CONTINUIDAD DE LOS SERVICIOS

La **Gestión de la Continuidad de los Servicios de TI** (ITSCM sus siglas en inglés IT Service Continuity Management) es un esquema estructurado de toma de decisiones para situaciones en donde los servicios no se pueden suspender o para que la interrupción sea lo más breve posible. Las pruebas del plan preve la recuperación de los servicios. Por ello, se debe probar el plan por medio de pruebas y tenerlo documentado.

Los objetivos principales de la Continuidad de servicios se resumen en:

- Garantizar la pronta recuperación de los servicios críticos de TI tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las perniciosas consecuencias de un desastre o causa de fuerza mayor.

Es importante tomar en cuenta los desastres naturales como inundaciones y terremotos, los producidos por la infraestructura como los incendios, los accidentales provocados por el usuario como una configuración equivocada, un error en el mantenimiento y los desastres informáticos producidos por ataques de denegación de servicio (DDOS), virus informáticos, entre otros.

El responsable de la Continuidad de Servicios debe prever los riesgos asociados a los casos anteriores y restaurar el servicio de TI con prontitud.

Además, tiene una responsabilidad especial en los servicios que paralicen a toda la organización como son procesos vitales.

Los principales beneficios de una correcta **Gestión de la Continuidad del Servicio** se resumen en:

- Se gestionan adecuadamente los riesgos.
- Se reduce el periodo de interrupción del servicio por causas de fuerza mayor.
- Se mejora la confianza en la calidad del servicio entre clientes y usuarios.
- Sirve de apoyo al proceso de Gestión de la Continuidad del Negocio.

Las principales dificultades a la hora de implementar la Gestión de la Continuidad del Servicio se resumen en:

- Puede haber resistencia a realizar inversiones cuya rentabilidad no es inmediata.

- No se presupuestan correctamente los costos asociados.
- No se asignan los recursos suficientes.
- No existe el compromiso suficiente con el proceso dentro de la organización.
- Las tareas y actividades correspondientes se demoran perpetuamente para hacer frente a "actividades más urgentes".
- No se realiza un correcto análisis de riesgos y se obvian amenazas y vulnerabilidades reales.
- El personal no está familiarizado con las acciones y procedimientos a ejecutar en caso de interrupción grave de los servicios.

Todo plan de continuidad de negocio debe responder a las cinco grandes preguntas:

¿QUÉ?: Definir las partes de la organización que serán críticas en los primeros momentos y por tanto, que deberán volver a la normalidad lo antes posible.

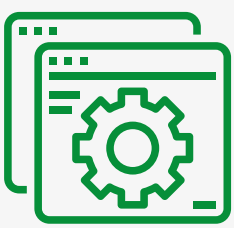
¿QUIÉN?: ¿Qué personas se tendrán que movilizar y en qué orden?. ¿Cuanta gente hará falta en las primeras horas, los primeros días? y sobre todo, cómo se comunicará el tema para que no se dé una situación caótica.

¿CUÁNDO?: ¿Qué ventanas de interrupción son tolerables? ¿En cuánto tiempo tenemos que volver a la normalidad? Todo esto viene definido por el Análisis de Impacto al Negocio (Businnes Impact Analysis - BIA) que establece los valores para los dos parámetros relevantes en continuidad de negocio, el RTO[1] y el RPO[2].

¿CÓMO?: ¿Qué tendrá que hacer para mitigar la contingencia, entrar en la fase de recuperación y por último, volver a la normalidad?.

¿DÓNDE?: ¿A cuáles lugares tendrá que acudir para poder hacer todo esto?. Si las ubicaciones físicas principales están afectadas, hay que tener lugares alternativos donde se pueda desplegar el plan. ¿Qué pasa si no tengo mi PC normal de trabajo o no se puede entrar al centro de datos?

1. Tiempo de recuperación(RTO)
2. Punto de recuperación (RPO)



central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de **Informática**