SOLVAN - IT Risk & Continuity Assessment

Evaluación Ejecutiva de Infraestructura, Continuidad Operativa y Ciberseguridad

---

Objetivo del Assessment

Identificar riesgos operativos, vulnerabilidades potenciales, oportunidades de optimización y áreas de fortalecimiento en infraestructura tecnológica, continuidad operativa y ciberseguridad, mediante una evaluación consultiva de alto nivel alineada a las necesidades del negocio.

Sesión consultiva ejecutiva

FASE 1 — Discovery Ejecutivo

30–45 minutos.

Conversación guiada. Participantes ideales:

- TI
- Infraestructura
- Seguridad
- Operaciones
- incluso Finanzas.

Según la necesidad del cliente, ajustar los bloques y preguntas, propuesta de enviar el cuestionario previo a la sesión de Discovery.

Opción a que lo conteste previo a la reunión, o que lo conteste con nosotros en l la sesión para abrir la conversación.

FASE 2 — Scorecard SOLVAN

Entrega visual:

- semáforo,
- hallazgos,
- riesgos,
- quick wins,
- recomendaciones.

FASE 3 — Workshop Técnico (solo si aplica)

Aquí entra:

- preventa,
- arquitectos,
- ingeniería.

He ajustado y equilibrado el Assessment seleccionando las **6 preguntas más críticas y representativas por cada bloque** de la metodología SOLVAN, descartando las redundantes para agilizar la evaluación.

Mantenemos la escala de valoración de **0 a 3 puntos** para tener certeza absoluta en el nivel de riesgo: **0 (Riesgo no controlado)**, **1 (Informal/Parcial)**, **2 (Con brechas)** y **3 (Maduro y probado)**.

Aquí tienes el cuestionario definitivo, perfectamente equilibrado con 42 preguntas en total:

BLOQUE 1 — Continuidad Operativa

1. ¿Tienen tiempos objetivos de recuperación (RTO y RPO) formalmente definidos por aplicación crítica?

- a) No existen RTO/RPO definidos ni documentados. *(0)*
- b) Están definidos de forma muy informal o como un estimado empírico. *(1)*
- c) Están documentados, pero la última caída superó el tiempo estimado. *(2)*
- d) Completamente documentados, probados y acordados formalmente con el negocio. *(3)*

2. ¿Cuál sería el impacto operativo si una aplicación crítica deja de funcionar?

- a) Pérdidas severas no cuantificadas y paro total inmediato. *(0)*
- b) Alto impacto, pero solo está estimado de manera informal. *(1)*
- c) Impacto medio, calculado y con tiempos de tolerancia definidos. *(2)*
- d) Impacto mínimo, la redundancia evita cualquier afectación visible. *(3)*

3. ¿Actualmente cuentan con redundancia, alta disponibilidad y un DR site (sitio alterno)?

- a) No, dependemos de un solo sitio con equipos vulnerables. *(0)*
- b) Redundancia parcial, pero sin replicación a un sitio alterno funcional. *(1)*
- c) Alta disponibilidad en el sitio principal, pero el sitio alterno no está sincronizado. *(2)*
- d) Alta disponibilidad completa (activo-activo) o replicación continua a nube/DR site. *(3)*

4. ¿Tienen identificados los puntos únicos de falla (SPOF) en su infraestructura?

- a) No hay un mapeo de infraestructura para identificar puntos de falla. *(0)*
- b) Se conocen algunos puntos informalmente, pero no están documentados. *(1)*
- c) Sí, están identificados y documentados, pero aún no mitigados. *(2)*
- d) Completamente identificados y mitigados mediante arquitecturas resilientes. *(3)*

5. ¿Cómo aseguran la continuidad del negocio ante incidentes mayores?

- a) Improvisamos según surja el problema, no hay plan formal. *(0)*
- b) Existe un plan de continuidad básico, pero es informal o muy antiguo. *(1)*
- c) Tenemos un DRP documentado, pero no se le realizan pruebas recientes. *(2)*
- d) Contamos con un plan (DRP/BCP) robusto y probado periódicamente. *(3)*

6. ¿Tienen procesos que operen 24/7 y que requieran infraestructura continua?

- a) Sí, operan 24/7 pero sin soporte ni redundancia para esos horarios. *(0)*
- b) Operan continuo, pero con TI limitada fuera del horario de oficina. *(1)*
- c) Solo operan en horarios comerciales, pero los sistemas deben estar en línea. *(2)*
- d) Sí, respaldados por alta disponibilidad total y soporte 24/7 formal. *(3)*

BLOQUE 2 — Infraestructura y Almacenamiento

7. ¿Tienen infraestructura próxima a su fin de vida útil (EOSL) o sin soporte?

- a) Sí, gran parte del almacenamiento o *core* está en EOSL y sin cobertura. *(0)*
- b) Varios equipos caducan pronto y no hay presupuesto aprobado de reemplazo. *(1)*
- c) Hay equipos *legacy* identificados, pero ya existe un plan de reemplazo en marcha. *(2)*
- d) Toda la infraestructura es vigente, moderna y con contratos de soporte activo. *(3)*

8. ¿Han tenido problemas de capacidad, rendimiento o saturación?

- a) Frecuentemente, con quejas graves que afectan la facturación u operación. *(0)*
- b) En ocasiones, especialmente en picos de demanda como cierres mensuales. *(1)*
- c) Rara vez, pero la ocupación de discos está por encima del 80-85%. *(2)*
- d) Nunca, la capacidad y el rendimiento fluyen holgadamente. *(3)*

9. ¿Conocen el rendimiento real de sus cargas críticas (IOPS y latencia)?

- a) No medimos IOPS ni latencia, solo evaluamos la capacidad por TB. *(0)*
- b) Medición reactiva: solo revisamos cuando hay lentitud notable. *(1)*
- c) Hay medición periódica, pero persisten cuellos de botella no resueltos. *(2)*
- d) Monitoreo continuo; la arquitectura All-Flash/NVMe está optimizada. *(3)*

10. ¿Cómo administran actualmente el crecimiento de almacenamiento?

- a) Totalmente reactivo, compramos discos solo cuando el sistema se llena. *(0)*
- b) Monitoreo informal basado en la intuición operativa. *(1)*
- c) Proyecciones de capacidad manuales de forma anual. *(2)*
- d) Gestión proactiva, automatizada y predictiva. *(3)*

11. ¿Qué porcentaje de almacenamiento tienen en una estrategia híbrida/multinube?

- a) 100% *on-premise* aislado y creando silos de información. *(0)*

- b) Mayormente local con iniciativas aisladas ("Shadow IT") en la nube. *(1)*
- c) Híbrido, operando en ambas partes pero con gestión separada. *(2)*
- d) Arquitectura híbrida optimizada, con portabilidad y visibilidad unificada. *(3)*

12. ¿Han realizado migraciones o consolidaciones de almacenamiento recientemente?

- a) No, la plataforma es muy antigua y existe temor a migraciones críticas. *(0)*
- b) Sí, pero fueron complejas y provocaron caídas de servicios. *(1)*
- c) Sí, con interrupciones menores pero requirieron ventanas de mantenimiento largas. *(2)*
- d) Migraciones transparentes y automatizadas sin ninguna afectación al usuario. *(3)*

BLOQUE 3 — Respaldo y Recuperación

13. ¿Aplican la regla 3-2-1 para sus respaldos (3 copias, 2 medios, 1 fuera de sitio)?

- a) No, guardamos los respaldos en el mismo sitio físico que la producción. *(0)*
- b) Parcialmente, enviamos cintas a otra sucursal, pero no es un sitio seguro. *(1)*
- c) Cumplimos la regla, pero las copias de red siguen siendo alterables. *(2)*
- d) Cumplimiento estricto de la regla 3-2-1 con ubicaciones remotas/nube seguras. *(3)*

14. ¿Cuentan con copias inmutables (WORM) o entornos *air-gapped* contra ransomware?

- a) No tenemos protección inmutable ni entornos aislados. *(0)*
- b) Confiamos únicamente en el antivirus corporativo general. *(1)*
- c) Separación lógica básica por red (VLANs), pero aún vulnerables a cifrados. *(2)*
- d) Almacenamiento inmutable implementado; los datos no pueden borrarse ni alterarse. *(3)*

15. ¿Cuándo fue la última prueba de restauración completa y cuál fue el resultado?

- a) Nunca, o hace más de 18 meses que no probamos una restauración total. *(0)*
- b) Solo hacemos pruebas aisladas restaurando archivos sueltos. *(1)*
- c) Se probó en el último año, pero tomó mucho tiempo o hubo errores menores. *(2)*
- d) Pruebas completas y periódicas con éxito validado frente al RTO. *(3)*

16. ¿Qué tan rápido podrían restaurar la operación desde un respaldo?

- a) Podría tomar semanas o podríamos no recuperarnos al 100%. *(0)*
- b) Entre 3 y 7 días, asumiendo que los respaldos no estén corruptos. *(1)*
- c) En menos de 24 horas. *(2)*
- d) En cuestión de horas o minutos de forma automatizada. *(3)*

17. ¿Cómo gestionan las credenciales de la consola de respaldo?

- a) Se utiliza la misma contraseña de administrador general para todo. *(0)*
- b) La consola de respaldo está vinculada al Active Directory de producción. *(1)*
- c) Cuentas separadas, pero no exigen Segundo Factor de Autenticación (MFA). *(2)*
- d) Credenciales totalmente independientes de producción y protegidas con MFA. *(3)*

18. ¿Existen políticas documentadas de retención y recuperación de datos?

- a) No existen políticas. *(0)*
- b) Retención "de facto" empírica ("lo que quepa en el disco"). *(1)*
- c) Políticas documentadas, pero a veces incumplidas por falta de capacidad. *(2)*
- d) Políticas oficiales alineadas al negocio, cumplidas al 100% y auditadas. *(3)*

BLOQUE 4 — Ciberseguridad

19. ¿Cuentan con monitoreo activo de amenazas de seguridad 24/7?

- a) No tenemos ningún tipo de monitoreo de seguridad. *(0)*
- b) Revisión manual reactiva en horario de oficina. *(1)*
- c) Contamos con herramientas pero sin personal asignado para respuestas nocturnas. *(2)*
- d) Servicio MDR o SOC activo gestionando alertas y respuestas 24/7/365. *(3)*

20. ¿Tienen un plan de respuesta a incidentes cibernéticos documentado?

- a) No existe ningún plan de contención o respuesta. *(0)*
- b) Es un borrador informal, sin roles definidos. *(1)*
- c) Está documentado, pero nunca hemos hecho simulacros. *(2)*
- d) Plan oficial, con roles claros, automatización de contención y simulacros regulares. *(3)*

21. ¿Qué controles tienen para prevenir fuga de información (DLP) y uso de USBs/Nube?

- a) Ningún control técnico; todo está abierto. *(0)*
- b) Políticas de confianza firmadas en papel y bloqueo manual muy rudimentario. *(1)*
- c) Restricciones vía Active Directory o controles de red básicos. *(2)*
- d) Plataforma DLP madura que controla endpoints, nube y correos salientes. *(3)*

22. ¿Cómo gestionan los accesos y las credenciales privilegiadas (PAM)?

- a) Cuentas de administrador compartidas entre varios miembros de TI. *(0)*
- b) Cuentas nominales, pero sin Segundo Factor de Autenticación (MFA). *(1)*
- c) MFA habilitado, pero sin una bóveda o solución PAM para auditar accesos críticos. *(2)*
- d) Solución PAM centralizada con gestión del ciclo de vida y MFA en toda la red. *(3)*

23. ¿Realizan evaluaciones de vulnerabilidades y pruebas de penetración (pentesting)?

- a) Nunca se han ejecutado estas evaluaciones. *(0)*
- b) Solo se realizan de forma reactiva tras sufrir un incidente. *(1)*
- c) Escaneo básico o pentesting anual para cumplir auditorías, con hallazgos rezagados. *(2)*
- d) Evaluaciones periódicas, pentesting regular y remediación de vulnerabilidades inmediata. *(3)*

24. ¿Qué nivel de visibilidad tienen sobre el comportamiento anómalo de usuarios?

- a) Nula, la red interna es una caja negra. *(0)*
- b) Muy baja, solo vemos a qué hora inician sesión en el sistema. *(1)*
- c) Tenemos *logs* almacenados, pero no se correlacionan ni generan alertas proactivas. *(2)*
- d) Alta visibilidad mediante herramientas (ej. UEBA) que alertan comportamientos sospechosos. *(3)*

BLOQUE 5 — Aplicaciones y Networking

25. ¿Tienen aplicaciones críticas expuestas a internet (ej. e-commerce)?

- a) Sí, están expuestas directamente sin filtros especiales. *(0)*
- b) Sí, protegidas solo por el *router* del proveedor o controles básicos. *(1)*
- c) Sí, resguardadas únicamente detrás de un *firewall* perimetral tradicional. *(2)*
- d) Sí, protegidas detrás de múltiples capas de seguridad especializadas. *(3)*

26. ¿Cómo protegen específicamente la capa web y las APIs críticas?

- a) No hay protección en la capa aplicativa. *(0)*
- b) Reglas manuales en balanceadores básicos. *(1)*
- c) Uso de módulos IPS en el firewall o un WAF solo en la app más crítica. *(2)*
- d) Soluciones avanzadas (ADC / WAF dedicado) y protección especializada de APIs. *(3)*

27. ¿Han experimentado caídas o degradación de servicio en sus aplicaciones?

- a) Quejas constantes de lentitud o caídas que afectan al usuario o las ventas. *(0)*
- b) Ocasionalmente, durante eventos de alta concurrencia o tráfico masivo. *(1)*
- c) Rara vez, usualmente se estabilizan con reinicios rápidos de servidores. *(2)*
- d) Nunca, mantenemos una disponibilidad del 99.99% sin afectaciones. *(3)*

28. ¿Tienen visibilidad de dependencias entre sus aplicaciones y la infraestructura?

- a) No hay mapa de dependencias, desconocemos el impacto cruzado de una falla. *(0)*
- b) Se conoce informalmente por la memoria de algunos ingenieros. *(1)*
- c) Documentación técnica existente, pero suele desactualizarse rápido. *(2)*
- d) Mapeo exacto, automatizado y actualizado en tiempo real. *(3)*

29. ¿Cómo monitorean el tráfico, la disponibilidad y la experiencia de usuario?

- a) No se monitorea de manera sistemática. *(0)*
- b) Revisiones visuales o *pings* manuales a los servidores. *(1)*
- c) Herramientas reactivas corporativas (NMS) que detectan caídas, no lentitud. *(2)*
- d) Uso de APM (Application Performance Monitoring) para asegurar una experiencia ininterrumpida. *(3)*

30. ¿Gestionan certificados TLS/SSL de forma centralizada?

- a) No, han ocurrido caídas de aplicaciones porque los certificados caducan sin previo aviso. *(0)*
- b) Se llevan en una hoja de cálculo manual y propensa a errores. *(1)*
- c) Renovación automática solo en aplicaciones externas; los internos son manuales. *(2)*
- d) Gestión 100% automatizada y centralizada de todos los certificados. *(3)*

BLOQUE 6 — Operación y Soporte

31. ¿Cómo gestionan la resolución de incidentes operativos diariamente?

- a) A través de pasillos, llamadas personales o WhatsApp ("Bomberazos"). *(0)*
- b) Tienen un *ticket* rudimentario pero sin orden de prioridad. *(1)*
- c) Mesa de ayuda estructurada pero reactiva, sin alineación a mejores prácticas. *(2)*
- d) Herramienta ITSM robusta totalmente alineada a procesos ITIL. *(3)*

32. ¿Los contratos de soporte cubren toda su infraestructura productiva (hardware/software)?

- a) No, varios componentes vitales operan sin contrato de soporte. *(0)*
- b) Cobertura intermitente o "según el equipo"; se escala por garantía básica. *(1)*
- c) Cobertura oficial, pero el soporte de terceros es lento. *(2)*
- d) Todo el entorno productivo tiene pólizas activas con resolución ágil garantizada. *(3)*

33. ¿Cuentan con soporte 7x24 oficial y estructurado?

- a) No existe soporte formal fuera del horario de oficina. *(0)*
- b) Esquema de "guardias" internas muy informales. *(1)*
- c) Soporte 24/7 externalizado pero solo para ciertas piezas de hardware clave. *(2)*
- d) Servicios administrados integrales 24/7/365 para la infraestructura completa. *(3)*

34. ¿Existen tiempos de respuesta definidos (SLAs) entre TI y el negocio?

- a) Ninguno, se resuelve según haya personal disponible. *(0)*
- b) Son acuerdos informales de "Mejor Esfuerzo". *(1)*
- c) Existen SLAs hacia los fabricantes, pero no están documentados internamente hacia el negocio. *(2)*
- d) SLAs estrictos, documentados, medidos y penalizados por incumplimiento. *(3)*

35. ¿La operación depende excesivamente de personas clave (Bus factor)?

- a) Totalmente; si 1 o 2 personas clave faltan, la operación corre peligro. *(0)*
- b) Alta dependencia en la memoria institucional, hay muy escasa documentación técnica. *(1)*
- c) Existen diagramas y manuales, pero están algo desactualizados. *(2)*
- d) Operación estandarizada mediante *runbooks* y automatización, sin dependencia personal crítica. *(3)*

36. ¿Tienen visibilidad ejecutiva del estado general de su infraestructura?

- a) Ninguna, para la dirección la TI sigue siendo una caja negra. *(0)*
- b) Generación manual de reportes en hojas de cálculo que suelen atrasarse. *(1)*
- c) Tableros técnicos detallados, pero poco legibles para la alta gerencia. *(2)*
- d) *Dashboards* ejecutivos consolidados, métricas de negocio y visibilidad en tiempo real. *(3)*

BLOQUE 7 — Estrategia Tecnológica

37. ¿Cuáles son las prioridades tecnológicas de este año?

- a) Sobrevivir operativamente y "apagar incendios" diarios con la infraestructura actual. *(0)*
- b) Cubrir huecos de seguridad tras incidentes recientes o sustos. *(1)*
- c) Ejecutar migraciones forzosas o renovar plataformas *legacy*. *(2)*
- d) Innovar en transformación digital, analítica, e inteligencia automatizada. *(3)*

38. ¿Qué retos tecnológicos preocupan más actualmente a la mesa directiva?

- a) Riesgos inminentes de caídas severas, paros en ventas y daños por *ransomware*. *(0)*
- b) La lentitud del departamento de TI para atender nuevas necesidades del negocio. *(1)*
- c) Incumplimientos de normativas de auditoría o de protección de datos (ej. PCI/Datos Personales). *(2)*

- d) Mejorar el *Time-to-Market* y habilitar nuevos negocios, el riesgo está mitigado. *(3)*

39. ¿Qué áreas de su infraestructura actual consideran más vulnerables?

- a) Todo el Core productivo (Redes principales, Servidores, Almacenamiento antiguo). *(0)*
- b) Las estrategias de Ciberseguridad y Recuperación ante desastres (Respaldos). *(1)*
- c) Ciertas aplicaciones secundarias o sucursales remotas. *(2)*
- d) Ninguna área se considera vulnerable de forma crítica. *(3)*

40. ¿Qué iniciativas críticas tienen detenidas actualmente y por qué?

- a) Proyectos de Seguridad o Continuidad (DRP) por falta total de presupuesto. *(0)*
- b) Proyectos de mitigación detenidos por falta de un caso de negocio que justifique la inversión. *(1)*
- c) Proyectos de modernización retrasados por miedo a la complejidad técnica o falta de tiempo operativo. *(2)*
- d) Ninguna, las planificaciones avanzan acorde al cronograma anual. *(3)*

41. ¿Existe presupuesto asignado y una ventana de decisión clara para mitigar sus riesgos actuales?

- a) No hay presupuesto ni panorama a corto o mediano plazo. *(0)*
- b) Se reconoce el problema, pero el presupuesto está completamente bloqueado. *(1)*
- c) Presupuesto tentativo o en exploración para el próximo ejercicio fiscal. *(2)*
- d) Hay presupuesto autorizado para ejecutar soluciones en un plazo de 0 a 6 meses. *(3)*

42. ¿Qué mejorarían primero si tuvieran recursos inmediatos ilimitados?

- a) Renovación urgente de equipos obsoletos a punto de colapsar. *(0)*
- b) Establecer un perímetro de ciberseguridad moderno y respaldos confiables inmutables. *(1)*

- c) Herramientas centralizadas de monitoreo u orquestación híbrida. *(2)*
- d) Iniciativas completamente enfocadas a optimizar la experiencia de usuario o la automatización. *(3)*

Cálculo Final (126 Puntos Máximos): Para presentar los resultados en la metodología SOLVAN, debes sumar todos los puntos que alcance el cliente y dividirlos entre 126. Al multiplicar el resultado por 100, obtendrás el **Índice SOLVAN global**. Con 6 preguntas por bloque, cada área de TI pesará exactamente lo mismo en tu calificación final.