RIESGO DE PROVEEDORES TECNOLÓGICOS Y SERVICIOS CRÍTICOS

Hernán Fagua

"El conocimiento adquiere valor cuando se comparte. Gracias por permitirme ser parte de este espacio."

SKYFALL IT SECURITY

SOBRE MI

COLOMBIA - BOGOTÁ

Ingeniero Informático / Especialista en Ciberseguridad

Gobierno de TI, Ciberseguridad, Riesgos, Continuidad y Resiliencia Operacional.

Experiencia Sectorial.

Gobierno | Financiero | Salud | Energético | Aéreo | Ambiental

¿ Qué pasa cuando falla un Proveedor Crítico ?

¿ Cuanto Tiempo puede seguir operando nuestra organización sin el?

5 Min | 1 Hora | 4 Horas | 24 Horas

¿ Qué tan dependientes somos de un proveedor ?

No siempre lo vemos.

Pero..... La dependencia también es una forma de riesgo..

ANTECEDENTES.....

2022

- Ransomware LockBit

- Entidad Financiera experimentó problemas reputacionales y de filtración de datos.

2023

Filtración de registros médicos confidenciales e historiales clínicos.

2024

- Filtración masiva de datos en el sector financiero.

- Degradación en los servicios críticos de diversas entidades del sector gobierno

2025

Proveedores de Telecomunicaciones / Filtración de datos sensibles

2026

- El "Apagón" Técnico por Proveedor

- Filtración información privada de miles de clientes

De la relación con el proveedor a la dependencia del negocio

¿ QUE OCURRE SI SE DETIENE ?

- Impacto
- Dependencia
- Sustitución
- Tiempo de Recuperación

¿ A cuál de estos le permitiría fallar mañana ?

Mayor Criticidad

Menor Criticidad

1. **PROCESOS DE PAGO / SERVICIOS FINANCIERO**
2. **CLOUD / INFRAESTRUCTURA**
3. **SOFTWARE / DESARROLLO**
4. **SUMINISTROS / SERVICIOS GENERALES**

Efectos / Consecuencias

- Interrupciones
- pérdidas económicas
- Daño Reputacional
- Afectación a clientes

Puntos Ciegos

- Dependencias Ocultas
- Concentración del Riesgo
- Visibilidad Limitada
- Recuperación Incierta

El error no es tener proveedores Críticos el error es tratarlos como si no lo fueran.

No se Puede Gestionar lo que No se identifica.

Radiografía base de proveedores.

- 300 + Proveedores activos
- 65 con acceso a información sensible
- 48 soportan procesos esenciales
- 17 puntos únicos de falla
- 12 Tiempos de recuperación Críticos

Descubrir / Responder

- ¿ Qué procesos y servicios soporta cada proveedor ?
- ¿ Cuanta concentración tenemos por proveedor ?
- ¿ Qué información y activos tiene bajo su control ?
- ¿ Tenemos alternativas y en cuanto tiempo ?
- ¿ Cuanto tardaríamos en volver a la normalidad ?

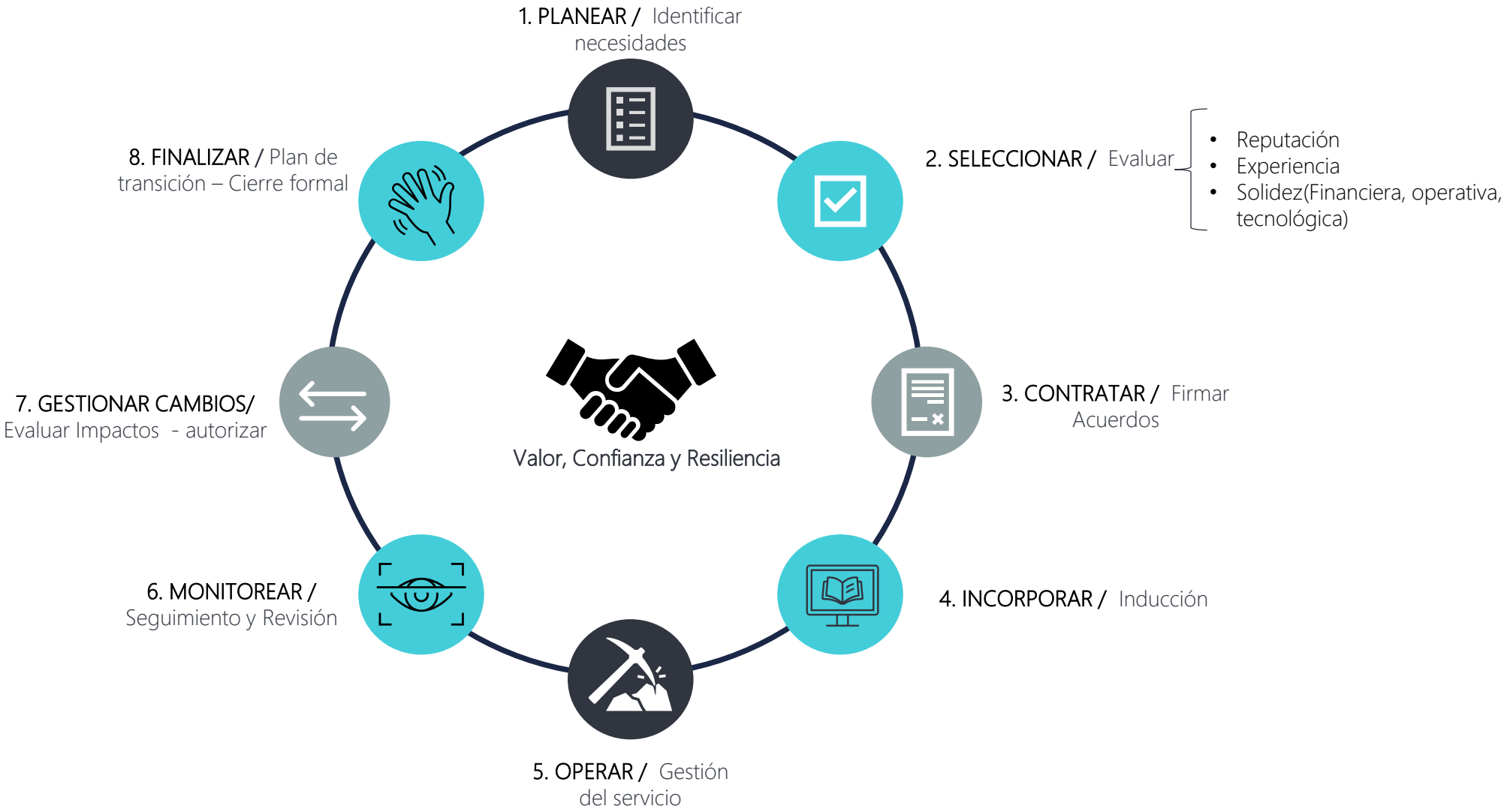
La visibilidad es el primer paso para gestionar el Riesgo.

Marco de Decisión

¿CUÁL ES LA PRIMERA LÍNEA DE DEFENSA?

Enfoque Estratégico	Alineación al Negocio	Basado en el apetito del riesgo	Generación de Valor - Resiliencia	Evitar SILOS funcionales

DEL RIESGO A LA RELACIÓN CON EL PROVEEDOR



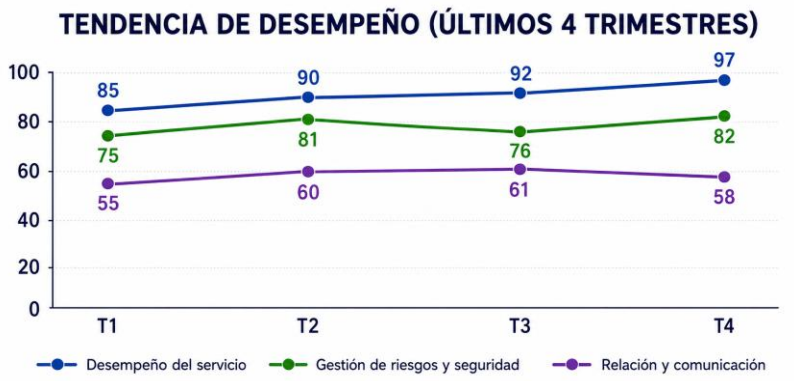
NO SOLO SE TRATA DE CONTRATAR.
Se trata de gestionar el riesgo durante toda la relación.

EVALUACIÓN Y DESEMPEÑO

SCORE GENERAL DE PROVEEDOR

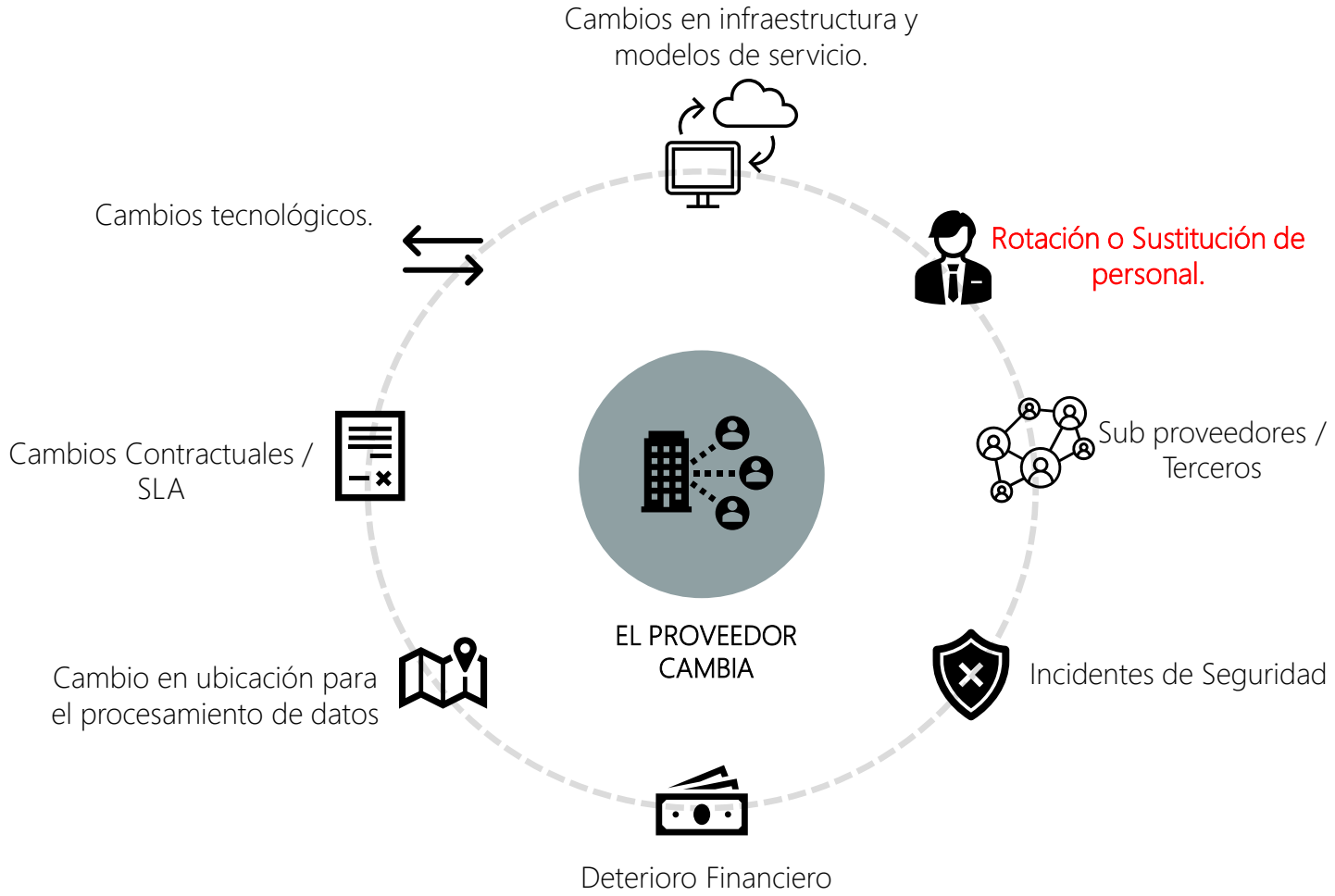
DESEMPEÑO DEL SERVICIO ANS - XLA	GESTIÓN DE RIESGOS / SEGURIDAD	RELACIÓN Y COMUNICACIÓN	CUMPLIMIENTO Y CONFORMIDAD	SOLIDEZ DEL PROVEEDOR Y SOSTENIBILIDAD
90 / 100	85 / 100	80 / 100	85 / 100	80 / 100
30%	25%	20%	15%	10%

Indicador	Resultado	Meta	Estado
Cumplimiento de SLA	92%	≥ 90%	Cumple
Disponibilidad del servicio	98,50%	≥ 95%	Cumple
Tiempo de respuesta a incidentes	2,1 h	≤ 4 h	Cumple
Incidentes críticos	0	≤ 1	Cumple
Vulnerabilidades críticas abiertas	1	≤ 2	Cumple
Cumplimiento de planes de mejora	78%	≥ 80%	Atención
Satisfacción del cliente interno - XLA	4,2 / 5	≥ 4,0	Cumple



El Riesgo No es Estático = ✕

Un proveedor puede tener un buen desempeño HOY y aumentar su riesgo mañana, debido a múltiples factores que están fuera de nuestro control directo.



Un buen desempeño pasado….. NO GARANTIZA UN BAJO RIESGO FUTURO

Gestión de Proveedores Críticos - Requisitos

De la definición del riesgo a la gestión de la relación con el proveedor.

Lo que no se Exige en los acuerdos, no se puede medir, ni gestionar, ni garantizar.

Del Requisito al Acuerdo

RIESGO		REQUISITO	¿CÓMO LO EXIGIMOS?	¿CÓMO LO COMPROBAMOS?
🔐	Ciberataques y fraude digital	Controles de acceso, MFA, monitoreo y detección	Cláusulas de seguridad, MFA obligatorio y gestión de accesos privilegiados	Logs, reportes de monitoreo, pruebas de seguridad y auditorías
🗄️	Fuga o pérdida de información	Protección, cifrado y confidencialidad	Cláusulas de confidencialidad, cifrado y protección de datos	Evidencias de cifrado, pruebas de seguridad y auditorías
☁️	Indisponibilidad de servicios críticos	Continuidad, recuperación y disponibilidad	SLA, RTO/RPO, BCP/DRP y pruebas periódicas	Pruebas de recuperación, disponibilidad y cumplimiento de SLA
🚨	Incidentes de ciberseguridad	Detección, notificación y respuesta oportuna	SLA de notificación, tiempos máximos de respuesta y cooperación	Registros de incidentes, tiempos de respuesta e informes
🔗	Terceros y sub proveedores	Visibilidad y control de la cadena de suministro	Declaración de subproveedores, evaluación previa y derecho de supervisión	Inventario de terceros, evaluaciones y auditorías
⚖️	Incumplimiento normativo	Cumplimiento regulatorio y contractual	Cláusulas específicas de cumplimiento y obligaciones regulatorias	Certificaciones, informes, auditorías y planes de acción
🚪	Dependencia y dificultad de salida	Portabilidad, transición y estrategia de salida	Cláusulas de terminación, devolución de información y asistencia en transición	Pruebas de salida, documentación y evidencias de portabilidad

Riesgo → Requisito → Evidencia

¿ Estamos Realmente Preparados ?

¿ SABEMOS CÚANTO PODEMOS RESISTIR?

¿ Conocemos El Impacto, El Tiempo Max Tolerable Y Dependencias Criticas ?

¿ DISPONEMOS DE ALTERNATIVAS VIABLES ?

¿ Contamos con opciones o alternativas que nos permitan mantener el servicio ?

¿ PODEMOS RECUPERAR EL SERVICIO ?

¿ Tenemos planes o estrategias de continuidad y recuperación funcionales ?

¿ PODEMOS EXIGIR LO QUE ACORDAMOS ?

¿ Nuestros acuerdos son claros, medibles y verificables?

¿ PODEMOS SALIR DEL PROVEEDOR SIN DETENER EL NEGOCIO ?

¿ Podemos hacer una transición ordenada y mantener la operación ?

La Verdadera gestión del riesgo asociado a proveedores o terceros, no consiste en evitar toda la dependencia.

- **Consiste en Conocerla, Gobernarla y estar preparados para cuando falle.**


GRACIAS