Catálogo de servicios de ciberseguridad

Alineado la Norma Internacional ISO/IEC 20000-1:2018

Organización: Technoma S.A.E.C.A.

Estado: Aprobado - Versión Pública

Fecha de Emisión: Julio 2026

Destinatarios: Clientes, Usuarios y Partes Interesadas

INTRODUCCIÓN Y PROPÓSITO

En el entorno corporativo actual, la resiliencia tecnológica y la protección de la información son pilares críticos para la continuidad del negocio. Technoma S.A.E.C.A., como empresa líder en soluciones tecnológicas en Paraguay, presenta su Catálogo de Servicios de Ciberseguridad alineado bajo el estándar internacional ISO/IEC 20000-1:2018.

Este catálogo tiene como finalidad primordial ser un documento claro, accesible y transparente para nuestros clientes, socios estratégicos y partes interesadas. En él se definen las características operativas, niveles de servicio (SLA), alcances y mecanismos de interacción para garantizar una entrega de valor medible y predecible.

ALINEACIÓN CON ISO/IEC 20000-1:2018

De acuerdo con la cláusula 7.5.1 y los requisitos de gobernanza del estándar ISO 20000-1, este catálogo representa la “Vista de Negocio”, estructurando los servicios desde la perspectiva de cara al cliente. Cada servicio aquí descrito cuenta con una matriz correlativa interna que asegura la correcta asignación de recursos, gestión de capacidades, gestión de niveles de servicio y mejora continua. Asimismo, en cumplimiento del requisito 8.2.4 de la norma ISO/IEC 20000-1:2018, cada ficha técnica de servicio identifica expresamente los clientes destinatarios a los que va dirigido el servicio, los resultados esperados de su prestación y las dependencias internas y externas necesarias para su entrega.

PORTAFOLIO DE SERVICIOS DISPONIBLES

A continuación, se detallan las fichas técnicas formales de los servicios de ciberseguridad activos.

MONITOREO Y RESPUESTA A INCIDENTES (SOC)

Estado del Servicio:	Activo
Propietario del Servicio:	SOC Manager
Descripción del Alcance (Objetivo/Medible):	Monitoreo continuo de eventos de seguridad (24x7), correlación de alertas mediante SIEM centralizado, triaje analítico de incidentes, contención primaria automatizada o manual de amenazas (aislamiento lógico de red) y escalamiento. Exclusiones explícitas: Excluye la remediación definitiva de infraestructura afectada y la restauración de copias de seguridad.
Usuarios Autorizados:	Toda la organización cliente (personal interno y terceros) para reportes de anomalías; administradores de infraestructura de TI para escalamiento conjunto.
Ventana de Disponibilidad:	24x7
SLA:	Tiempo de respuesta ante alertas críticas: $T_{resp} \leq 15$ min. Fórmula de medición: $T_{resp} = T_{detección\_SIEM} - T_{notificación\_analista}$ Tiempo de contención inicial: $T_{cont} \leq 60$ min desde la confirmación del incidente.
Mecanismo de Solicitud:	Ingesta automatizada de alertas en plataforma de operaciones de ciberseguridad, formulario estandarizado de "Incidentes de Seguridad" en el Portal de Service Desk de Technoma, o llamada directa a la línea de emergencia telefónica del SOC.
Clientes Destinatarios:	Organizaciones clientes con contrato vigente del servicio de SOC gestionado: entidades de los sectores financiero, industrial, comercial, de servicios y público que operan infraestructura tecnológica crítica. Interlocutores designados: Oficial de Seguridad de la Información (CISO), Gerencia de TI y responsables de infraestructura del cliente.

GESTIÓN DE VULNERABILIDADES

Estado del Servicio:	Activo
Propietario del Servicio:	SOC Manager
Descripción del Alcance (Objetivo/Medible):	Ejecución periódica de análisis de vulnerabilidades en infraestructura tecnológica, redes corporativas y aplicaciones web, clasificación de criticidad técnica basada estrictamente en la escala CVSSv3, y entrega de informes estructurados con planes de remediación priorizados dirigidos a los custodios de los activos.
Usuarios Autorizados:	Administradores de Servidores, Equipos de Desarrollo de Software, Gerentes de Aplicaciones de Negocio y Oficial de Seguridad de la Información (CISO) del cliente.
Ventana de Disponibilidad:	Lunes a viernes de 08:00 a 18:00.
SLA:	Emisión del reporte técnico de vulnerabilidades: $T_{Rep} \leq 48$ horas hábiles tras la finalización del escaneo.
Mecanismo de Solicitud:	Lanzamiento automático programado mensual según el inventario de activos de la CMDB, solicitud extraordinaria vía correo electrónico soc@technoma.com.py o mediante el Portal de Servicios.
Clientes Destinatarios:	Organizaciones clientes con contrato vigente del servicio, dirigido a las áreas de Tecnología de la Información, Desarrollo de Software y Seguridad de la Información del cliente, así como a los custodios de los activos tecnológicos incluidos en el alcance.
Resultados Esperados:	Identificación y clasificación de las vulnerabilidades presentes en los activos evaluados conforme a la escala CVSSv3; entrega de un reporte técnico con plan de remediación priorizado por criticidad; reducción progresiva y medible de la superficie de exposición.
Dependencias del Servicio:	Internas: herramienta de escaneo de vulnerabilidades con licenciamiento y firmas actualizadas, personal técnico especializado, inventario de activos vigente en la CMDB y el servicio de Monitoreo y Respuesta a Incidentes (SOC) para el tratamiento de hallazgos. Externas (del cliente y terceros): accesos y credenciales de escaneo autorizados, ventanas de mantenimiento aprobadas, disponibilidad de los custodios de activos para la remediación y operatividad.

Resultados Esperados:	Detección y notificación oportuna de eventos de seguridad; reducción del tiempo de exposición ante amenazas activas; contención temprana de los incidentes confirmados; trazabilidad completa del ciclo de vida de cada incidente en la herramienta de gestión; e informe mensual de eventos, incidentes y cumplimiento de los SLA comprometidos.
Resultados Esperados:	Internas: plataforma SIEM centralizada con licenciamiento vigente, personal analista del SOC en turnos 24x7, inventario de activos actualizado en la CMDB y el servicio de Gestión de Vulnerabilidades como insumo de contexto de riesgo. Externas (del cliente y terceros): conectividad permanente y envío continuo de logs desde los activos monitoreados (agentes/colectores), disponibilidad del personal de TI del cliente para las acciones de remediación definitiva, proveedor de enlace de datos y servicio de telefonía de la línea de emergencia.