

CIBERRESILIENCIA CONECTADA

Del esfuerzo individual a la defensa colectiva

Cómo convertir la seguridad digital en capacidad operativa para cumplir la promesa de valor del CSC

Jorge Fernando Bejarano Lobo

Consultor de organismos multilaterales y entidades públicas
Director y fundador de Tech and Law



Ciberresiliencia, Satisfacción, Confianza

La concentración que crea valor también concentra el impacto



80% de los centros operan con
alcance regional o global

Fuente: ANDI-KPMG, Evolución e impacto de los GBS en Colombia 2025, p. 8.

El efecto CSC

- **Escala**
Una falla local puede afectar varias compañías, países y procesos.
- **Automatización**
Un error o abuso se replica con velocidad y volumen.
- **Datos**
La centralización amplía el valor del activo y el daño potencial.
- **Dependencias**
Nube, identidades, integraciones y terceros comparten el mismo servicio.

La promesa de valor ahora depende de confianza que podemos demostrar...

Eficiencia

Procesos estables
y costos previsibles

Experiencia

Servicio confiable
para clientes
internos

Escala e innovación

Datos,
automatización e
IA

Rendimiento

Valor agregado y
credibilidad

CONFIANZA

Continuidad, integridad de transacciones, protección de
datos y respuesta transparente

La confianza acelera la contratación, la ampliación del alcance y la renovación del servicio.

Base: cuatro palancas de evolución de GBS, EY-ANDI. Interpretación de ciberresiliencia del autor.

Ciberseguridad y ciberresiliencia responden preguntas distintas

CIBERSEGURIDAD

¿Cómo reducimos la probabilidad y el impacto de un incidente?

Controles de acceso
Protección de datos
Vulnerabilidades y configuración
Monitoreo y respuesta

CIBERRESILIENCIA

¿Cómo mantenemos el servicio cuando algo ya falló o fue comprometido?

Anticipar

Resistir

Recuperar

Adaptar

Diseñar para continuar con identidades, integraciones o proveedores degradados

El perímetro real del CSC es el servicio de punta a punta



Herramientas: mapa de servicio + BIA + flujo de datos + inventario de terceros

Seis pruebas de capacidad

Capacidad	Prueba ejecutiva	Evidencia mínima / indicador
Gobierno	¿Quién decide detener, degradar o reanudar?	Dueño del servicio, umbrales y autoridad
Dependencias	¿Qué necesita operar y por cuánto tiempo?	Mapa E2E, BIA, RTO/RPO y ruta alterna
Identidad y datos	¿Podemos limitar el radio de impacto?	MFA resistente, PAM, segregación e integridad
Detección y respuesta	¿Vemos y contenemos a través de la cadena?	Telemetría, playbooks, MTTC y comunicación
Recuperación	¿Restauramos limpio y reconciliamos?	Backups inmutables y prueba contra RTO/RPO
Terceros	¿Conocemos concentración, subcontratación y salida?	Tiering, cláusulas, monitoreo y ejercicio conjunto

Lo que un cliente corporativo realmente compra

PROMESA

**“Operación
segura y
disponible”**



EVIDENCIA

- 1 Alcance de controles por servicio, no solo certificación corporativa
- 2 Excepciones de auditoría, responsables y fechas de remediación
- 3 RTO/RPO y resultado del último ejercicio de recuperación
- 4 Reglas de notificación y coordinación de incidentes
- 5 Ubicación, acceso, subprocesadores y eliminación de datos
- 6 Plan de salida, portabilidad y continuidad de conocimiento

Reto:

La respuesta de seguridad existe a nivel del grupo, pero es muy difícil probar su alcance en el servicio del CSC.

Terceros: el riesgo se gestiona por servicio y concentración



La dependencia crítica puede estar en un cuarto proveedor

Elementos / servicios con subcontratación, concentración geográfica, credenciales compartidas, alternativas de operación y borrado seguro.

Ej.: Un viernes a las 16:42: una credencial del proveedor fue comprometida

Escenario: la cuenta administra una automatización de pagos. Hay transacciones en cola y no se conoce aún el alcance.

0–15 min

Contener

- Suspender la cuenta y tokens
- Aislar la automatización
- Preservar evidencia
- Activar mando del incidente

15–60 min

Mantener

- Activar ruta manual o alterna
- Validar integridad de la cola
- Definir impacto y clientes
- Aplicar criterio de notificación

1–4 h

Recuperar

- Rotar secretos
- Reconstruir desde base confiable
- Reconciliar transacciones
- Reanudar de forma controlada

< 24 h

Aprender

- Comunicar hechos y ventana
- Revisar con cliente y proveedor
- Asignar correctivos
- Actualizar playbook y contrato

Se debería garantizar que sea posible continuar con la prestación el servicio sin perder integridad ni ocultar incertidumbre, a pesar del incidente.

Ejemplos de herramientas que deberíamos tener, integradas por flujo de decisión

Decisión	Herramientas útiles	Resultado que debe producir
¿Qué es crítico?	Mapa de servicio, BIA, CMDB/CAASM, flujo de datos	Dependencias, dueño y tolerancia
¿Quién puede hacer qué?	IAM, MFA, PAM, bóveda de secretos, IGA	Acceso mínimo, trazable y revocable
¿Qué está ocurriendo?	SIEM/SOAR, EDR/XDR, NDR, telemetría cloud	Detección priorizada por servicio
¿Cómo limitamos daño?	Segmentación, DLP, controles cloud/CNAPP	Contención sin apagar todo el CSC
¿Cómo recuperamos?	Backup inmutable, clean room, orquestación, conciliación	Restauración limpia dentro del RTO/RPO
¿Cómo demostramos?	GRC, repositorio de evidencias, monitoreo de terceros	Paquete de aseguramiento actualizado

La integración, la propiedad y la práctica convierten licencias en capacidad

Tablero gerencial: indicadores que conectan seguridad con servicio

1

Cobertura

% de servicios críticos con mapa E2E y BIA vigentes

2

Identidad

% de accesos privilegiados revisados y con MFA resistente

3

Visibilidad

% de activos críticos con telemetría útil en el SOC

4

Contención

Tiempo para limitar el escenario prioritario, medido en ejercicio

5

Recuperación

% de pruebas que cumplen RTO/RPO e integridad

6

Terceros

% de proveedores críticos con salida y ejercicio validados

Evite métricas de actividad sin contexto: alertas bloqueadas, vulnerabilidades contadas o cursos completados.

Seis preguntas para reflexionar estratégicamente

- 1 **¿Cuáles tres servicios no pueden fallar el próximo lunes?**
- 2 **¿Cuánto tiempo puede operar cada uno en modo degradado?**
- 3 **¿Qué identidad o proveedor genera el mayor radio de impacto?**
- 4 **¿Quién puede detener una automatización o un pago?**
- 5 **¿La última restauración cumplió RTO, RPO e integridad?**
- 6 **¿Qué diremos al cliente durante la primera hora?**

La ciberresiliencia vive en el ADN del CSC cuando la organización puede demostrar que anticipa, contiene, continúa y aprende junto con clientes y proveedores.

¡Muchas gracias!



¿Y sí además de
haber participado, te
llevas mi contacto
escaneando este
código QR?



@jfbejarano
@TechAndLawCo



www.techandlaw.com.co



jfbejarano@techandlaw.com.co

