

laSalle

UNIVERSIDAD RAMON LLULL

Curs d'Implantació i Gestió de la Seguretat

Módulo 4

Herramientas de Gestión de Procesos de
Recuperación

Profesor: Alex Collado

Alumno: Julián Gordon

Indice

Ejercicio: Herramientas de Gestión de Procesos de Recuperación.....	3
Objetivo.....	3
Aspectos Básicos / Escenario.....	3
Instrucciones.....	3
Introducción.....	4
Empresa Ficticia: InnovateTech Solutions.....	5
Conclusión.....	9

Curs d'Implantació i Gestió de la Seguretat

Ejercicio: Herramientas de Gestión de Procesos de Recuperación

Objetivo

Analizar nuestros procesos/servicios y garantizar su recuperación en caso de un incidente. Además, analizar herramientas de control remoto, elegir una y justificar por qué.

Aspectos Básicos / Escenario

Dado que las empresas sufren cada vez más ataques, es imprescindible para la continuidad y viabilidad del negocio tener un buen plan de recuperación ante un incidente.

Instrucciones

Se debe elegir un proceso o servicio de la empresa (o puede ser ficticio), definir su criticidad, realizar un análisis de riesgos, un plan de continuidad de negocio, planteamiento según RTO y RPO, con la definición del respaldo y las necesidades que pueda tener este servicio o proceso. Es importante definir el alcance, es decir, cuál es el proceso o activo crítico elegido, sus características para luego definir el análisis de riesgo y el plan de continuidad de negocio de manera razonada. También se deberá elegir una herramienta de acceso, control y mantenimiento remoto de activos y justificar el motivo de esta herramienta de manera razonada.

Introducción

En un entorno empresarial caracterizado por amenazas cibernéticas sofisticadas y la creciente frecuencia de desastres naturales, la implementación de un plan integral de recuperación ante incidentes se convierte en un imperativo para asegurar la continuidad operativa y la protección de los activos críticos de una organización. Este documento aborda en profundidad el servicio de gestión de bases de datos de InnovateTech Solutions, una empresa ficticia líder en soluciones tecnológicas, analiza rigurosamente los riesgos asociados, y presenta un plan detallado de continuidad de negocio. Además, se selecciona y justifica exhaustivamente la herramienta de control remoto TeamViewer para asegurar la operatividad continua del servicio durante emergencias.

Empresa Ficticia: InnovateTech Solutions

Descripción de la Empresa: InnovateTech Solutions se estableció en 2005 como una empresa pionera en el desarrollo de software empresarial y soluciones tecnológicas personalizadas. Con sede principal en Nueva York y centros de desarrollo en Bangalore y Berlín, InnovateTech emplea a 250 profesionales altamente calificados. La compañía se especializa en la creación de plataformas de gestión de datos, aplicaciones móviles y software empresarial para diversos sectores, incluyendo finanzas, salud y logística. Su éxito se fundamenta en la capacidad para innovar y adaptarse rápidamente a las demandas del mercado global.

Servicio Crítico Elegido: Servicio de Gestión de Bases de Datos

Definición y Criticidad: El servicio de gestión de bases de datos de InnovateTech es esencial para su funcionamiento diario y estratégico. Esta plataforma centralizada almacena y administra datos críticos de clientes, registros financieros, transacciones comerciales y otro tipo de información corporativa vital. La integridad y disponibilidad de estos datos son cruciales para la toma de decisiones estratégicas, la continuidad operativa y el cumplimiento normativo de la empresa.

Análisis de Riesgos

Amenazas Internas:

Amenaza	Descripción	Impacto	Probabilidad	Riesgo
Errores humanos	Borrado accidental de datos o configuraciones incorrectas	Un borrado podría resultar en pérdidas de datos significativas.	Moderada	Alto
Fallos de hardware	Fallos en discos duros, servidores	Si no se cuenta con redundancia de hardware, puede resultar en tiempos de inactividad prolongados.	Baja	Medio
Fallos de software	Errores en el sistema de gestión de bases de datos	Pueden conducir a la corrupción de datos o pérdida de funcionalidad crítica.	Moderada	Alto

Amenazas Externas:

Amenaza	Descripción	Impacto	Probabilidad	Riesgo
Ataques cibernéticos	Ransomware, SQL injection, intentos de intrusión	La pérdida o compromiso de datos confidenciales podría dañar la reputación y resultar en sanciones legales.	Alta	Muy alto
Desastres naturales	Inundaciones, incendios, terremotos	Podrían resultar en pérdida total de los centros de datos y equipos críticos.	Baja	Alto
Cortes de energía	Interrupciones prolongadas del suministro eléctrico	Si no se cuenta con generadores de respaldo, podría afectar la operación continua.	Moderada	Alto

Plan de Continuidad de Negocio

Objetivos de Recuperación

- **RTO (Recovery Time Objective):** 4 horas. El servicio de gestión de bases de datos debe estar restaurado dentro de un máximo de 4 horas desde el inicio del incidente para minimizar el impacto en las operaciones.
- **RPO (Recovery Point Objective):** 15 minutos. Se permitirá una pérdida de datos mínima, asegurando que no se pierda más de 15 minutos de información registrada.

Medidas de Recuperación

- **Backup:** Se realizan copias de seguridad incrementales cada 15 minutos y copias completas diarias de las bases de datos. Estas copias se almacenarán en un centro de datos secundario ubicado en una región geográficamente separada para mitigar riesgos relacionados con desastres naturales y ataques físicos.
- **Replicación:** Implementación de replicación en tiempo real hacia un servidor de respaldo ubicado en otra ubicación geográfica para garantizar la disponibilidad continua de datos.
- **Plan de Respuesta a Incidentes:** Establecimiento de un equipo de respuesta a incidentes con roles y responsabilidades claramente definidos. Se llevarán a cabo simulacros periódicos para mantener la preparación y mejorar los tiempos de respuesta ante incidentes.

Herramienta de Control Remoto Elegida: TeamViewer

TeamViewer ha sido seleccionado como la herramienta óptima para acceso, control y mantenimiento remoto de activos debido a su robusta seguridad, facilidad de uso y amplia funcionalidad. A continuación, se detallan las razones:

- **Seguridad Avanzada:** Utiliza encriptación AES de 256 bits y autenticación de dos factores para asegurar conexiones seguras y proteger datos confidenciales durante las sesiones remotas.
- **Interfaz Intuitiva:** Su interfaz de usuario intuitiva permite tanto a técnicos como a usuarios no técnicos realizar conexiones rápidas y estables, lo cual es crucial durante situaciones de emergencia donde cada minuto cuenta.
- **Compatibilidad Universal:** Compatible con una amplia gama de sistemas operativos, incluyendo Windows, macOS, Linux, Android e iOS, garantizando acceso remoto a diferentes tipos de dispositivos y plataformas.
- **Funcionalidades Avanzadas:** Ofrece características como transferencia de archivos segura, reinicio remoto y soporte para múltiples monitores, mejorando

la eficiencia operativa y facilitando el mantenimiento proactivo de sistemas críticos.

Conclusión

La implementación de un plan de recuperación de alta calidad y la elección de herramientas adecuadas como TeamViewer son fundamentales para garantizar la continuidad operativa y la resiliencia empresarial frente a diversos tipos de amenazas. InnovateTech Solutions está preparada no solo para hacer frente a los desafíos actuales, sino también para adaptarse y prosperar en un entorno empresarial dinámico y cada vez más complejo.

Este documento exhaustivo asegura que InnovateTech esté equipada no solo para enfrentar desafíos inesperados, sino también para mantener altos estándares de seguridad y disponibilidad de datos, fortaleciendo así su posición como líder en innovación tecnológica a nivel global.