qualoom®

Inspiring Technology
for People

Resolución de Incidentes de Alta Criticidad: **Protocolo, Análisis y Documentación Técnica**

Área de Soporte Informático
Fecha 07/01/2026
Versión 1.0
Clasificación: Público

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

01 Cuando el tiempo cuenta, el proceso importa

02 Identificar antes de actuar

03 Guía operativa para momentos críticos

04 Tecnología al servicio del tiempo de reacción

05 Aprender para no repetir

06 Del caos a la estructura

07 Un incidente crítico es una oportunidad de mejora

qualoom®

Inspiring Technology
for People

Introducción.
Cuando el tiempo cuenta, el proceso importa

Los incidentes de alta criticidad son inevitables en cualquier infraestructura tecnológica compleja. No se trata de si ocurrirán, sino de **cuándo y cómo se manifestarán.**

La diferencia entre un impacto devastador y una recuperación controlada radica en la **aplicación de un protocolo estandarizado, documentado y probado.**

Este documento proporciona una visión integral para:

- Responder con precisión y rapidez.
- Coordinar equipos bajo presión.
- Documentar cada fase con criterios técnicos verificables.
- Prevenir recurrencias mediante análisis estructurados.

qualoom®

Inspiring Technology
for People

Identificar antes de actuar

La clasificación temprana de un incidente crítico es el primer paso para garantizar una respuesta eficiente.
Cada tipo de incidente conlleva riesgos específicos y **requiere protocolos adaptados:**

Pérdida de servicio

Impacto

Paralización inmediata de operaciones críticas.

Ejemplo

Caída de servidores productivos, interrupción de red troncal.

Riesgo asociado

Pérdidas económicas por minuto de inactividad y afectación directa a clientes.

Brechas de seguridad

Impacto

Exposición de información confidencial, acceso no autorizado o compromisos de infraestructura.

Ejemplo

intrusión detectada en servidores externos, filtración de credenciales en la Dark Web.

Riesgo asociado

sanciones regulatorias, pérdida de confianza de clientes y daño reputacional.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Identificar antes de actuar

Fallos en sistemas core

Impacto

Interrupción en los procesos nucleares de la organización (ERP, core, bancario, etc.)

Ejemplo

Fallo en el motor de procesamiento de pagos o en el sistema de reservas.

Riesgo asociado

Degradación masiva de la experiencia del cliente y retrasos operativos de gran escala.

Corrupción de datos

Impacto

Imposibilidad de confiar en registros y transacciones.

Ejemplo

Corrupción en bases de datos financieras o borrado accidental de sistemas de almacenamiento crítico.

Riesgo asociado

Afectación a la continuidad del negocio y posibles incumplimientos legales.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Guía operativa para momentos críticos

Un protocolo bien estructurado permite **actuar bajo presión sin perder precisión.** A continuación, se detalla el flujo recomendado:

Detección y priorización

Identificar el incidente, categorizar su impacto y severidad.

01

02

Activación de equipo de respuesta

Reunir roles clave con responsabilidades definidas.

Comunicación interna y externa

Flujos claros hacia dirección, usuarios y clientes.

03

04

Análisis técnico inmediato

Identificación de causa probable y mitigación inicial.

Recuperación y control

Restauración de servicios y monitorización post-reincorporación

05

qualoom®

Inspiring Technology
for People

Tecnología al servicio del tiempo de reacción

Durante la gestión de incidentes críticos, la rapidez y precisión de la respuesta depende en gran medida del soporte tecnológico disponible.
Contar con soluciones que faciliten la coordinación, el registro de eventos y la recuperación rápida de sistemas permite a los equipos responder de manera ordenada y precisa.

War rooms virtuales — Entornos de colaboración en tiempo real. Teams, Slack, Zoom

Logs centralizados y time stamping — Para seguimiento y auditoría precisa de eventos.

Integración con herramientas de ticketing y CMDB — Trazabilidad de activos y relación con incidentes anteriores.

Scripts de rollback y restauración rápida — automatización de procesos de recuperación segura

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Aprender para no repetir

El análisis de causa raíz (Root Cause Analysis, RCA) es un componente esencial para fortalecer la resiliencia de la organización. Su objetivo no es solo entender qué ocurrió, sino identificar por qué sucedió y cómo se pueden implementar medidas que eviten su recurrencia.
Un RCA estructurado incluye:

Qué pasó

Descripción precisa del incidente y su impacto en sistemas y procesos.

Por qué ocurrió

Identificación de fallas técnicas, humanas o de proceso que provocaron el evento

Cómo prevenirlo

Cómo prevenirlo: medidas correctivas y preventivas, ajustes de procedimientos y recomendaciones de mejora continua.

La documentación técnica post-incidente permite:

- ☑ Consolidar hallazgos
- ☑ Mantener una base de conocimiento activa
- ☑ Generar informes que respalden auditorías y revisiones internas.

Integrar estos aprendizajes en protocolos y entrenamientos futuros es clave para **reducir tiempos de respuesta y mejorar la coordinación de los equipos ante futuros incidentes**

qualoom®

Inspiring Technology
for People

Del caos a **la estructura**

Los **protocolos bien definidos y ensayados** marcan la diferencia en incidentes críticos.

Restauración en 30 minutos

Reactivación de sistemas críticos gracias a **procedimientos previamente ensayados.**

Prevención de recurrencias

Análisis en un entorno financiero que **evitó la repetición de fallos críticos.**

Coordinación cross-team eficaz

Gestión remota de un incidente nocturno con **equipos distribuidos.**

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Un incidente crítico es una **oportunidad de mejora**

La gestión de incidentes de alta criticidad no se mide solo por la rapidez de respuesta, sino por la capacidad de aprender y reforzar procesos. Cada incidente manejado correctamente se convierte en una **oportunidad para optimizar protocolos, fortalecer la seguridad y garantizar la continuidad del negocio.**

Un enfoque estructurado incluye:

- **Documentación completa**: evidencia técnica y acciones registradas.
- **Análisis de causa raíz (RCA):** identificar causas y medidas preventivas.
- **Mejora continua:** integrar aprendizajes en protocolos y entrenamientos.
- **Coordinación y comunicación:** flujos claros entre equipos y stakeholders.

Las organizaciones que adoptan este enfoque logran no solo minimizar el impacto operativo, sino también consolidar la confianza de clientes y usuarios.

qualoom®

Inspiring Technology
for People

Actúa con **precisión y control** en cualquier situación.

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es