

## Informe de Ciberseguridad y Desempeño Tecnológico

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

PERÍODO 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

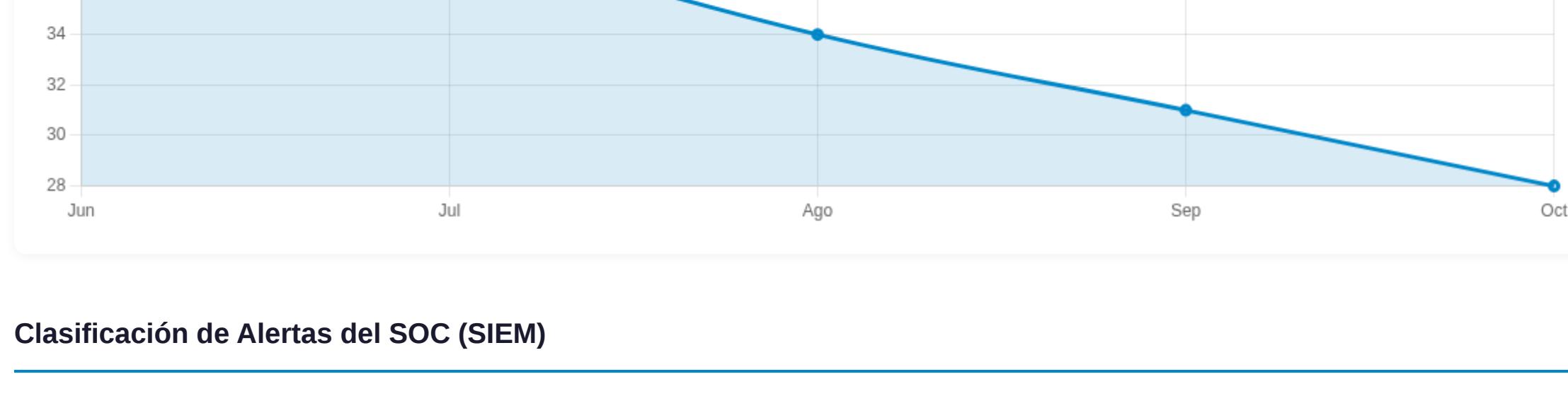
## Indicadores Principales del Periodo

DISPONIBILIDAD DEL SISTEMA <b>99.92%</b> ↑ +0.05% vs mes anterior	INCIDENTES DE SEGURIDAD <b>15</b> ↓ -3 vs mes anterior	CUMPLIMIENTO SGSI (PHVA) <b>93%</b> ↑ +2.0% avance mensual	SLA MESA DE AYUDA <b>95%</b> ↑ +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	Degrado 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: 2
► 04/Oct: Intentos fallidos masivos de MFA en cuentas administrativas.
► 10/Oct: Anomalía crítica en tráfico SSH hacia nodo DB-02 del ERP.

## Resumen Ejecutivo del Periodo

Estado General Tecnológico y de Seguridad
Durante octubre de 2025 se registraron 15 incidentes tecnológicos y de seguridad en los módulos TI, SOC, ERP, VPN y DevOps. La mayor concentración se ubicó en alertas de severidad alta y media, con dos incidentes clasificados como críticos y atendidos de forma prioritaria.

A pesar del incremento natural de actividad por expansiones operativas, la disponibilidad del sistema se mantuvo en **99.92%**, respaldada por mejoras en redundancia de servidores y controles SGSI. El cumplimiento del ciclo PHVA del SGSI alcanzó el **93%**, mejorando procesos de auditoría interna, análisis de vulnerabilidades y trazabilidad.

El SOC registró dos alertas críticas asociadas a intentos de intrusión y anomalías SSH. Gracias a la correlación SIEM y el monitoreo continuo, no se identificaron brechas de datos.

Los tiempos de respuesta de la Mesa de Ayuda mostraron un SLA del **95%**, reflejando estabilidad operativa y cumplimiento de metas técnicas.

Medidas de Mejora Tecnológica
✓ Ajustar reglas avanzadas de correlación SIEM para tráfico SSH y VPN. ✓ Implementar autenticación reforzada en pipelines DevOps. ✓ Extender segmentación de red en VLAN SCADA y equipos críticos. ✓ Activar monitoreo FIM en nodos de base de datos del ERP. ✓ Ampliar el programa de capacitación sobre phishing y amenazas sociales.

Resumen de Seguridad y Cumplimiento
-------------------------------------

Periodo de Reporte	Monitoreo Central	Resumen Ejecutivo
Octubre 2025	SOC – Centro de Operaciones de Seguridad	95% SLA

Resumen de Seguridad y Cumplimiento
-------------------------------------

Resumen de Seguridad y Cumplimiento
-------------------------------------

Resumen de Seguridad y Cumplimiento
-------------------------------------

Resumen de Seguridad y Cumplimiento
-------------------------------------