GlobalSuite
SOLUTIONS

GRC – Incident

Entradas

Entradas

Id	Asunto	Descripción	Tipo
260123162356	ISO/IEC 27011 Security Incident	Detected repeated failed authentication attempts against the Session Border Controller (SBC-01) administrative interface, indicating a potential brute-force attempt and risk of toll fraud or service disruption. This incident requires immediate containment, verification of exposure, and validation of controls aligned with ISO/IEC 27011 (telecommunications security).	Incidencias y Problemas

Datos del Ticket

Id	"260123145454"
Asunto	ISO/IEC 27011 Internal Audit – Telecom & Network Security Controls
Descripción	Detected repeated failed authentication attempts against the Session Border Controller (SBC-01) administrative interface, indicating a potential brute-force attempt and risk of toll fraud or service disruption. This incident requires immediate containment, verification of exposure, and validation of controls aligned with ISO/IEC 27011 (telecommunications security).
Fecha de Registro	02/02/2026 09:18:20
Tipo	Incidencia
Estado	Investigación
Cliente/Contacto	Joshua Ortiz
Contacto/Grupo	Otro Contacto
ticketFields.anotherContact	
E-mail	joshua.ortiz@gcr.com
Alerta E-Mail	No

Servicios

Servicios/Procesos
- Vulnerability Remediation & Mitigation Service

Áreas Afectadas

Áreas Afectadas
Seguridad
Aplicación

Trabajo de Auditoría

Nombre	Plan Auditoría

Suministrador	
¿Supera SLA?	No
Cumplimiento SLA	Si
Agente de Evento	SIEM Alert (Correlation Rule: VoIP Admin Brute Force)
Detectado por	Cybersecurity Engineer
Elemento Afectado	Session Border Controller – SBC-01 (Management Interface)

Referencias

Nombre	URL
Risk of service disruption	

Impacto	Baja
Urgencia	Media
Prioridad	Baja

Riesgos

Riesgos

Empleados

Empleados

Empleado	Descripción
Joshua Ortiz	

Evidencias

Evidencias	SIEM screenshot/export showing timestamps, source IPs, username attempts Firewall logs (edge) confirming inbound attempts SBC-01 authentication logs Any applied ACL change record (change ticket / diff)

Evidencias

Evidencias	Extensión	Fecha	Descripción

Seguimiento

Tiempo de respuesta	15 minutes (initial triage + containment started)

Causa raíz	SBC management interface was reachable from a broader network segment than intended due to an overly permissive firewall/ACL rule.
Solución Temporal	Block offending source IPs at the firewall Restrict management access to VPN/admin subnet only Force credential rotation for SBC admin accounts
Medidas	Implement strict allowlist for management ports Enable MFA (where supported) and enforce least privilege Review all telecom management exposures (SBC, PBX, VoIP gateways) Improve SIEM detection thresholds + alert routing Schedule a post-incident review and update runbooks (ISO/IEC 27011)
Datos restaurados	Not applicable (no data loss confirmed).
Procedimientos	IRP-27011-001 – Telecom Security Incident Handling CHG-001 – Change Management (Firewall/Network)

Seguimientos

Usuario	Fecha	Descripción

Riesgos en Tiempo Real

Relacionar elementos

Nombre	Categoría	Propietario	Análisis

Cierre

Resolución	
Tiempo de resolución	
Fecha de cierre	
Recomendaciones	

Salidas

Salidas

Id	Asunto	Descripción	Tipo