Indicadores y métricas de seguridad

Sede Barcelona

TechSys Solutions S.L.

Apreciación

No hemos encontrado ninguna documentación que hable específicamente sobre las métricas que se aplican en la sede de Barcelona de TechSys.

Teniendo en cuenta que las métricas son un aspecto realmente importante para poder monitorear, planificar y verificar que se cumplen las políticas y planes previamente preestablecidos. Hemos decidido incluir este archivo para que TechSys lo utilicé como base para sus indicadores y métricas.

Introducción

Con el objetivo de fortalecer la gestión de la seguridad de la información en la sede de Barcelona, se han definido un conjunto de indicadores clave de desempeño (KPIs) y acuerdos de nivel de servicio (SLAs). Estos permiten realizar un seguimiento continuo de la eficacia de las medidas de protección, la capacidad de respuesta ante incidentes, la disponibilidad de los sistemas críticos y el cumplimiento de políticas internas y normativas.

Las métricas presentadas se alinean con las directrices de la Política de Seguridad de la Información de TechSys Solutions S.L., el análisis de impacto del negocio (BIA), la metodología MAGERIT, y los principios de la Guía Nacional de Notificación y Gestión de Ciberincidentes. Están diseñadas para ser medibles, realistas y accionables, facilitando la toma de decisiones basada en datos.

---

1. Indicadores de Incidentes

Estos indicadores permiten medir la frecuencia, resolución y calidad del tratamiento de incidentes de seguridad informática registrados en la sede. Proveen visibilidad sobre la carga de trabajo del equipo de respuesta, la efectividad del sistema de detección y la evolución del entorno de amenazas.

Indicador	Descripción	Frecuencia	Fuente
Nº de incidentes registrados (mensual)	Total de incidentes detectados por IDS, antivirus, reportes manuales, etc.	Mensual	SIEM / Registro SGSI
% de incidentes resueltos dentro del SLA	Medido vs. el tiempo máximo definido para cada categoría de incidente	Mensual	Registro de incidentes / Bitácoras
Nº de falsos positivos (IDS/IPS)	Incidentes registrados que no resultaron ser amenazas reales	Trimestral	IDS logs / SOC

---

2. Indicadores de Tiempos (SLAs)

Los tiempos de detección, respuesta y recuperación son métricas esenciales para evaluar la eficiencia operativa del SOC y del equipo de TI. Su seguimiento permite optimizar la coordinación entre áreas técnicas y asegurar la continuidad operativa ante eventos de seguridad.

Indicador	Descripción	Objetivo	Fuente
Tiempo medio de detección (MTTD)	Tiempo entre ocurrencia y detección del incidente	< 1 hora	SOC / IDS
Tiempo medio de respuesta (MTTR)	Desde la detección hasta la mitigación	< 4 horas	Registro de tickets
Tiempo medio de recuperación (MTTR2)	Desde mitigación hasta restauración total	< 8 horas	Equipos TI / DRP

---

3. Indicadores de Disponibilidad

La disponibilidad de los sistemas críticos es una métrica directa del impacto que pueden tener los fallos técnicos o incidentes de seguridad en la operativa del negocio. Estos indicadores permiten anticipar problemas, justificar inversiones en redundancia y evaluar la resiliencia de la infraestructura.

Indicador	Descripción	Meta	Fuente
% de disponibilidad de sistemas críticos	Tiempo efectivo operativo sobre tiempo total planificado	≥ 99,5%	Zabbix / Nagios / Logs

Nº de caídas no planificadas	Fallos imprevistos de sistemas esenciales (ERP, VPN, SIEM)	≤ 1 mensual	Herramientas de monitoreo

---

4. Indicadores de Cumplimiento

Estos indicadores miden el grado de alineación de la organización con las políticas de seguridad, procedimientos de protección de datos y medidas preventivas. Refuerzan el componente humano y el control de acceso como factores críticos en la defensa integral de la información.

Indicador	Descripción	Meta	Fuente
% de usuarios con formación en seguridad vigente	Personal con capacitación actualizada < 12 meses	100%	RRHH / Comité Seguridad
Nº de accesos no autorizados detectados	Intentos fallidos, alertas por MFA, accesos indebidos	0	Logs / SIEM
% de backups verificados y restaurables	Verificaciones exitosas de pruebas de restauración	≥ 90%	DRP / Informes de prueba