respuesta; luego se amplían servicios, horarios y especialidades según demanda, riesgo y recursos disponibles.

Resultado esperado: Una capacidad nacional reconocida, accesible y confiable, capaz de coordinar incidentes sin invadir las responsabilidades operativas o legales de las entidades atendidas.

2. Gobernanza, interesados y constitución

Mapa de actores

La planificación comienza con la identificación de partes interesadas. La guía distingue patrocinadores, clientes, proveedores, socios estratégicos y actores con influencia. Entre ellos pueden figurar la Presidencia, ministerios, Poder Legislativo y Judicial, defensa, fuerzas del orden, reguladores, proveedores de Internet, sector financiero, operadores de infraestructura crítica, academia, empresas tecnológicas, sociedad civil y organismos internacionales. Un mismo actor puede cumplir varios papeles.

No basta con enumerarlos. El equipo del proyecto debe analizar interés, influencia y posición frente a la iniciativa. Los actores con alto poder y alto interés requieren gestión cercana; los de alto poder y menor interés deben mantenerse satisfechos; quienes muestran alto interés y menor capacidad de influencia deben mantenerse informados. Entrevistas, talleres y actas de acuerdos permiten detectar expectativas, fuentes de apoyo y posibles resistencias.

Documento de constitución

El documento de constitución establece la razón de ser del CSIRT y sirve como referencia durante todo su ciclo de vida. Debe definir la naturaleza de la organización, objetivos, misión, visión, comunidad atendida, marco institucional y fundamento legal. La misión expresa qué hace el equipo, para quién y bajo qué valores; la visión fija la posición futura que aspira a alcanzar. Ambas deben ser claras, estables y aprobadas por representantes con autoridad suficiente.

Ubicación institucional

La entidad anfitriona debe poder influir en políticas nacionales de seguridad de las TIC, acceder a los niveles superiores de gobierno, obtener financiamiento y disponer de jurisdicción y autonomía apropiadas. El CSIRT puede constituirse como organización independiente o como unidad de otra institución; también puede incorporar participación del sector privado, la academia o la sociedad civil. La elección debe documentar responsabilidades, autoridad, interacción con interesados, recursos, infraestructura, resiliencia y modelo de financiamiento.

Debido al carácter transversal de la respuesta a incidentes, resulta conveniente un comité directivo o de coordinación con representación seleccionada. Sus facultades —consultivas o vinculantes— deben quedar expresamente definidas para evitar ambigüedades en crisis.

Riesgo de gobernanza: Un CSIRT situado lejos de los centros de decisión, sin autonomía operativa o sin una fuente estable de financiamiento difícilmente podrá coordinar incidentes de alcance nacional.

3. Marco legal, alcance y comunidad objetivo

Fundamento jurídico

El marco legal debe otorgar existencia y autoridad al CSIRT mediante el instrumento compatible con el ordenamiento del país —ley, decreto, resolución u otra figura—. Su revisión debe involucrar especialistas jurídicos del gobierno, la academia o ambos. Un diseño deficiente puede generar conflictos de competencia, exposición a litigios, obstáculos para intercambiar información o limitaciones para actuar durante un incidente.

El análisis jurídico debe responder, como mínimo, si el mandato contradice normas vigentes o deja vacíos explotables; qué instrumento institucionaliza al equipo; qué medidas permiten financiarlo; cómo se contratará al personal; qué reglas aplican al tratamiento de datos, confidencialidad, preservación de evidencia y cooperación; y qué límites existen frente a investigación penal, defensa o inteligencia. Sus conclusiones deben anexarse al documento de constitución.

Definición del alcance

Una vez aprobados misión, visión y marcos institucional y legal, el país debe establecer con precisión qué entidades recibirán servicios y bajo qué condiciones. La comunidad objetivo puede abarcar todo el gobierno, determinados sectores, infraestructuras críticas, empresas o una combinación de ellos. También puede haber niveles de servicio diferenciados según criticidad, capacidades existentes y acuerdos formales.

La delimitación debe reconocer a organizaciones que ya cuentan con equipos propios —por ejemplo, defensa, grandes operadores o sectores regulados— y definir cómo se coordinarán con el CSIRT nacional. La promesa de cobertura universal sin personal, procedimientos y presupuesto suficientes genera expectativas imposibles de cumplir.

Reglas de relacionamiento

- Publicar canales oficiales, horarios, criterios de admisión, prioridades, tiempos orientativos y condiciones de confidencialidad.
- Formalizar, cuando corresponda, acuerdos de cooperación, convenios de intercambio, cláusulas de confidencialidad y niveles de servicio.
- Definir responsabilidades del reportante, del CSIRT, de proveedores y de autoridades durante el análisis, la contención y la recuperación.
- Establecer mecanismos para compartir información con control de acceso, propósito definido y protección acorde con su sensibilidad.

Criterio ejecutivo: El alcance debe ser jurídicamente válido, operativamente alcanzable y comprensible para toda la comunidad.

4. Catálogo de servicios y evolución

La guía agrupa la cartera en servicios reactivos, proactivos y de valor agregado. La selección debe surgir de los riesgos y necesidades de la comunidad, no de la imitación de otros equipos. Cada servicio requiere propietario, procedimientos, recursos, horarios, niveles de atención, canales, métricas y dependencias. La ampliación debe producirse solo cuando la operación básica sea estable.

Familia	Finalidad	Ejemplos prioritarios
Reactivos	Atender hechos que ya ocurrieron y reducir su impacto.	Recepción y clasificación; análisis; coordinación; contención; recuperación; manejo de vulnerabilidades y artefactos.
Proactivos	Disminuir probabilidad e impacto antes de que se materialice un incidente.	Alertas; avisos; evaluaciones; monitoreo; pruebas; gestión y divulgación responsable de vulnerabilidades.
Valor agregado	Elevar la madurez de la comunidad y anticipar necesidades futuras.	Concientización; formación; ejercicios; asesoría; I+D; análisis de tendencias y apoyo a políticas públicas.

Núcleo operativo recomendado

La capacidad inicial debe priorizar un punto único de contacto, un mecanismo de registro y seguimiento, clasificación por tipo y gravedad, procedimientos de escalamiento, coordinación con la entidad afectada y documentación de decisiones. El CSIRT debe poder mantener trazabilidad desde el reporte hasta el cierre, preservar la información relevante y convertir cada caso en conocimiento reutilizable.

Criterios de priorización

- Impacto sobre servicios esenciales, seguridad pública, economía, gobierno o derechos de las personas.
- Extensión geográfica, número de entidades afectadas y posibilidad de propagación.
- Sensibilidad de la información comprometida y consecuencias legales o reputacionales.
- Disponibilidad de capacidades alternativas y necesidad de coordinación nacional o internacional.

Evolución controlada

El paso de una postura reactiva a otra preventiva exige información, personal y disciplina operacional. Las alertas y evaluaciones deben ser oportunas y accionables; la formación debe responder a brechas observadas; la investigación y el análisis de tendencias deben alimentar decisiones. La efectividad no se mide por la cantidad de servicios anunciados, sino por su utilidad, calidad, oportunidad y sostenibilidad.

Advertencia: Ofrecer atención permanente o análisis especializado sin turnos, competencias y herramientas suficientes deteriora la confianza y crea una falsa sensación de seguridad.

5. Organización, talento y sostenibilidad

Estructura organizacional

La organización debe reflejar la cartera de servicios. La guía propone cuatro áreas principales: Dirección, Operaciones, Investigación y Desarrollo (I+D) y Tecnología de Información (TI). Dirección asegura estrategia, relaciones, presupuesto y rendición de cuentas. Operaciones recibe y gestiona incidentes. I+D desarrolla capacidades, analiza malware, vulnerabilidades y tendencias. TI administra la plataforma que soporta al propio CSIRT. En equipos pequeños, una persona puede desempeñar varias funciones, pero deben conservarse responsabilidades claras y controles de segregación.

Perfiles y selección

La contratación es uno de los mayores desafíos. Los cargos directivos requieren liderazgo, experiencia técnica y capacidad de coordinación. Operaciones demanda criterio, organización, resistencia a la presión y comunicación. I+D necesita disciplina analítica, desarrollo de sistemas y conocimientos forenses. TI exige administración segura de sistemas, redes y servicios. La formación universitaria y las certificaciones son referencias útiles, pero la selección debe valorar experiencia práctica, ética, colaboración y capacidad de aprendizaje.

Programa de formación

- Fundamentos de seguridad de la información, gestión de riesgos, redes, sistemas y criptografía.
- Manejo de incidentes: triaje, análisis, coordinación, contención, recuperación, comunicación y lecciones aprendidas.
- Análisis forense, respuesta avanzada, análisis de malware, vulnerabilidades y preservación de evidencia.
- Gestión, liderazgo, comunicación ejecutiva, negociación y cooperación interinstitucional.

La capacitación debe planificarse como una capacidad continua. Conviene combinar formación externa, laboratorios, simulaciones, mentoría y transferencia interna de conocimientos. La dependencia de cursos o certificaciones aisladas no reemplaza procedimientos practicados y experiencia operacional.

Presupuesto y cronograma

El presupuesto debe cubrir no solo la puesta en marcha, sino salarios, guardias, formación, licencias, mantenimiento, comunicaciones, soporte, viajes, membresías, reposición tecnológica y contingencias. El cronograma debe vincular actividades, responsables, dependencias, productos y criterios de aceptación. La inauguración pública no debe fijarse antes de probar procesos, canales, personal y tecnología.

Sostenibilidad: La financiación inicial crea el equipo; el financiamiento recurrente, la retención del talento y la renovación tecnológica lo mantienen operativo.

6. Infraestructura física y tecnológica

Instalaciones

El CSIRT manejará información sensible y deberá funcionar durante situaciones de presión. Sus instalaciones requieren control de acceso, registro y acompañamiento de visitas, protección de áreas restringidas, almacenamiento bajo llave, vigilancia, energía y comunicaciones resilientes. Deben contemplarse espacios para Operaciones, TI, I+D, coordinación, formación, logística y, según madurez, laboratorio, centro de monitoreo o sala de crisis.

Arquitectura de red

La guía recomienda segmentar al menos cinco zonas: Internet, DMZ externa, DMZ interna, laboratorio de pruebas y LAN del CSIRT. Los servicios públicos —sitio web o correo— se ubican en la DMZ externa; los servicios internos —archivos, tickets y herramientas— no deben publicarse en Internet; el laboratorio debe aislar software, malware y equipos potencialmente comprometidos para que las pruebas no afecten el entorno productivo. La complejidad y las barreras deben aumentar conforme crezcan los servicios y el riesgo.

Plataforma mínima

- Sistema de registro y seguimiento de incidentes, integrado con correo y formularios, con colas, asignación, escalamiento y base de conocimiento.
- Servicios institucionales de web, correo, intranet, archivos, DNS y copias de seguridad, con administración y monitoreo dedicados.
- Recolección y correlación de eventos, monitoreo de activos y mecanismos de alerta conforme al alcance autorizado.
- Equipos de trabajo exclusivos, telefonía, almacenamiento controlado y mecanismos seguros para destruir información y soportes.

Controles esenciales

La arquitectura debe incorporar mínimo privilegio, autenticación robusta, registros protegidos, copias de seguridad fuera del sitio, cifrado, gestión de vulnerabilidades, administración de cambios y recuperación. La información de casos no debe mezclarse con entornos personales ni almacenarse en servicios no autorizados. Las herramientas han de seleccionarse por su adecuación al proceso y por su costo de ciclo de vida, no por notoriedad comercial.

Prioridad tecnológica: El sistema de gestión de incidentes es la fuente institucional de verdad: conserva comunicaciones, decisiones, tiempos, responsables, evidencias y conocimiento acumulado.

7. Políticas, procedimientos y cierre formal

Políticas mínimas

Las políticas traducen el mandato y los compromisos de los patrocinadores en reglas operativas. Deben proteger confidencialidad, integridad, disponibilidad y calidad del servicio. La guía identifica como mínimo políticas de clasificación, protección, retención, destrucción, divulgación y acceso a la información; uso aceptable de sistemas; definición de eventos e incidentes; gestión de incidentes; y cooperación con terceros.

A ellas pueden añadirse políticas de notificación, comunicaciones, capacitación, seguridad de estaciones y redes, correo, dispositivos móviles, telecomunicaciones, copias de seguridad, segregación de funciones, control de cambios y contraseñas. Cada política debe tener propietario, alcance, responsabilidades, excepciones, mecanismos de cumplimiento y calendario de revisión.

Procedimientos operativos

- Recepción, validación, clasificación, priorización y asignación de reportes.
- Análisis técnico, coordinación, escalamiento, comunicación, preservación de evidencia y cierre.
- Gestión de vulnerabilidades, divulgación responsable, alertas y relación con proveedores.
- Activación de guardias, crisis, continuidad, recuperación y comunicaciones públicas.
- Revisión posterior al incidente, incorporación de lecciones y actualización de controles.

Cierre del proyecto

El establecimiento concluye cuando se verifica la integridad de los productos y el patrocinador aprueba formalmente el resultado. Deben existir lista de interesados, documento de constitución, soporte legal, instalaciones y contratos, personal contratado y capacitado, manual de operaciones, infraestructura tecnológica y acuerdos de soporte. También deben confirmarse alcance, presupuesto y cronograma ejecutados.

El informe final debe registrar objetivo, actividades, desempeño frente a alcance, plazo y presupuesto, lecciones aprendidas y recomendaciones. La sesión de cierre no es un acto administrativo menor: permite corregir deficiencias antes de transferir la responsabilidad desde el equipo del proyecto hacia la operación permanente del CSIRT.

Criterio de aceptación: El CSIRT está listo cuando puede recibir, priorizar, coordinar, documentar y cerrar incidentes mediante personal, procesos y tecnología probados; no simplemente cuando dispone de una oficina o herramientas.

8. Hoja de ruta para la alta dirección

La secuencia siguiente convierte las buenas prácticas de la OEA en decisiones de implantación. Debe ajustarse al marco jurídico, al perfil de riesgo y a la capacidad institucional del país.

1. Mandato y patrocinio. Designar patrocinador, gerente del proyecto y equipo multidisciplinario; acordar misión, visión, autoridad, comunidad y fuente de financiamiento recurrente.

2. Gobernanza y legalidad. Mapear interesados, definir ubicación institucional y comité de coordinación, validar competencias, protección de información, contratación y cooperación.

3. Diseño del servicio. Priorizar servicios iniciales, horarios, canales, criterios de severidad, escalamiento, niveles de atención, responsabilidades y métricas.

4. Capacidad operativa. Contratar y formar al personal; habilitar instalaciones seguras; desplegar tickets, comunicaciones, almacenamiento, monitoreo, copias y laboratorio aislado.

5. Control y prueba. Aprobar políticas y procedimientos; realizar ejercicios de extremo a extremo; corregir hallazgos; verificar continuidad y soporte.

6. Puesta en marcha. Comunicar oficialmente alcance y contactos; activar mecanismos de cooperación; iniciar con una cartera controlada y seguimiento ejecutivo.

7. Mejora continua. Revisar incidentes, riesgos, satisfacción, tiempos, recurrencia, desempeño y presupuesto; ampliar servicios solo con evidencia de demanda y capacidad.

Conclusión

La guía presenta al CSIRT nacional como una capacidad soberana de coordinación y confianza. Su éxito depende menos de la cantidad de tecnología adquirida que de la coherencia entre mandato, comunidad, servicios, talento, procesos y recursos. Una constitución jurídicamente sólida, una cartera realista y una operación trazable permiten responder con rapidez sin sacrificar confidencialidad, control ni rendición de cuentas.

Para la alta dirección, la prioridad es asegurar continuidad institucional: presupuesto recurrente, autoridad para coordinar, personal estable y mecanismos de cooperación. Para la dirección técnica, el desafío consiste en convertir esos elementos en procedimientos practicados, infraestructura segmentada y conocimiento acumulativo. El resultado esperado es un CSIRT capaz de reducir el impacto de los incidentes, acelerar la recuperación y fortalecer la resiliencia nacional.

Fuente

Organización de los Estados Americanos. (2016). *Buenas prácticas para el establecimiento de un CSIRT nacional*. Programa de Ciberseguridad del CICTE/OEA.