README: KIT INTEGRAL DE ENCUESTA DE CIBERSEGURIDAD

Guía de Uso, Implementación y Distribución

Versión: 2.0 | **Fecha:** Enero 2026 | **Última Actualización:** Enero 2026

1. DESCRIPCIÓN GENERAL DEL KIT

Este Kit Integral proporciona un **conjunto completo de herramientas, metodologías y plantillas** para evaluar, medir y mejorar la madurez de ciberseguridad de organizaciones españolas de todos los tamaños.

Componentes del Kit

```
KIT INTEGRAL DE CIBERSEGURIDAD 2026
│
├─ 📋 01_Encuesta_Integral.md
│  └─ 60+ preguntas estructuradas en 8 bloques
│     (Gobierno, Identificar, Proteger, Detectar, Responder, Recuperar,
│      Vulnerabilidades, SIEM, Capacitación)
│
├─ 📊 02_Guia_Metodologica.md
│  └─ Cálculo detallado de IGM, KRIs, KPIs, análisis ROI
│     Niveles madurez ACET, interpretación benchmarking
│
├─ 📖 03_Narrativa_Explicativa.md
│  └─ Guía literaria, irónica y constructiva
│     Explicación amigable de conceptos ciberseguridad
│
├─ 📌 04_Mapeo_Normativo.md
│  └─ Matriz de trazabilidad: preguntas → NIST CSF, ENS, NIS2, GDPR, ISO 27001
│     Demostración de cumplimiento regulatorio por cada pregunta
│
├─ 💾 05_Plantilla_Excel_IGM.md
│  └─ Especificaciones técnicas para hoja de cálculo
│     Fórmulas automatizadas, cálculo IGM, ROI, benchmarking
│
├─ 🎬 06_Plantilla_PowerPoint.md
│  └─ 15+ diapositivas de reporte ejecutivo
│     Visualizaciones, KPIs, recomendaciones
│
└─ 📚 07_README.md (Este archivo)
   └─ Guía implementación, uso, distribución

ARCHIVOS RELACIONADOS COMPLEMENTARIOS:
│
├─ INFORME_ACET_España_2024_2025.md
│  └─ Análisis territorial, benchmarking, tendencias 2024-2025
│
└─ Datos de Referencia Externa (INCIBE, ISMS Forum, ITU, ENISA)
   └─ Benchmarks nacionales y sectoriales
```

2. FLUJO DE IMPLEMENTACIÓN (12 PASOS)

Fase 1: Preparación (Semana 1)

Paso 1: Definir Alcance y Respondentes
- ¿Quién? Líderes técnicos, CISO, IT Manager, SOC Lead, Compliance Officer, RH
- ¿Cuántos? Mínimo 5-10 respondentes (para validación cruzada)
- ¿Dónde? Todas las ubicaciones / sedes relevantes
- **Output:** Lista de respondentes, confirmación participación

Paso 2: Personalizar Encuesta
- Abrir `01_Encuesta_Integral.md`
- Adaptar preguntas si es necesario (ej. añadir preguntas OT si industrial)
- Crear versión desplegable en Google Forms o MS Forms
- **Output:** Encuesta online lista para distribución

Paso 3: Diseñar Cronograma
- Distribución encuesta: [Fecha inicio]
- Plazo respuestas: 2 semanas
- Seguimiento: Recordatorios semana 1 y 2
- Análisis: Semana 3-4
- **Output:** Calendario confirmado

Fase 2: Recolección de Datos (Semanas 2-3)

Paso 4: Distribuir Encuesta
- Enviar link a respondentes con instrucciones
- Establecer helpdesk (CISO/IT manager) para dudas
- Garantizar confidencialidad y anonimato (si aplica)
- **Output:** ≥80% de respuestas completadas

Paso 5: Validación de Respuestas
- Revisar respuestas por completitud
- Identificar "DK" (Desconoce) excesivos
- Seguimiento de respondentes con baja participación
- **Output:** Base de datos limpia y completa

Fase 3: Análisis (Semanas 4-5)

Paso 6: Cálculo de IGM
- Importar respuestas a `05_Plantilla_Excel_IGM.md`
- Ejecutar fórmulas automáticas
- Generar puntuaciones por dominio NIST
- Calcular IGM global, KRIs, KPIs
- **Output:** Dashboard Excel con resultados

Paso 7: Benchmarking y Gap Analysis
- Usar `02_Guia_Metodologica.md` para interpretación
- Comparar vs. benchmarks nacional/sectorial
- Identificar top 3 brechas críticas
- Asignar prioridades (matriz impacto × esfuerzo)
- **Output:** Matriz de priorización y roadmap preliminar

Paso 8: Validación Cruzada
- Revisar resultados vs. auditorías previas / datos técnicos
- Reconciliar discrepancias (ej. "Sí" a SIEM pero logs incompletos)
- Ajustar puntuaciones si hay evidencia conflictiva
- **Output:** Hallazgos validados, confianza >95%

Fase 4: Generación de Reportes (Semana 6)

Paso 9: Elaborar Reporte Ejecutivo
- Usar `06_Plantilla_PowerPoint.md`
- Personalizar con datos de organización
- Incluir visualizaciones, KPIs, recomendaciones
- Crear versiones ejecutiva (10 slides) y técnica (20 slides)
- **Output:** Presentación PowerPoint profesional

Paso 10: Crear Narrativa
- Usar `03_Narrativa_Explicativa.md` como referencia
- Escribir resumen ejecutivo (1-2 páginas)
- Explicar hallazgos en lenguaje ejecutivo/no técnico
- Destacar oportunidades (no solo riesgos)
- **Output:** Documento narrativo de contexto

Paso 11: Demostración de Cumplimiento
- Usar `04_Mapeo_Normativo.md`
- Documentar alineación con NIST CSF, ENS, NIS2, GDPR
- Preparar matriz de trazabilidad para reguladores
- Evidenciar que encuesta valida conformidad
- **Output:** Mapeo para auditorías/reguladores

Fase 5: Comunicación y Acción (Semanas 7-8)

Paso 12: Presentación y Roadmap
- Presentar hallazgos a Junta/Ejecutivos
- Obtener aprobación presupuesto roadmap
- Designar propietarios por iniciativa
- Establecer métricas de éxito y seguimiento trimestral
- **Output:** Plan de acción aprobado, presupuesto asignado

3. GUÍA POR ARCHIVO

📋 01_Encuesta_Integral.md

Uso: Instrumento de recolección de datos

Cómo usar:
1. Abrir archivo en editor (Markdown viewer o Word)
2. Copiar contenido a herramienta survey (Google Forms, MS Forms, Qualtrics)
3. Configurar validaciones, lógica condicional si es necesario
4. Distribuir link a respondentes
5. Descargar respuestas en CSV/Excel

Tiempo de Finalización: 45-90 minutos por respondente

Validación:
- ✓ Respuestas obligatorias: NO (permite NA, DK)
- ✓ Cierre automático: SÍ (2 semanas después)
- ✓ Recordatorios: SÍ (días 3, 7, 10)

Adaptaciones Recomendadas:
- PyMEs: Simplificar a 40 preguntas (quitar preguntas OT/ICS avanzadas)
- Grandes Empresas: Añadir 10-15 preguntas especializadas (Cloud, Terceros, Cumplimiento Regulatorio)
- Sector Industrial (OT/ICS): Enfatizar dominio "Detectar" en infraestructura crítica

📊 02_Guia_Metodologica.md

Uso: Manual de cálculos, interpretación, análisis

Cómo usar:
1. Después de recolectar respuestas
2. Seguir paso a paso el proceso de normalización y ponderación
3. Aplicar fórmulas a datos reales
4. Validar cálculos manuales vs. automatizados (Excel)
5. Usar para entrenar a equipo analítico

Secciones Clave:
- 3. Esquema de Puntuación (mapeo respuestas → puntos)
- 4. Cálculo del IGM (fórmula ponderada)
- 5. Análisis Comparativo (benchmarking)
- 6. Gap Analysis (brechas)
- 7. Cálculo ROI (justificación inversiones)

Referencia Rápida:
- IGM 0-40%: Crisis, intervención urgente
- IGM 40-60%: Básico, mejoras necesarias

- IGM 60-80%: Profesional, optimización continua
- IGM 80-100%: Excelencia, innovación

📖 03_Narrativa_Explicativa.md

Uso: Comunicación ejecutiva, contexto interpretativo

Cómo usar:
1. Leer antes de presentar hallazgos (entender la "historia")
2. Adaptar analogías para audiencia (ej. "castillo medieval" → "ciudad digital")
3. Usar tonalidad irónica para mantener engagement
4. Citar en resumen ejecutivo para añadir profundidad
5. Compartir con equipo para alineación de mensaje

Estructura:
- Acto I: Contextualización del problema
- Acto II-VII: Explicación de cada dominio NIST con analogías
- Epílogo: Verdad incómoda + camino adelante

Tono:
- Irónico pero constructivo
- Ameno pero riguroso
- Literario pero técnicamente preciso

📌 04_Mapeo_Normativo.md

Uso: Trazabilidad regulatoria, cumplimiento normativo

Cómo usar:
1. Para cada pregunta, consultar tabla asociada
2. Identificar artículos NIST, ENS, NIS2, GDPR, ISO aplicables
3. Recopilador evidencia de cumplimiento
4. Documentar para auditorías internas/externas
5. Construir matriz de cumplimiento para reguladores

Normas Cubiertas:
- NIST CSF 2.0 (Global)
- ENS (España Admin. Pública)
- NIS2 (EU, sectores críticos)
- GDPR (EU, datos)
- ISO 27001 (Certificación internacional)

Caso de Uso Típico:
- Auditor NIS2 solicita: "¿Cómo cumple con Art. 19 (Evaluación Riesgos)?"
- Respuesta: Consultar Mapeo → P1.2.1 Evaluaciones Riesgos Formales → mostrar evidencia (informe evaluación riesgos 2025, documento), ✓ CUMPLE

💾 05_Plantilla_Excel_IGM.md

Uso: Cálculos automatizados, generación de dashboards

Cómo usar:

1. Crear libro Excel nuevo (o Google Sheet)
2. Crear 5 hojas: INPUT, SCORING, BENCHMARKING, ROI_ANALYSIS, DASHBOARD
3. Copiar estructuras de columnas desde plantilla
4. Implementar fórmulas (AVERAGEIF, SUMPRODUCT, SWITCH)
5. Importar respuestas encuesta en hoja INPUT
6. Verificar cálculos automáticos en SCORING
7. Generar gráficos (Radar, Gauge, Barras)

Hojas y Propósito:

Hoja	Propósito	Salida
INPUT	Ingesta respuestas encuesta	Base datos limpia
SCORING	Cálculos IGM, dominios, KRIs, KPIs	Puntuaciones por dominio
BENCHMARKING	Comparativa vs. sector/nacional	Radar comparativo, gaps
ROI_ANALYSIS	Calcular ROI controles inversión	Matriz priorización, payback
DASHBOARD	Resumen ejecutivo visual	Gauge IGM, KPIs, alertas

Validación:

- Sumar todos los puntos manuales vs. Excel (deben coincidir)
- Verificar IGM = SUMPRODUCT de dominios ponderados
- Confirmar nivel asignación correcta según rango %

Exportación:

- PDF: File → Print → Print to PDF
- CSV: Guardar como CSV para análisis adicional
- Imágenes: Copiar gráficos a PowerPoint

🎬 06_Plantilla_PowerPoint.md

Uso: Presentación de hallazgos a stakeholders

Cómo usar:

1. Crear presentación PowerPoint/Google Slides nueva
2. Copiar estructura de 15 diapositivas desde plantilla
3. Personalizar con datos del análisis Excel
4. Insertar gráficos (Radar, Gauge, Barras) desde Excel
5. Redactar narrativa en notas de orador
6. Practicar presentación (20-30 minutos)
7. Exportar a PDF para distribución

Diapositivas Clave:
1. Portada: Título, organización, IGM
3. Resumen Ejecutivo: IGM, benchmark, fortalezas/debilidades
4. Metodología: NIST CSF, marcos normativos
6. Análisis Dominio: Radar comparativo
8. KRIs: Alertas críticas en rojo/amarillo/verde
12. Roadmap: Gantt 12 meses con inversiones
14. Análisis ROI: Tabla controles con ROI %
15. Recomendaciones: Action items por trimestre

Timing Recomendado:
- Ejecutivos (C-suite): 10 slides, 20 minutos
- IT Leadership: 16 slides, 30 minutos
- Auditorios/Reguladores: 20+ slides, 45+ minutos

📚 07_README.md
Uso: Este archivo - guía de implementación general

Secciones:
- Descripción general kit
- Flujo implementación 12 pasos
- Guía por archivo
- Mejores prácticas
- Solución de problemas
- FAQ

4. MEJORES PRÁCTICAS

Recolección de Datos
✓ **Hacer:**
- Obtener respuestas de múltiples departamentos (triangulación)
- Permitir tiempo suficiente (2+ semanas)
- Proporcionar contacto para dudas (CISO/IT Manager)
- Recordar a no respondentes amablemente (3 veces máximo)
- Garantizar confidencialidad de respondientes individuales

✗ NO hacer:
- Confiar en una sola respuesta (sesgo individual)
- Apresurar (menos de 1 semana)
- Penalizar respondentes por participación
- Publicar respuestas individuales (privacidad)
- Cambiar preguntas a mitad del proceso (invalida comparabilidad)

Análisis

✓ **Hacer:**

- Validar cruzada respuestas vs. auditorías técnicas previas
- Usar múltiples fuentes de datos (no solo autoevaluación)
- Documentar supuestos y limitaciones
- Incluir contexto histórico (comparación años previos)
- Buscar razones subyacentes, no solo síntomas

✗ NO hacer:

- Aceptar respuestas "Sí" sin evidencia
- Ignorar "NA" (puede indicar falta de visibilidad)
- Suponer linealidad entre IGM y riesgo real (no es 1:1)
- Comparar directamente con competidores (contextos diferentes)
- Hacer recomendaciones sin analizar impacto/esfuerzo

Comunicación

✓ **Hacer:**

- Presentar hallazgos como "oportunidades" (no fracasos)
- Reconocer fortalezas junto a brechas
- Proporcionar roadmap práctico con timelines claros
- Obtener buy-in de ejecutivos antes de presentar
- Celebrar victorias pequeñas (incrementos IGM trimestral)

✗ NO hacer:

- Culpar individuos ("El CISO no hace...")
- Exagerar riesgos para justificar presupuesto
- Proponer 50 mejoras sin priorización (parálisis)
- Presentar hallazgos sin recomendaciones
- Generar reporte y archivarlo (usar para acción)

5. SOLUCIÓN DE PROBLEMAS

Problema: Baja Tasa de Respuesta (<50%)

Causas Comunes:

- Encuesta muy larga (>90 minutos)
- Respondentes no tienen autorización para participar
- Comunicación de propósito insuficiente
- Timing inadecuado (durante vacaciones, crisis operativa)

Soluciones:

1. Acortar encuesta a versión "lite" (40 preguntas vs 60)
2. Obtener sponsorship de CEO/Junta (enviar introducción ejecutiva)
3. Proporcionar contexto claro: "Por qué esto importa"

4. Extender plazo o cambiar fecha
5. Hacer seguimiento personalizado (llamadas, no emails)

Problema: Respuestas Inconsistentes ("SÍ" a SIEM pero "NO" a logs centralizados)

Causas Comunes:
- Respondentes de diferentes departamentos (IT dice "Sí", SOC dice "Parcial")
- Falta de alineación sobre definiciones
- Respondente no tiene visibilidad completa

Soluciones:
1. Crear grupo de validación (CISO + IT Manager + SOC Lead)
2. Revisar respuestas conflictivas en sesión con respondentes
3. Aclarar términos ("¿SIEM = centralización logs? ¿O incluye correlación?")
4. Tomar respuesta más conservadora cuando hay conflicto
5. Documentar discrepancia como "nota de auditoría"

Problema: IGM Parece Demasiado Alto/Bajo

Validación:
1. Revisar puntuaciones dominio por dominio
2. Verificar ponderación (GV 20%, ID 15%, PR 25%, etc.)
3. Comparar vs. benchmarks sector (¿está en rango esperado?)
4. Comprobar que "Sí" respuestas tienen evidencia
5. Entrevistar a respondentes de dominios elevados/bajos

Razones Comunes - IGM Muy Alto:
- Respondentes sobreestiman madurez
- Preguntas muy binarias (SÍ/NO) sin validación técnica

Razones Comunes - IGM Muy Bajo:
- Respondentes pesimistas sobre progreso
- Faltan contexto de mejoras recientes

Corrección:
- Ajustar puntuaciones downward si hay sesgo optimista
- Investigar aumentos rápidos (¿implementaciones recientes?)

Problema: Presupuesto Rechazado para Roadmap

Contexto:
- Ejecutivos dicen: "¿Por qué gastar €530K si IGM es 71%?"

Respuesta (usar Guía 02 - ROI):
1. Mostrar ROI esperado: €530K inversión → €825K beneficio → 55% ROI
2. Payback: 8 meses (recuperan en menos de 1 año)
3. Comparar vs. costo breach: 1 ataque serio = €2-5M (vs €530K preventivo)

4. Priorizar "quick wins" (capacitación €30K, ROI 200%)
5. Proponer fase (Q1-Q2 prioritarios, Q3-Q4 stretch)

6. PREGUNTAS FRECUENTES (FAQ)

¿Con qué frecuencia debo hacer esta encuesta?

Respuesta: Mínimo anual. Organizaciones maduras: semestral o trimestral.
- Año 1 (Línea base): Completa (60 preguntas)
- Años 2+: Encuesta completa anualmente + delta trimestral (10 preguntas clave)

¿Puedo hacer encuesta solo CISO sin otros respondentes?

Respuesta: NO. CISO tiene sesgo hacia riesgos (percibe más vulnerabilidades).
Necesitas triángulo: CISO (riesgo), IT Manager (implementación), Negocio (prioridades).

¿Cuál es el mínimo IGM para cumplir NIS2?

Respuesta: NIS2 requiere "nivel básico" = ~60-70% en dominios críticos.
- Gobierno + Identificar + Proteger: >70%
- Detectar + Responder + Recuperar: >60% mínimo
Recomendación: Target 75%+ para estar seguro.

¿Cómo aplico esto si soy PyME sin CISO dedicado?

Respuesta:
1. Encuesta "lite" de 40 preguntas (quitar temas OT/complejo)
2. Respondentes: Propietario TI + 2 empleados clave + Dueño negocio
3. Roadmap acortado: Primeros 6 meses, 3 iniciativas máximo
4. Considerar outsourcing (MSSP) para suplir capacidad
5. Presupuesto típico PyME: €50-100K año 1

¿Qué hacer si encuentro vulnerabilidad crítica en análisis?

Respuesta:
1. ESCALAR inmediatamente a CISO (no esperar fin análisis)
2. Crear ticket respuesta incidentes (si es breach actual)
3. Documentar en "Hallazgos Críticos" de reporte (separado del IGM)
4. No incluir en cálculo IGM (es issue de seguridad operativa, no madurez)
5. Seguimiento: Verificar remediación en 24-48h

¿Puedo automatizar completamente la encuesta (no preguntas)?

Respuesta: Parcialmente. Usar escaneos técnicos para validar:
- P2.1.1 (CMDB): Ejecutar descubrimiento de activos (Nessus, Qualys)
- P3.1.1 (MFA): Auditar AD/Okta
- P4.1.1 (SIEM): Verificar integración fuentes
- P7.1.1 (Escaneos Vuln): Leer resultados últimos escaneos

Pero NO automatizar: Política, Gobernanza, Cultura, Capacitación (necesita input humano).

7. ROADMAP DE MEJORA CONTINUA (Años 1-3)

AÑO 1: LÍNEA BASE Y QUICK WINS

- Q1: Encuesta basal (IGM ~71%)
- Q2-Q3: Implementar capacitación, MFA, backups
- Q4: Revisión anual (target IGM 75%)
- Inversión: ~€530K | ROI: ~55%

AÑO 2: MADURACIÓN ESTRUCTURAL

- Q1: Encuesta completa (target IGM 78%)
- Q2-Q3: SIEM, EDR, automatización respuesta incidentes
- Q4: Readiness NIS2 100%, revisión
- Inversión: ~€400K | ROI: ~45%

AÑO 3: OPTIMIZACIÓN Y SOSTENIBILIDAD

- Q1: Encuesta (target IGM 82%)
- Q2-Q3: Zero Trust, threat intelligence integrada, AI-driven detection
- Q4: Revisión estratégica, plan 2027
- Inversión: ~€300K | ROI: ~35% (disminuye porque base cost es menor)

Éxito Esperado

- Año 1: IGM 71% → 75% (+4 puntos)
- Año 2: IGM 75% → 80% (+5 puntos)
- Año 3: IGM 80% → 85% (+5 puntos)
- Target Final (2028): IGM 85%+ (Nivel Advanced) + NIS2 compliant

8. DISTRIBUCIÓN Y ACCESO

A Quién Compartir Cada Componente

Archivo	Junta	CEO	CISO	IT Mgr	Auditor	Empleados
01_Encuesta	-	-	√	√	-	√ (responder)
02_Metodología	-	-	√	√	√	-
03_Narrativa	√	√	√	√	-	-
04_Mapeo_Norm	√	-	√	-	√	-
05_Excel_IGM	-	-	√	√	-	-
06_PowerPoint	√	√	√	√	√ (v. ejecutiva)	√ (resumen)
07_README	-	-	√	√	-	-

Seguridad de Acceso

- Pública: README, Narrativa (educación general)
- Interno: Encuesta, Metodología, Excel, PowerPoint (solo equipo seguridad)
- Restringida: Mapeo Normativo (CISO + Compliance + Auditores)
- C-Level: PowerPoint ejecutiva, Narrativa, algunos KPIs clave

9. SOPORTE Y ACTUALIZACIONES

Versión Actual: 2.0 (Enero 2026)

Cambios vs. v1.0:

- Añadidas 15 preguntas sobre IA en ciberseguridad
- Integración NIS2 (nueva norma transposición 2026)
- Mejora scoring SIEM + KPIs
- Narrativa reescrita con tono más ameno

Próxima Versión: 2.1 (Abril 2026)

Previsto incluir:

- Preguntas Quantum-safe cryptography
- ENS 4.0 (revisión esperada)
- Integración COBIT 2023
- Templates para industrias específicas (Finanzas, Sanitaria, Energía)

Contacto para Actualizaciones

Para reportar bugs, sugerencias o adaptaciones sectorialesContactar a:
- Equipo de Ciberseguridad Nacional (CCN-CERT)
- ISMS Forum (coordinador observatorio)
- Investigador/Consultor: [Información Contacto]

10. RECONOCIMIENTOS Y REFERENCIAS

Basado en marcos y estándares:
- NIST Cybersecurity Framework 2.0 (NIST, Feb 2024)
- Esquema Nacional de Seguridad v3.0 (CCN-CERT, RD 311/2022)
- Directiva NIS2 (UE 2022/2555)
- Reglamento GDPR (UE 2016/679)
- ISO/IEC 27001:2022
- ACET User Guide (NCUA)
- FAIR Institute (Cuantificación Riesgos)
- INCIBE Balance Ciberseguridad 2024

Contribuyentes:
- Consorcio Científicos de Datos y Estrategas Ciberseguridad
- ISMS Forum Spain
- Observatorio Ciberseguridad (Universidades + Privado)
- Auditores y Reguladores colaboradores

¡Kit Listo para Usar! Comience Implementación Hoy.

Para preguntas: Consulte sección FAQ o contacte responsable ciberseguridad organizacional.