Informes Periódicos de Seguridad

Sede Barcelona

TechSys Solutions S.L.

Introducción

Al momento de la auditoría no se encontró esta documentación.

Este documento presenta tres modelos de informes periódicos de seguridad: mensual, trimestral y anual. Cada uno está diseñado para facilitar el seguimiento, análisis y comunicación del estado de la ciberseguridad en diferentes niveles.

El informe mensual aborda eventos recientes y métricas clave. El trimestral permite detectar tendencias y evaluar controles. El anual ofrece una visión estratégica para la dirección y la planificación futura.

Estos formatos buscan estandarizar la gestión informativa de la seguridad, apoyar la toma de decisiones y cumplir con los requisitos de mejora continua y cumplimiento normativo.

Informe Mensual de Seguridad

Objetivo: Supervisar y reportar el estado de la seguridad en corto plazo. Se centra en detección temprana, respuesta rápida e indicadores tácticos.

Estructura sugerida:

1. **Resumen ejecutivo**
    - Breve estado general del mes
    - Eventos más relevantes (positivo o negativo)
2. **Incidentes destacados del mes**
    - Breve descripción de cada incidente relevante
    - Categoría (malware, acceso no autorizado, phishing, etc.)
    - Estado (abierto, mitigado, cerrado)

    - Tiempo de respuesta
3. **Métricas clave**
    - Nº total de incidentes detectados
    - Nº de vulnerabilidades corregidas
    - Tiempo medio de detección y respuesta
    - Usuarios bloqueados / intentos fallidos de acceso
4. **Hallazgos de monitoreo y auditoría**
    - Alertas del IDS/IPS
    - Actividades sospechosas detectadas
    - Logs anómalos
5. **Recomendaciones y acciones pendientes**
    - Acciones implementadas durante el mes
    - Tareas planificadas para el mes siguiente

Informe Trimestral de Seguridad

Objetivo: Evaluar la evolución de las medidas de seguridad y analizar tendencias. Útil para tomar decisiones tácticas y ajustar políticas.

Estructura sugerida:

1. **Resumen ejecutivo**
    - Comparativa con trimestres anteriores
    - Avances en planes de mejora
2. **Análisis de incidentes acumulados**
    - Total de incidentes por tipo
    - Análisis de causas raíz
    - Incidentes recurrentes
3. **Evaluación de vulnerabilidades**
    - Resumen de escaneos trimestrales

    - Estado de las mitigaciones aplicadas
4. **Cumplimiento y auditoría**
    - Estado de cumplimiento normativo (ISO, RGPD, ENS)
    - Resultados de auditorías internas o externas
5. **Evolución de indicadores clave**
    - Comparativa de KPIs: detección, respuesta, resolución
    - Tendencias en accesos, alertas, uso de recursos
6. **Estado de planes y proyectos de seguridad**
    - Avance de iniciativas (MFA, backups, campañas de concienciación, etc.)
7. **Recomendaciones estratégicas**
    - Ajustes necesarios a políticas o infraestructura
    - Formación recomendada

Informe Anual de Seguridad

Objetivo: Visión estratégica del estado de ciberseguridad. Análisis global para la dirección, planificación y auditoría.

Estructura sugerida:

1. **Resumen ejecutivo**
    - Estado global de la ciberseguridad en el año
    - Principales logros y desafíos
    - Nivel de riesgo residual
2. **Resumen de incidentes del año**
    - Incidentes más críticos y su impacto
    - Costes asociados (si se conocen)
    - Tiempo medio de respuesta/resolución
3. **Análisis de riesgo**
    - Riesgos identificados vs mitigados

    - Evaluación general de exposición
4. **Cumplimiento legal y normativo**
    - Situación frente a normativas aplicables (ISO 27001, LOPD, ENS, etc.)
5. **Proyectos de seguridad ejecutados**
    - Proyectos iniciados y completados
    - Evaluación del retorno (ROI)
6. **Estado del SGSI (Sistema de Gestión de Seguridad de la Información)**
    - Revisión del ciclo PDCA (Plan-Do-Check-Act)
    - Auditorías, simulacros, campañas
7. **Plan estratégico de seguridad para el año siguiente**
    - Objetivos
    - Presupuesto estimado
    - Recursos necesarios
    - Prioridades