GRCForce

Modelo de gobernanza de respuesta a incidentes: Lista de preparación y guía de simulación

8 de julio de 2026

grcforce.com/es/#contact

Practical governance, risk and compliance guidance for European organisations.

Lista de preparación y guía de simulación

Una guía práctica para la respuesta a incidentes, el mando de crisis y la preparación de las notificaciones regulatorias.

Utilice esta guía antes de su próximo ejercicio, revisión regulatoria o conversación de aseguramiento de la resiliencia. Ayuda a CISOs, responsables de GRC, responsables de incidentes y alta dirección a comprobar si la gobernanza situada por encima de la respuesta técnica resistirá bajo presión.

Contenido

- Matriz del modelo de gobernanza de respuesta a incidentes
- Lista de preparación
- Referencia de notificación regulatoria
- Clasificación de gravedad de incidentes
- Guía priorizada de simulación
- Cinco preguntas para la primera hora
- Una acción para esta semana
- Siguiente paso

Un modelo práctico para respuesta a incidentes, mando de crisis y notificación regulatoria

En una crisis, las organizaciones descienden hasta el nivel de su preparación.

La mayoría tiene un plan de respuesta a incidentes. Muchas menos han probado si funciona realmente la gobernanza situada por encima de la capa técnica: quién tiene autoridad de mando, quién comunica externamente, quién decide entre contención y continuidad y si puede cumplirse el plazo regulatorio de notificación.

Utilice esta guía para:

- Comprobar si el plan es operativamente realista
- Preparar ejercicios de notificación bajo NIS2, DORA o normas sectoriales
- Diseñar o mejorar la estructura de mando de crisis
- Planificar un ejercicio de mesa o una simulación
- Revisar acciones de gobernanza después de un incidente real
- Mantener conversaciones de aseguramiento con consejos, clientes o reguladores

El objetivo no es crear más documentación, sino saber si el modelo resistirá cuando la presión sea real.

Matriz del modelo de gobernanza

Capa	Preparar	Responder	Aprender	Responsable de evidencias	Estado
1. Mando	Funciones y suplentes identificados; escalado documentado	Responsable del incidente activo, cadencia clara y derechos de decisión comprendidos	Revisión de carencias tras ejercicios e incidentes	Director del incidente / CISO	Verde / Ámbar / Rojo

Capa	Preparar	Responder	Aprender	Responsable de evidencias	Estado
2. Decisiones	Umbrales de aprobación y decisores suplentes definidos	Decisiones críticas tomadas en el nivel adecuado sin retrasos	Cuellos de botella analizados y corregidos	Director del incidente / Dirección ejecutiva	Verde / Ámbar / Rojo
3. Comunicaciones	Plantillas internas, para clientes, medios y personal preparadas	Mensajes aprobados y emitidos en la secuencia y canal adecuados	Retrasos y confusión registrados para mejora	Comunicación / Jurídico	Verde / Ámbar / Rojo
4. Notificación	Obligaciones, plazos, contactos y plantillas documentados	La cadena de aprobación funciona bajo presión	Los fallos o retrasos generan mejoras	Cumplimiento / Jurídico	Verde / Ámbar / Rojo
5. Aprendizaje	Método y responsable de revisión acordados	Evidencias recopiladas durante el evento	Acciones seguidas hasta cierre e incorporadas al modelo	GRC / Riesgos	Verde / Ámbar / Rojo

Puntuación rápida

- Verde: documentado, asignado, actualizado y probado
- Ámbar: existe, pero está desactualizado, incompleto o es poco claro bajo presión
- Rojo: ausente, sin responsable o probablemente fallará en un evento real

Si existen más de dos capas en rojo, corrija primero el modelo antes de realizar otro ejercicio.

Lista de preparación

1. La autoridad de mando está asignada

- Una persona identificada tiene autoridad operativa sobre el incidente
- Una persona sénior identificada es responsable de la crisis a nivel ejecutivo
- El escalado de incidente a crisis está documentado y comprendido
- Existen suplentes para todas las funciones críticas
- La estructura se ha probado en los últimos 12 meses

Fallo habitual: la autoridad aparece en un documento, pero las personas no la comprenden.

2. Los derechos de decisión son explícitos

- El equipo técnico sabe qué puede aprobar sin escalado
- La dirección sabe qué decisiones requieren participación ejecutiva
- Los umbrales de notificación al consejo están documentados
- Pago, apagado y comunicaciones relevantes tienen vías preacordadas
- Ninguna decisión crítica depende de una sola persona no disponible

Fallo habitual: el plan explica qué debe ocurrir, pero no quién puede decidirlo.

3. Las comunicaciones están preparadas

- Plantillas internas de crisis preparadas y accesibles
- Declaraciones provisionales para clientes y socios
- Canales alternativos disponibles si fallan los sistemas corporativos
- Redacción para medios cuando proceda
- Cadena de aprobación probada

Fallo habitual: el primer mensaje externo se redacta desde cero bajo máxima presión.

4. La notificación regulatoria está operativamente preparada

- Obligaciones aplicables de NIS2, DORA, RGPD o normas sectoriales documentadas
- Contactos y canales actualizados
- Plantillas para comunicaciones iniciales, intermedias y finales
- Vías de aprobación acordadas y probadas
- Jurídico, cumplimiento, comunicación y dirección conocen su función

Fallo habitual: la detección es rápida, pero la notificación llega tarde porque nadie controla la aprobación.

5. Las relaciones externas están preparadas

- Soporte externo de respuesta o análisis forense confirmado
- Asesoría jurídica con experiencia en incidentes identificada
- Proceso y contactos del seguro cibernético conocidos
- Apoyo de relaciones públicas o comunicación de crisis identificado
- Vías de escalado de proveedores y cloud documentadas

Fallo habitual: se contacta por primera vez con terceros críticos durante el incidente.

6. El modelo refleja la realidad operativa

- Plan revisado en los últimos 12 meses
- Sistemas, proveedores y equipos actuales reflejados
- Servicios prioritarios claramente definidos
- Supuestos clave probados al menos una vez
- Escenarios de ransomware, disponibilidad y presión de notificación cubiertos

Fallo habitual: el plan describe la organización de hace dos reorganizaciones.

Referencia de notificación regulatoria

Marco	Plazo inicial	Destinatario	Desencadenante
NIS2 (UE)	24 horas — alerta temprana	CSIRT nacional / autoridad competente	Incidente significativo
NIS2 (UE)	72 horas — notificación	CSIRT nacional / autoridad competente	Incidente significativo
Artículo 33 RGPD	72 horas	Autoridad de control	Brecha de datos con riesgo para personas
DORA — sector financiero UE	Dentro de las 4 horas siguientes a la clasificación como grave y, como máximo, 24 horas después de la detección — inicial	Autoridad competente	Incidente TIC grave
DORA — sector financiero UE	72 horas — intermedia	Autoridad competente	Incidente TIC grave
UK GDPR	72 horas	ICO	Brecha de datos con riesgo para personas
Sectorial	Variable	Regulador sectorial	Evento significativo definido por el sector

Acción: Confirme qué obligaciones son aplicables y documente el contacto, canal y proceso de aprobación de cada una.

Clasificación de gravedad

Nivel	Descripción	Ejemplos	Respuesta
Nivel 1 — Evento	Actividad sospechosa sin impacto confirmado	Inicio de sesión inusual, intentos fallidos, tráfico anómalo	Investigación SOC; sin escalado
Nivel 2 — Incidente	Brecha de control confirmada, impacto limitado y contenido	Malware aislado, credencial comprometida sin acceso a datos	Activar equipo de incidentes y notificar a dirección
Nivel 3 — Significativo	Impacto material en sistemas, servicios o datos	Ransomware, exfiltración confirmada, caída prolongada	Activar mando de crisis y evaluación regulatoria
Nivel 4 — Crisis	Servicios críticos afectados e impacto regulatorio, reputacional o comercial grave	Ransomware generalizado, brecha grave, caída multisistema	Mando completo, notificación y liderazgo ejecutivo activo

Los umbrales de notificación suelen corresponder a los niveles 3 o 4. Confírmelos con jurídico y cumplimiento.

Guía priorizada de simulación

Prioridad	Escenario	Qué comprueba	Por qué importa
Alta	Ransomware con copias cifradas	Recuperación sin disponibilidad de TI	Amenaza habitual que expone supuestos falsos
Alta	Exfiltración bajo presión regulatoria	Cadena de aprobación y plantillas	Exposición regulatoria y reputacional directa
Alta	Caída de proveedor cloud o tercero	Operación degradada de servicios críticos	Dependencia creciente
Media	Amenaza interna y abuso de privilegios	Coordinación entre registros, RR. HH., jurídico y seguridad	Difícil de detectar y políticamente sensible
Media	Fallo simultáneo cibernético y de suministro	Gestión de múltiples crisis	Prueba límites de resiliencia
Media	Fallo de comunicación ejecutiva durante incidente público	Gobernanza de comunicaciones bajo presión pública	Riesgo reputacional elevado
Baja	Demanda de pago de ransomware	Marco de decisión del consejo	Menos frecuente, pero de gran presión
Baja	Auditoría regulatoria durante incidente	Gestión de demandas paralelas	Poco común, pero intensiva en gobernanza
Baja	Phishing al equipo financiero	Respuesta conjunta de finanzas y seguridad	Coordinación negocio-ciberseguridad
Baja	Fallo de seguridad física en emplazamiento sensible	Integración de respuesta física y cibernética	Relevante para instalaciones o prototipos sensibles

Priorice según su modelo de amenazas: un fabricante debería probar la seguridad física; un proveedor SaaS debería priorizar los escenarios de caída del cloud.

Cinco preguntas para la primera hora

1. ¿Qué ha ocurrido? ¿Qué está confirmado y qué sigue siendo un supuesto?
2. ¿Está contenido? ¿La amenaza sigue activa o propagándose?
3. ¿Quién debe saberlo? ¿Qué partes internas y externas deben ser informadas ahora?
4. ¿Cuál es el servicio prioritario? ¿Qué servicio crítico debe protegerse primero?
5. ¿Qué plazos están corriendo? ¿Qué fechas regulatorias, contractuales o comerciales están activas?

Una acción para esta semana

Pruebe la cadena de aprobación de notificaciones. Pregunte quién aprobaría una notificación inicial si el incidente ocurriera un viernes a las 16:00, si esa persona estaría disponible, si existe suplente, si la plantilla está preparada y dónde se encuentra si la red corporativa no funciona.

Siguiente paso

GRCForce puede realizar una Revisión de Preparación de Respuesta a Incidentes que cubra:

- Estructura de mando y derechos de decisión
- Preparación de notificaciones regulatorias
- Modelo y plantillas de comunicación
- Diseño y facilitación de simulaciones
- Gobernanza posterior al ejercicio y planificación de acciones

Comience en https://grcforce.com/es/#contact.