Where Cyber Meets Intelligence

🚨 PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

Plantilla práctica para empresas | Fortinix

DATOS DE LA EMPRESA

- **Nombre:** _____
- **CIF:** _____
- **Dirección:** _____
- **Teléfono principal:** _____
- **Email contacto:** _____
- **Sector:** _____
- **Nº empleados:** _____

CONTROL DE VERSIÓN

- **Versión:** 1.0
- **Fecha creación:** _____
- **Última revisión:** _____
- **Próxima revisión:** _____
- **Aprobado por:** _____

📞 1. CONTACTOS DE EMERGENCIA

🚨 EQUIPO DE RESPUESTA INTERNO

Comandante de Incidentes

- **Nombre:** _____
- **Cargo:** _____
- **Móvil 24/7:** _____
- **Email:** _____
- **Suplente:** _____

Where Cyber Meets Intelligence

Responsable Técnico

- **Nombre:** _____
- **Cargo:** _____
- **Móvil 24/7:** _____
- **Email:** _____
- **Suplente:** _____

Responsable Comunicación

- **Nombre:** _____
- **Cargo:** _____
- **Móvil 24/7:** _____
- **Email:** _____
- **Suplente:** _____

Contacto Legal

- **Nombre:** _____
- **Empresa:** _____
- **Móvil 24/7:** _____
- **Email:** _____

🇪🇸 AUTORIDADES Y SERVICIOS OFICIALES

Entidad	Teléfono	Email	Cuándo contactar
INCIBE-CERT	017	cert@incibe.es	SIEMPRE - Primer contacto
Policía Nacional - Delitos Telemáticos	091		Daños económicos, chantaje
Guardia Civil - Delitos Telemáticos	062		Daños económicos, chantaje
AEPD	901 100 099	canal24h@aepd.es	Datos personales comprometidos

Where Cyber Meets Intelligence

🏢 PROVEEDORES CRÍTICOS

Empresa de Ciberseguridad

- **Empresa:** Fortinix
- **Contacto:** _____
- **Teléfono emergencia:** _____
- **Email:** _____

Proveedor Internet/Telecomunicaciones

- **Empresa:** _____
- **Contacto:** _____
- **Teléfono soporte:** _____

Proveedor Cloud (Microsoft 365, Google, AWS, etc.)

- **Empresa:** _____
- **Contacto:** _____
- **Teléfono soporte:** _____

Empresa de Backup

- **Empresa:** _____
- **Contacto:** _____
- **Teléfono soporte:** _____

⏰ 2. MATRIZ DE ESCALADO - NIVELES DE GRAVEDAD

🟢 NIVEL 1 - BAJO

Criterios:

- [ ] Impacto limitado a 1-2 usuarios
- [ ] Sin afectación a sistemas críticos
- [ ] Sin datos sensibles comprometidos
- [ ] Operaciones normales continúan

Where Cyber Meets Intelligence

Acciones:

- [ ] Responsable técnico maneja internamente
- [ ] Documentar incidente
- [ ] Monitorizar evolución

🟡 **NIVEL 2 - MEDIO**

Criterios:

- [ ] Impacto a departamento completo
- [ ] Sistemas importantes afectados
- [ ] Posible compromiso datos internos
- [ ] Operaciones ralentizadas

Acciones:

- [ ] Activar equipo de respuesta básico
- [ ] Comandante de incidentes informado
- [ ] Comunicación interna

🟠 **NIVEL 3 - ALTO**

Criterios:

- [ ] Impacto a múltiples departamentos
- [ ] Sistemas críticos comprometidos
- [ ] Datos de clientes posiblemente afectados
- [ ] Operaciones significativamente afectadas

Where Cyber Meets Intelligence

Acciones:

- [ ] **ACTIVAR PLAN COMPLETO**
- [ ] Contactar INCIBE-CERT
- [ ] Preparar comunicación externa
- [ ] Evaluar notificación RGPD

🔴 NIVEL 4 - CRÍTICO

Criterios:

- [ ] Paralización total o parcial operaciones
- [ ] Sistemas críticos completamente comprometidos
- [ ] Datos sensibles definitivamente comprometidos
- [ ] Amenaza para continuidad del negocio

Acciones:

- [ ] **ACTIVACIÓN INMEDIATA PROTOCOLO CRISIS**
- [ ] Contactar todas las autoridades
- [ ] Comunicación inmediata stakeholders
- [ ] Activar plan de continuidad de negocio

✅ 3. CHECKLISTS POR FASES

🚨 FASE 1: DETECCIÓN Y ANÁLISIS (0-15 minutos)

Quien detecta el incidente:

- [ ] **NO TOCAR NADA** - Preservar evidencias
- [ ] Fotografiar pantalla con móvil
- [ ] Anotar hora exacta: _____
- [ ] Documentar qué se observó: _____
- [ ] **LLAMAR inmediatamente** al Comandante de Incidentes
- [ ] Enviar mensaje al grupo WhatsApp de crisis

Where Cyber Meets Intelligence

Comandante de Incidentes:

- [ ] Confirmar activación del plan de crisis
- [ ] Evaluar nivel de gravedad (1-4): _____
- [ ] Convocar equipo de respuesta
- [ ] Activar sala de crisis (física/virtual)
- [ ] Contactar empresa ciberseguridad si nivel ≥ 3
- [ ] Iniciar log de decisiones y acciones

Responsable Técnico:

- [ ] Evaluar alcance inicial
- [ ] Identificar sistemas afectados: _____
- [ ] Verificar estado de backups
- [ ] Preservar evidencias forenses
- [ ] Evaluar si es incidente real o falsa alarma

⏰ Tiempo máximo para esta fase: 15 minutos

🛡️ FASE 2: CONTENCIÓN (15-60 minutos)

Contención inmediata:

- [ ] Aislar sistemas infectados de la red
- [ ] Documentar sistemas aislados: _____
- [ ] Cambiar contraseñas administrativas críticas
- [ ] Bloquear accesos sospechosos
- [ ] Revisar logs de acceso recientes
- [ ] Preservar evidencias antes de cualquier acción

Comunicación interna:

- [ ] Informar a todos los empleados del incidente
- [ ] Enviar email con instrucciones claras
- [ ] Establecer canal de comunicación temporal
- [ ] Informar a dirección/consejo de administración

Where Cyber Meets Intelligence

Evaluación continua:

- [ ] Monitorizar si la contención es efectiva
- [ ] Verificar que el incidente no se extiende
- [ ] Documentar todas las acciones realizadas
- [ ] Preparar información para autoridades

⏰ Tiempo máximo para esta fase: 45 minutos adicionales

🔧 FASE 3: ERRADICACIÓN (1-24 horas)

Análisis de causa raíz:

- [ ] Identificar cómo ocurrió el incidente
- [ ] Causa raíz identificada: _____
- [ ] Evaluar vulnerabilidades explotadas
- [ ] Determinar punto de entrada: _____

Eliminación de amenazas:

- [ ] Eliminar malware/código malicioso
- [ ] Cerrar vulnerabilidades identificadas
- [ ] Aplicar parches de seguridad pendientes
- [ ] Fortalecer medidas de seguridad

Preparación para recuperación:

- [ ] Verificar integridad de backups
- [ ] Planificar secuencia de restauración
- [ ] Preparar sistemas limpios para recuperación
- [ ] Coordinar con proveedores si es necesario

⏰ Tiempo objetivo: Menos de 24 horas

Where Cyber Meets Intelligence

🚀 FASE 4: RECUPERACIÓN (1-7 días)

Restauración de sistemas:

- [ ] Restaurar sistemas desde backups limpios
- [ ] Verificar integridad de datos restaurados
- [ ] Probar funcionalidad de sistemas críticos
- [ ] Restablecer conectividad de red

Monitorización reforzada:

- [ ] Implementar monitorización adicional
- [ ] Verificar no hay actividad residual maliciosa
- [ ] Confirmar normalidad de operaciones
- [ ] Documentar lecciones técnicas aprendidas

Comunicación de recuperación:

- [ ] Informar empleados de normalización
- [ ] Comunicar a clientes (si procede)
- [ ] Actualizar autoridades sobre resolución
- [ ] Preparar informe final

⏰ Tiempo objetivo: Menos de 7 días

📚 FASE 5: LECCIONES APRENDIDAS (Posterior)

Análisis post-incidente:

- [ ] Reunión de equipo completo programada para: _____
- [ ] Revisar efectividad del plan
- [ ] Identificar puntos de mejora
- [ ] Evaluar tiempos de respuesta

Where Cyber Meets Intelligence

Actualizaciones:

- [ ] Actualizar plan de respuesta
- [ ] Mejorar medidas de seguridad
- [ ] Formar equipo en mejoras identificadas
- [ ] Programar próximo simulacro para: _____

📧 4. TEMPLATES DE COMUNICACIÓN

📨 EMAIL INTERNO - INCIDENTE EN CURSO

Asunto: [URGENTE] Incidente de Seguridad en Curso - Instrucciones Inmediatas

Estimado equipo,

Hemos detectado un incidente de ciberseguridad que está siendo gestionado por nuestro equipo de respuesta.

INSTRUCCIONES INMEDIATAS:

- NO utilizar sistemas informáticos hasta nuevo aviso
- NO abrir emails sospechosos
- Reportar cualquier actividad inusual a [CONTACTO]
- Mantener la calma y seguir instrucciones

ESTADO ACTUAL:

- Incidente detectado a las: [HORA]
- Sistemas afectados: [SISTEMAS]
- Equipo de respuesta activado

Os mantendremos informados cada [FRECUENCIA] horas.

Contacto para dudas urgentes: [TELÉFONO]

[NOMBRE COMANDANTE] Comandante de Incidentes

Where Cyber Meets Intelligence

📨 EMAIL CLIENTES - NOTIFICACIÓN TRANSPARENTE

Asunto: Información Importante sobre Incidente de Seguridad

Estimado cliente,

Le informamos de manera transparente que hemos experimentado un incidente de ciberseguridad que estamos gestionando activamente.

QUÉ HA PASADO: [DESCRIPCIÓN BREVE DEL INCIDENTE]

QUÉ ESTAMOS HACIENDO:

- Equipo experto trabajando 24/7 en la resolución
- Cooperación con autoridades competentes
- Implementación de medidas adicionales de seguridad

IMPACTO EN SUS DATOS: [INFORMACIÓN ESPECÍFICA SOBRE DATOS DEL CLIENTE]

QUÉ DEBE HACER: [INSTRUCCIONES ESPECÍFICAS SI ES NECESARIO]

Estimamos tener la situación normalizada en [TIEMPO ESTIMADO].

Para cualquier consulta: [CONTACTO ESPECÍFICO]

Gracias por su comprensión.

[NOMBRE] [CARGO]

📰 COMUNICADO DE PRENSA - SI ES NECESARIO

PARA DIFUSIÓN INMEDIATA

[NOMBRE EMPRESA] INFORMA SOBRE INCIDENTE DE CIBERSEGURIDAD

[CIUDAD], [FECHA] - [NOMBRE EMPRESA] informa que ha detectado y está respondiendo a un incidente de ciberseguridad.

Where Cyber Meets Intelligence

Hechos principales:

- Incidente detectado el [FECHA] a las [HORA]
- Protocolo de respuesta activado inmediatamente
- Autoridades competentes notificadas
- Medidas de contención implementadas

Respuesta de la empresa: "La seguridad de nuestros clientes y datos es nuestra máxima prioridad", declaró [NOMBRE], [CARGO]. "Hemos activado nuestro protocolo de respuesta y estamos trabajando con expertos para resolver esta situación."

Impacto y medidas: [INFORMACIÓN SOBRE IMPACTO Y MEDIDAS TOMADAS]

La empresa mantendrá informados a todos los stakeholders sobre la evolución de la situación.

Contacto de prensa: [NOMBRE] [TELÉFONO] [EMAIL]

📋 5. FORMULARIOS DE DOCUMENTACIÓN

🕵️ REGISTRO INICIAL DE INCIDENTE

ID del Incidente: INC-[AAAAMMDD]-[###]

DETECCIÓN:

- **Fecha:** _____ **Hora:** _____
- **Detectado por:** _____
- **Método de detección:** _____
- **Descripción inicial:** _____
- **Screenshots/Evidencias:** _____

CLASIFICACIÓN INICIAL:

- **Tipo de incidente:** _____
- **Nivel de gravedad:** _____
- **Sistemas afectados:** _____
- **Datos comprometidos:** _____

Where Cyber Meets Intelligence

PRIMERA RESPUESTA:

- **Comandante asignado:** _____
- **Equipo activado:** _____
- **Hora activación plan:** _____

⏰ LOG DE ACCIONES Y DECISIONES

Hora	Acción/Decisión	Responsable	Resultado	Observaciones

📊 INFORME FINAL DE INCIDENTE

RESUMEN EJECUTIVO:

- **Duración total:** _____
- **Sistemas afectados:** _____
- **Impacto en operaciones:** _____
- **Datos comprometidos:** _____
- **Coste estimado:** _____

CRONOLOGÍA DE EVENTOS:

1. **[Hora]** - [Descripción]
2. **[Hora]** - [Descripción]
3. **[Hora]** - [Descripción]

CAUSA RAÍZ:

LECCIONES APRENDIDAS:

1. _____
2. _____
3. _____

Where Cyber Meets Intelligence

MEJORAS IMPLEMENTADAS:

1. _____
2. _____
3. _____

PRÓXIMOS PASOS:

- [ ] Actualizar plan de respuesta
- [ ] Formar equipo en mejoras
- [ ] Implementar medidas adicionales
- [ ] Programar próximo simulacro

🎯 6. MATRIZ DE ESCALADO DETALLADA

📞 CUÁNDO CONTACTAR CADA AUTORIDAD

Situación	INCIBE-CERT	Policía/GC	AEPD	Otros
Cualquier incidente	✅ SIEMPRE	❌	❌	
Datos personales comprometidos	✅	❌	✅	
Chantaje/Rescate	✅	✅	❌	
Daño económico >€3000	✅	✅	❌	
Infraestructura crítica	✅	✅	✅	CCN-CERT
Servicios esenciales	✅	✅	✅	Sector regulador

⏰ TIEMPOS DE NOTIFICACIÓN OBLIGATORIOS

Autoridad	Plazo máximo	Información requerida
INCIBE-CERT	Inmediato	Descripción inicial, contacto
AEPD (si RGPD)	72 horas	Naturaleza, categorías datos, medidas
Afectados (si RGPD)	Sin demora indebida	Lenguaje claro, medidas adoptadas

---

🛠️ 7. KIT DE HERRAMIENTAS DE EMERGENCIA

Where Cyber Meets Intelligence

💻 HERRAMIENTAS TÉCNICAS

- [ ] **Acceso remoto seguro:** _____
- [ ] **Software forense:** _____
- [ ] **Herramientas de análisis de malware:** _____
- [ ] **Backup de configuraciones críticas:** _____
- [ ] **Dispositivos offline para análisis:** _____

📱 HERRAMIENTAS DE COMUNICACIÓN

- [ ] **Grupo WhatsApp crisis:** _____
- [ ] **Teléfonos satélite/backup:** _____
- [ ] **Acceso email alternativo:** _____
- [ ] **Plataforma reuniones backup:** _____

📄 DOCUMENTACIÓN DE RESPALDO

- [ ] **Copias impresas contactos críticos**
- [ ] **Procedimientos en papel**
- [ ] **Contratos con proveedores**
- [ ] **Pólizas de seguros ciberseguridad**

🎓 8. PROGRAMA DE FORMACIÓN Y SIMULACROS

📚 FORMACIÓN OBLIGATORIA ANUAL

Todo el personal:

- [ ] **Reconocimiento de phishing** (2 horas)
- [ ] **Procedimientos básicos ante incidentes** (1 hora)
- [ ] **Contactos de emergencia** (30 min)

Equipo de respuesta:

- [ ] **Roles y responsabilidades** (4 horas)
- [ ] **Herramientas técnicas** (6 horas)
- [ ] **Comunicación de crisis** (3 horas)
- [ ] **Aspectos legales** (2 horas)

Where Cyber Meets Intelligence

🎯 PROGRAMA DE SIMULACROS

Simulacros trimestrales:

- **Q1:** Phishing con compromiso de email
- **Q2:** Ransomware en sistema crítico
- **Q3:** Fuga de datos de clientes
- **Q4:** Ataque a infraestructura

Métricas de evaluación:

- Tiempo hasta detección: _____ minutos
- Tiempo hasta contención: _____ minutos
- Efectividad comunicación: _____ / 10
- Seguimiento procedimientos: _____ %

✅ 9. CHECKLIST DE REVISIÓN MENSUAL

🔍 VERIFICACIONES OBLIGATORIAS

Contactos y comunicación:

- [ ] Verificar todos los teléfonos de emergencia
- [ ] Probar grupo WhatsApp de crisis
- [ ] Actualizar contactos que hayan cambiado
- [ ] Verificar emails alternativos funcionan

Herramientas y accesos:

- [ ] Probar acceso remoto de emergencia
- [ ] Verificar backups son accesibles
- [ ] Comprobar herramientas forenses
- [ ] Revisar contratos proveedores vigentes

Documentación:

- [ ] Revisar y actualizar procedimientos
- [ ] Verificar compliance con nuevas normativas
- [ ] Actualizar matriz de escalado
- [ ] Revisar lecciones de incidentes recientes

Where Cyber Meets Intelligence

Preparación del equipo:

- [ ] Confirmar disponibilidad miembros equipo
- [ ] Planificar formación adicional si necesaria
- [ ] Evaluar necesidad nuevos miembros equipo
- [ ] Programar próximo simulacro

Revisión realizada por: _____ **Fecha:** _____ **Próxima revisión:** _____

📞 10. GUÍA RÁPIDA DE BOLSILLO

Recortar y llevar siempre encima

🚨 INCIDENTE DETECTADO

1. NO TOCAR NADA 2. FOTOGRAFIAR CON MÓVIL
3. LLAMAR INMEDIATAMENTE:

Comandante: _____ **Suplente:** _____ **Fortinix:** _____ _____

4. GRUPO WHATSAPP: _____ **5. INCIBE-CERT:** 017

Si no localizas a nadie: Policía Nacional: 091 **Guardia Civil:** 062

¡MANTÉN LA CALMA!

Where Cyber Meets Intelligence

📝 PERSONALIZACIÓN DE LA PLANTILLA

✏️ INSTRUCCIONES PARA COMPLETAR:

1. **Rellenar todos los campos** marcados con líneas
2. **Adaptar procedimientos** a tu sector específico
3. **Validar contactos** con proveedores y autoridades
4. **Revisar aspectos legales** con tu asesor
5. **Probar con simulacro** antes de dar por válido
6. **Distribuir a equipo** y entrenar en su uso
7. **Revisar mensualmente** y actualizar

🔄 CONTROL DE VERSIONES:

- Mantener historial de cambios
- Fecha cada actualización
- Comunicar cambios al equipo
- Archivar versiones anteriores

Plantilla desarrollada por Fortinix
Ciberseguridad sin tecnicismos
www.fortinix.eu | info@fortinix.eu

Esta plantilla debe adaptarse a las necesidades específicas de cada organización y validarse con asesoramiento legal especializado.