qualoom®

Inspiring Technology
for People

Plantilla avanzada de Plan de Respuesta a Incidentes

Área de Ciberseguridad
Fecha 28/04/2026
Versión 1.0
Clasificación: Público

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Importancia estratégica de un **plan de respuesta a incidentes**

El **Plan de Respuesta a Incidentes (PRI)** constituye un componente esencial dentro de la gestión de riesgos de ciberseguridad de cualquier organización. Su correcta implementación permite la identificación, contención y remediación de incidentes de manera eficiente, minimizando el impacto operativo, financiero y reputacional.

El PRI se alinea con los **estándares internacionales de referencia,** incluyendo **NIST SP 800-61 e ISO 27035,** asegurando que la organización adopte prácticas consistentes con los marcos reconocidos de la industria. La existencia de un PRI formalizado contribuye a:

Mitigación de riesgos

Reducción de interrupciones operativas y pérdida de activos críticos.

Continuidad del negocio

Garantizar la resiliencia y la disponibilidad de servicios esenciales.

Cumplimiento regulatorio

Facilitando auditorías y reporte ante autoridades nacionales e internacionales.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Modelo organizativo del CSIRT

La respuesta eficaz ante incidentes de ciberseguridad requiere una **estructura de gobernanza clara**, con roles y responsabilidades formalmente definidos. Para ello, la organización debe disponer de un **Equipo de Respuesta a Incidentes de Seguridad (CSIRT)** responsable de la gestión integral de los incidentes, desde su detección hasta su cierre.

Composición del CSIRT

El **equipo de respuesta** debe estar compuesto, como mínimo, por los siguientes perfiles:

Coordinador del CSIRT

Dirección global del incidente, toma de decisiones estratégicas, priorización de acciones y escalado a la alta dirección y partes interesadas.

Analistas de seguridad

Detección y análisis técnico del incidente, ejecución de acciones de contención, erradicación de la amenaza y apoyo en la recuperación de los sistemas afectados.

Especialistas forenses

Gestión regulatoria y comunicaciones internas y externas. Responsables legales y comunicación

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Modelo organizativo del CSIRT

Responsables legales y de comunicación

Evaluación del impacto legal y regulatorio, gestión de notificaciones obligatorias y coordinación de las comunicaciones internas y externas.

Contactos críticos y escalado

El CSIRT debe disponer de una lista actualizada de contactos críticos, incluyendo:

Proveedores tecnológicos y de servicios de seguridad.

CERT/CSIRT nacionales o sectoriales.

Autoridades regulatorias y **organismos** competentes.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Identificación y priorización de incidentes

Una **clasificación y categorización adecuada de los incidentes de ciberseguridad** es fundamental para garantizar una respuesta coherente, proporcional al riesgo y alineada con los objetivos del negocio.

De acuerdo con **ISO 27035**, se considera incidente de seguridad cualquier evento o conjunto de eventos que comprometa, o tenga el potencial de comprometer, la **confidencialidad, integridad o disponibilidad** de los activos de información de la organización.

Clasificación por tipo de incidente

Malware — Infección por software malicioso, incluyendo ransomware y spyware.

Acceso no autorizado — Infección por software malicioso, incluyendo ransomware y spyware.

Fuga o exposición de datos — Pérdida, robo o divulgación no autorizada de información.

DoS/DDoS — Denegación de servicio, interrupción de la disponibilidad de servicios.

Fraude — Actividades maliciosas con impacto económico o reputacional.

Incidentes físico-tecnológicos — Fallos o manipulaciones que afecten a infraestructuras críticas

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology for People

Identificación y priorización de incidentes

Niveles de seguridad

Nivel	Descripción
BAJO	Impacto limitado y fácilmente controlable, sin afectación relevante a servicios ni activos críticos.
MEDIO	Impacto moderado sobre servicios o activos, que requiere intervención controlada para su resolución.
ALTO	Afectación significativa a operaciones críticas, con impacto operativo, financiero o reputacional potencial.
CRÍTICO	Impacto grave en el negocio, la seguridad de la información o el cumplimiento legal y regulatorio, requiriendo respuesta inmediata y escalado.

Criterios de priorización

La priorización de los incidentes debe basarse en criterios objetivos, tales como:

- Impacto sobre activos críticos y procesos de negocio.
- Alcance y propagación del incidente.
- Riesgos legales, regulatorios y reputacionales.
- Urgencia de respuesta y dependencia de terceros

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Fases del ciclo de respuesta a incidentes

El **ciclo de respuesta a incidentes** es un proceso estructurado que garantiza que los eventos de ciberseguridad se gestionen de manera eficiente, minimizando el impacto operativo y asegurando la trazabilidad de todas las acciones. Este ciclo, basado en los lineamientos de NIST SP 800-61, comprende seis fases fundamentales:

PREPARACIÓN

FASE 1

Define **políticas, procedimientos y protocolos** de seguridad, incorpora herramientas de **monitoreo y detección**, y asegura la **capacitación** del personal para responder con eficacia a posibles incidentes. Esta fase establece las **bases para una respuesta organizada y coherente.**

IDENTIFICACIÓN

FASE 2

Implica la detección temprana de incidentes mediante sistemas de monitoreo y la validación de alertas. Toda actividad sospechosa se registra, clasificando el incidente según su severidad y priorizando la respuesta según criterios de riesgo.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Fases del ciclo de respuesta a incidentes

CONTENCIÓN

FASE 3

Busca **limitar la propagación del incidente.** Incluye acciones inmediatas para aislar sistemas afectados y medidas estratégicas de corto y largo plazo para proteger la infraestructura crítica y los activos comprometidos.

ERRADICACIÓN

FASE 4

Se centra en **eliminar la causa del incidente**, eliminando malware, accesos no autorizados y restaurando los sistemas a un estado seguro. También se aplican medidas preventivas adicionales para evitar recurrencias.

RECUPERACIÓN

FASE 5

Asegura la reactivación controlada de servicios y sistemas críticos, verificando la integridad de la información y monitorizando la infraestructura para confirmar que la amenaza ha sido neutralizada.

LECCIONES APRENDIDAS

FASE 6

Consiste en el análisis posterior al incidente, documentando causas, impactos y medidas correctivas. Esta fase permite actualizar políticas, procedimientos y planes de respuesta, fortaleciendo la resiliencia organizativa frente a futuros incidentes.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Flujos operativos para la gestión técnica de incidentes

La gestión técnica de un incidente de ciberseguridad requiere **protocolos claros y procedimientos estandarizados** que permitan una respuesta rápida, eficiente y trazable. Esta sección describe las principales áreas de actuación del CSIRT durante un incidente.

Protocolos de contención

La contención busca limitar la propagación del incidente y reducir su impacto sobre los sistemas críticos. Incluye acciones como:

Desconexión inmediata de sistemas comprometidos para evitar la propagación de amenazas

Suspensión preventiva de credenciales comprometidas, garantizando la protección de cuentas críticas mientras se analiza.

Configuración temporal de firewalls, segmentación de redes y control de accesos, asegurando que solo personal autorizado pueda interactuar con los sistemas afectados.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Flujos operativos para la gestión técnica de incidentes

La gestión técnica de un incidente de ciberseguridad requiere **protocolos claros y procedimientos estandarizados** que permitan una respuesta rápida, eficiente y trazable. Esta sección describe las principales áreas de actuación del CSIRT durante un incidente.

Protocolos de contención

La contención busca limitar la propagación del incidente y reducir su impacto sobre los sistemas críticos. Incluye acciones como:

Desconexión inmediata de sistemas comprometidos para evitar la propagación de amenazas

Suspensión preventiva de credenciales comprometidas, garantizando la protección de cuentas críticas mientras se analiza.

Configuración temporal de firewalls, segmentación de redes y control de accesos, asegurando que solo personal autorizado pueda interactuar con los sistemas afectados.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Flujos para la gestión técnica de incidentes

Análisis forense

El análisis forense asegura la **preservación de evidencia digital** y la trazabilidad completa del incidente, cumpliendo con requisitos legales y regulatorios:

Captura de imágenes forenses de sistemas afectados y registros de logs relevantes.

Mantenimiento riguroso de la cadena de custodia para garantizar integridad y validez de la evidencia.

Documentación detallada de cada paso del análisis, permitiendo futuras auditorías o investigaciones judiciales si corresponde

Gestión de comunicaciones

Una comunicación adecuada es fundamental para la coordinación interna y el cumplimiento de obligaciones externas:

INTERNA: informes periódicos a directivos, gerentes de áreas afectadas y miembros del CSIRT.

EXTERNA: notificaciones a reguladores, clientes, según la gravedad y requerimientos legales.

La comunicación debe ser controlada, consistente y basada en hechos verificados, para minimizar riesgos reputacionales.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Flujos para la gestión técnica de incidentes

Acciones específicas según tipo de incidente

Los procedimientos técnicos deben adaptarse al tipo de incidente detectado:

Ransomware Aislamiento de sistemas infectados, análisis de cifrado y restauración segura de respaldos.

Acceso no autorizado Análisis de vectores de ataque y eliminación de accesos indebidos.

Fuga de datos Identificación de la fuente de exfiltración, cierre de brechas y notificación a autoridades si aplica.

DoS/DDoS Mitigación del tráfico malicioso y fortalecimiento de la infraestructura para restablecer disponibilidad.

Fraude Investigación forense y medidas disciplinarias o legales.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Registro y trazabilidad del incidente

La **documentación y reporting de incidentes** es un elemento crítico dentro de la gestión de ciberseguridad, ya que garantiza la trazabilidad de todas las acciones realizadas, facilita la evaluación del impacto y permite la mejora continua del Plan de Respuesta a Incidentes (PRI). Un registro completo asegura que cada evento pueda ser auditado, analizado y utilizado para fortalecer la resiliencia organizativa.

Registro de incidentes

Fecha y hora de detección

Momento exacto en que se identificó el incidente.

Sistemas afectados

Activos y servicios impactados.

Evidencias recolectadas

Logs, capturas forenses, archivos relevantes y cualquier información necesaria para análisis posterior.

Acciones realizadas

Medidas tomadas durante contención, erradicación y recuperación.

Responsables involucrado

Personal del CSIRT y otras áreas implicadas en la respuesta.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Registro y trazabilidad del incidente

Métricas clave (KPIs)

MTTD

Mean Time to Detect, tiempo promedio **desde la aparición del incidente hasta su detección.**

MTTR

Mean Time to Respon, tiempo promedio de **respuesta efectiva al incidente.**

Número de incidentes por categoría

Permite identificar patrones y priorizar recursos de seguridad.

Métricas clave (KPIs)

La información recopilada debe sintetizarse en informes claros para la dirección y auditores, facilitando la toma de decisiones estratégicas. Estos informes incluyen:

- **Resumen del incidente y acciones** correctivas implementadas.
- **Visualización de métricas clave** y tendencias de seguridad.
- **Recomendaciones** de mejora para prevenir recurrencias y optimizar procesos.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Comunicaciones estratégicas ante incidentes

La gestión de la comunicación durante un incidente de ciberseguridad debe ser estructurada, clara y trazable, garantizando coordinación interna, cumplimiento legal y protección de la reputación corporativa.

Escalado interno

- Notificación inmediata al CSIRT según nivel de severidad.
- Información periódica a áreas afectadas y alta dirección.
- Protocolos definidos para asegurar respuesta oportuna y coordinada.

Notificación a autoridades

- Cumplimiento de **plazos legales y regulatorios, e.g., GDPR**
- Reporte claro del **alcance, impacto y medidas** correctivas implementadas.
- Registro formal de cada notificación para auditoría y trazabilidad.

Comunicación externa

- Coordinación de mensajes hacia clientes, proveedores y socios.
- Gestión de información hacia medios de comunicación, solo en casos críticos.
- Mensajes consistentes, verificados y alineados con la estrategia corporativa.

Copyright @2026 Qualoom Expertise Technology

qualoom®

Inspiring Technology
for People

Fortaleciendo la resiliencia digital

La implementación de **un Plan de Respuesta a Incidentes (PRI)** estructurado y alineado con estándares internacionales es un elemento crítico para cualquier organización que busque proteger sus activos, garantizar la continuidad del negocio y cumplir con sus obligaciones regulatorias.
Un PRI eficaz permite:

Responder con rapidez y precisión ante cualquier incidente de ciberseguridad.

Minimizar impactos operativos, financieros y reputacionales, asegurando la continuidad de los servicios críticos.

Documentar y analizar cada incidente, promoviendo la mejora continua y la resiliencia organizativa.

Coordinar comunicaciones internas y externas de forma controlada, cumpliendo con requisitos legales y preservando la confianza de clientes y socios.

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Fortalece la resiliencia de tu organización hoy

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Copyright @2026 Qualoom Expertise Technology

Más información www.qualoom.es