Gestión de Disponibilidad y Continuidad

1. Disponibilidad

1.1 ¿Se monitorean los eventos generados por los activos y/o servicios tecnológicos?

- Tener en cuenta los servicios principales, o servicios críticos para la operación del negocio; Preferiblemente contar con una herramienta o software que permita tal monitoreo

1.2 ¿Se cuenta con un plan de Alta disponibilidad para los servicios tecnológicos que se ajuste a los objetivos y prioridades del negocio?

- ¿La operación conoce el plan de alta disponibilidad?, ¿La operación conoce cuáles son los objetivos y prioridades del negocio?. Si no existe un plan formal, ¿cómo responde la operación frente a la caída de un servicio?: ¿se cuenta con un canal de respaldo?, ¿se realiza backup a los servidores?, ¿Los servidores de respaldo suben automáticamente?

1.3 ¿Frecuentemente se realizan pruebas de los planes de Alta disponibilidad como medida proactiva frente a fallas críticas de los servicios tecnológicos?

- ¿Cada cuánto se realizan las pruebas del plan de disponibilidad?, ¿Se planifican las pruebas?, ¿Quién las hace?, ¿Qué documentación se deja como evidencia de las pruebas del plan de disponibilidad?

1.4 ¿El personal de tecnología tiene conocimiento del plan de Alta disponibilidad y cómo ponerlo en marcha cuando es requerido?

- Revisar si existe un procedimiento documentado, contacto con proveedores,

1.5 ¿Se realiza la supervisión de los planes de Alta disponibilidad teniendo en cuenta los objetivos y prioridades del negocio?

- Verificar la existencia de evidencia sobre alguna reunión o revisión de los planes de alta disponibilidad, en la que se demuestre que la alta gerencia está involucrada. Tener en cuenta la alineación con lo que espera el negocio de acuerdo a la estrategia

1.6 ¿Frecuentemente se toman decisiones o acciones correctivas sobre los planes de Alta disponibilidad de los servicios tecnológicos teniendo como base los resultados del monitoreo de la disponibilidad?

- Tomando como base el monitoreo de la disponibilidad y el plan de disponibilidad, ¿Hay evidencia de las decisiones tomadas?, ¿Se siguen procedimientos para la toma de decisiones?¿Se cuenta con un plan de mejoras a la disponibilidad?

1.7 ¿Existe recopilación de datos necesarios para medir la disponibilidad?

- ¿Se cuenta con indicadores?¿Se realiza seguimiento, análisis y reporte de la disponibilidad de sus servicios y/o componentes?

2. Continuidad

2.1 ¿Se identifican y gestionan los incidentes que generan la NO continuidad de los servicios tecnológicos?

- Tener en cuenta la herramienta de gestión de incidentes para filtrar los incidentes relacionados con la falta de continuidad de los servicios tecnológicos
- Se debería asegurar la disponibilidad y rendimiento de los servicios en niveles suficientes en caso de desastre
- Se gestionan las dependencias de los servicios y se mantienen bajo medidas de control para prevenir la caída de los servicios

2.2 ¿Existe un procedimiento estandarizado para la ejecución, almacenamiento y prueba de las copias de seguridad (backups)?

- Indagar sobre el procedimiento establecido para la ejecución de backups. ¿El personal de la operación conoce y maneja claramente el procedimiento? Indicar qué incluye el procedimiento

2.3 Cuenta la organización con planes de contingencia y continuidad de negocio?

- Plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada

3. Riesgos

3.1 ¿Existen lineamientos ó guías claras para la gestión de riesgos de T.I?

- Indagar sobre la documentación existente sobre cómo funciona la gestión de riesgos de T.I., políticas, partes involucradas, información requerida, herramienta o software autorizado, métricas, cultura de gestión de riesgos, frecuencia de las actividades de gestión de riesgo. Verificar si estas guías cumplen un ciclo de identificación, análisis, evaluación, controles (tratamientos), monitoreo y revisión

3.2 ¿Se gestionan los riesgos asociados a los servicios tecnológicos?

- Verificar si existe evidencia de la gestión de riesgos del área de T.I. (evidencia sobre algun tipo de software o herramienta). Quién hace la identificación de riesgos, cómo lo hace, cada cuanto lo hace, como se analizan los riesgos, categorías de riesgo, respuesta a los riesgos, controles. Tener en cuenta los servicios tecnológicos principales o críticos para la operación del negocio. Verificar si existe evidencia sobre algun software o herramienta. Se debe encontrar principalmente información técnica de cada servicio, la gestión de riesgos debe tener un enfoque operacional y estratégico

---

Revision #1
Created 20 January 2021 22:34:22 by CertMind
Updated 21 January 2021 15:27:25 by CertMind