Informe de Ejercicios y Simulacros BCP/DRP

TechSys Solutions S.L.

Sede Barcelona

Aclaración:
Actualmente no hay constancia de la realización de simulacros en la empresa. Este documento es una guía sobre cómo se deberían gestionar este tipo de actividades. A lo largo de este documento se detallan varios ejemplos.

1. Introducción

Este informe documenta los resultados de los ejercicios y simulacros de los Planes de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP) realizados durante el ciclo anual 2024-2025. Estos simulacros tienen como objetivo evaluar la eficacia de los mecanismos de respuesta de TechSys Solutions S.L. ante incidentes críticos que puedan afectar la operatividad de sus procesos clave.

2. Objetivo del informe

- Verificar la eficacia del BCP/DRP.
- Identificar desviaciones, cuellos de botella y áreas de mejora.
- Proponer acciones correctivas y preventivas.

3. Escenarios simulados

Los escenarios fueron definidos en base al Análisis de Impacto del Negocio (BIA) y al árbol de dependencia de activos. Se seleccionaron los siguientes:

1. **Corte total de conectividad en sede central.**
2. **Infección por ransomware en entorno de desarrollo.**
3. **Caída de servicios cloud críticos (repositorio de código y CRM).**
4. **Pérdida total de datos en el servidor de correo.**

4. Resultados de los simulacros

4.1 Corte total de conectividad en sede central

- **RTO estimado:** 3 horas
- **RTO real:** 2 horas 40 minutos

- **Observaciones:** Se activó VPN y operación en remoto según lo previsto. Buen cumplimiento del protocolo.

4.2 Ransomware en entorno de desarrollo

- **RTO estimado:** 6 horas
- **RTO real:** 9 horas
- **Observaciones:** Se detectó lentitud en el acceso a respaldos por falta de pruebas recientes. Se restauró desde backup diario.

4.3 Caída de servicios cloud

- **RTO estimado:** 4 horas
- **RTO real:** 4 horas 20 minutos
- **Observaciones:** Buena comunicación con proveedor cloud, pero falta de procedimiento de escalado interno ralentizó la acción inicial.

4.4 Pérdida de datos en servidor de correo

- **RPO estimado:** 1 hora
- **RPO real:** 30 minutos
- **Observaciones:** Excelente gestión gracias a replicación continua. El área de soporte demostró competencia técnica.

5. Evaluación general

- **Participación:** Todos los responsables de área participaron.
- **Disponibilidad de manuales de acción:** 100%
- **Documentación de incidentes:** Completa y firmada.
- **Revisión posterior:** Realizada por el Comité de Seguridad.

6. Recomendaciones de mejora

- Realizar pruebas de restauración de respaldos cada 3 meses.
- Establecer procedimientos de escalado con todos los proveedores críticos.
- Documentar escenarios específicos de ataque con malware en cloud.
- Mejorar la formación del personal en tiempos de respuesta.

7. Cierre del ciclo anual

Este informe queda archivado como evidencia de cumplimiento y mejora continua en el marco del SGSI de TechSys Solutions S.L.
Su contenido servirá de referencia para la revisión de los planes BCP/DRP del siguiente ciclo.
