SPACEX

TEC-CYB-2025-001

Informe de Ciberseguridad y Desempeño Tecnológico

Tecnología, DevOps, Redes, Servidores y SGSI – Módulo TI

PERIODO DE REPORTE	FECHA DE GENERACIÓN	RESPONSABLE TI	MONITOREO CENTRAL
Octubre 2025	09 de Noviembre de 2025	Ing. Laura Méndez – Directora de Tecnología	SOC – Centro de Operaciones de Seguridad

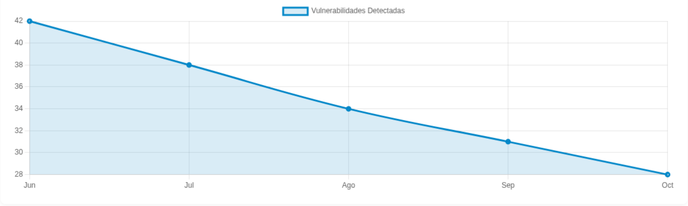
Indicadores Principales del Periodo

DISPONIBILIDAD DEL SISTEMA	INCIDENTES DE SEGURIDAD	CUMPLIMIENTO SGSI (PHVA)	SLA MESA DE AYUDA
99.92%	8	93%	95%
↑ +0.05% vs mes anterior	↓ -3 vs mes anterior	↑ +2.0% avance mensual	↑ +1.2% vs meta

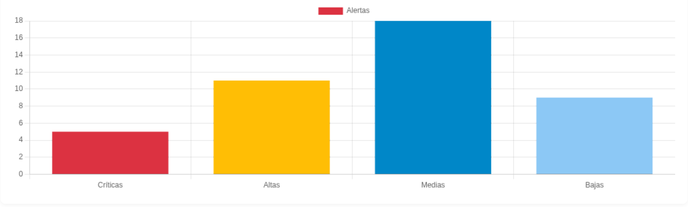
Incidentes Tecnológicos y de Seguridad

ID INC.	MÓDULO / SISTEMA	DESCRIPCIÓN	SEVERIDAD	IMPACTO	ESTADO
IT-001	SOC / Firewall	Intento de intrusión vía fuerza bruta desde IP extranjera	CRÍTICA	Riesgo de acceso no autorizado	Cerrado
IT-002	DevOps / CI-CD	Token expuesto en repositorio público durante commit	ALTA	Riesgo de despliegos manipulados	Cerrado
IT-003	Redes / VLAN SCADA	Tráfico anómalo detectado entre PLC y nodo industrial	CRÍTICA	Impacto potencial en producción	En proceso
IT-004	Servidores / Linux	Falla de kernel durante actualización programada	ALTA	Degradación de rendimiento	Cerrado
IT-005	ERP / Base de Datos	Consulta bloqueada por deadlock en módulo financiero	MEDIA	Retraso en procesos contables	Cerrado
IT-006	Mesa de Ayuda	Error en autenticación SSO para 27 usuarios	MEDIA	Interrupción parcial de acceso	Cerrado
IT-007	Correo Corporativo	Campaña de phishing simulada: 12 clics reportados	BAJA	Riesgo educativo	Cerrado
IT-008	SGSI / PHVA	Desviación en control de eliminación de medios digitales	MEDIA	Incumplimiento parcial de política	En proceso
IT-009	SOC / SIEM	Alertas correlacionadas por comportamiento anómalo en BD	ALTA	Riesgo de fuga de datos	Abierto
IT-010	Redes / WiFi Corporativa	Cliente no autorizado intentando asociarse al SSID interno	BAJA	Intento de acceso menor	Cerrado
IT-011	Servidores / Windows	Parches críticos pendientes en servidor de respaldos	ALTA	Riesgo de explotación conocida	En proceso
IT-012	DevSecOps	Fallo en escaneo SAST por configuración errónea	MEDIA	Reducción de visibilidad en código	Cerrado
IT-013	Infraestructura / UPS	Descarga inesperada en UPS secundaria del clúster	ALTA	Riesgo de apagado no controlado	Abierto
IT-014	ERP / API	Timeout en módulo de autenticación	MEDIA	Demora en inicio de sesión	Cerrado
IT-015	VPN Corporativa	Usuario externo dejó sesión activa durante 26 horas	BAJA	Riesgo bajo por persistencia	Cerrado

Tendencia de Vulnerabilidades Detectadas



Clasificación de Alertas del SOC (SIEM)



Alertas Críticas del SOC

Resumen de Alertas Detectadas – Total: 5

- **04/Oct:** Múltiples intentos fallidos de MFA en cuentas administrativas.
- **10/Oct:** Anomalía en tráfico SSH detectada en nodo DB-02 del ERP.
- **16/Oct:** Script sospechoso detectado en pipeline de integración continua.
- **21/Oct:** Comunicación no autorizada entre segmentos de red internos.
- **28/Oct:** Archivo con comportamiento malicioso aislado por EDR.

Resumen Ejecutivo del Periodo

Estado General Tecnológico y de Seguridad

Durante octubre de 2025, el ecosistema tecnológico de SpaceX mantuvo un desempeño estable con una disponibilidad del 99.92% en los servicios principales del ERP y los sistemas críticos del área operativa.

El cumplimiento del SGSI alcanzó un 93%, evidenciando avances constantes en controles de acceso, gestión de vulnerabilidades y auditorías internas. Se identificaron 8 incidentes relevantes, de los cuales dos fueron clasificados como críticos, siendo gestionados oportunamente por el SOC.

El fortalecimiento del pipeline DevSecOps permitió reducir el tiempo de detección de fallos de seguridad en repositorios, mientras que las medidas aplicadas en la red interna y SCADA garantizaron integridad operativa en áreas sensibles.

En general, el entorno TI presenta madurez creciente y alineación con las políticas SGSI–PHVA.

Medidas de Mejora Tecnológica

- ✓ Actualizar reglas de detección en el SIEM para correlación avanzada de tráfico SSH y VPN corporativa.
- ✓ Implementar autenticación reforzada en pipelines DevOps para evitar exposición de tokens.
- ✓ Ampliar segmentación de red en VLAN internas vinculadas a SCADA y equipos críticos.
- ✓ Integrar monitoreo de integridad (FIM) en nodos de base de datos del ERP.
- ✓ Reforzar el programa de capacitación sobre ingeniería social y phishing para todo el personal.