Plan de Recuperación ante Incidencias (DRP) - Servidor Web WordPress

Empresa: Innovatech Solutions EU

Sistema Cubierto: Servidor Debian (10.0.2.11) alojando Sitio Web WordPress Corporativo

Versión: 1.1

Fecha: 3 de Abril de 2025

Preparado por: Rodrigo Martinez Jefe de CiberCeguridad

1. Introducción y Propósito

Este documento establece el Plan de Recuperación ante Incidencias (DRP) para el servidor web corporativo principal de Innovatech Solutions EU, alojado en 10.0.2.11. Este servidor ejecuta un sitio WordPress que es fundamental para la presencia online, marketing y comunicación con clientes de la empresa. El propósito de este DRP es proporcionar un marco de actuación claro y detallado para restaurar el servicio web y minimizar la pérdida de datos de manera eficiente y predecible en caso de un evento disruptivo mayor (fallo crítico de hardware, desastre natural, corrupción de datos irrecuperable, ciberataque destructivo, etc.), asegurando así la continuidad del negocio y cumpliendo con las expectativas de servicio.

2. Alcance

Este DRP cubre específicamente la recuperación de los siguientes componentes críticos asociados al servidor 10.0.2.11 y su función como host del sitio web WordPress corporativo:

- **Infraestructura Base:** Configuración y estado operativo del Sistema Operativo Debian 12 (incluyendo el hardening de seguridad aplicado post-incidente).
- **Servicios de Red y Soporte:** Configuraciones y operatividad de Apache2 (servidor web), PHP (intérprete de lenguaje), MariaDB/MySQL (servidor de base de datos local), SSH (acceso administrativo seguro), UFW (firewall de host), Fail2ban (protección anti-fuerza bruta).
- **Aplicación WordPress:** La totalidad de los archivos que componen el sitio web, ubicados en /var/www/html/, incluyendo el núcleo de WordPress, temas, plugins, configuraciones (wp-config.php, .htaccess) y todo el contenido subido por los usuarios (directorio wp-content/uploads).
- **Base de Datos WordPress:** La base de datos completa denominada wordpress dentro del servidor MariaDB/MySQL local, que contiene todo el contenido dinámico del sitio (posts, páginas, usuarios, comentarios, configuraciones, etc.).

Fuera de Alcance: Este plan no cubre la recuperación de otros servidores o servicios de Innovatech Solutions EU, ni la respuesta inicial a incidentes de seguridad (cubierta en el Informe de Incidente IS-20250403-001).

---

3. Objetivos de Recuperación (RTO y RPO)

Para el servicio web WordPress corporativo, se establecen los siguientes objetivos:

- **Objetivo de Tiempo de Recuperación (RTO):** El tiempo máximo aceptable desde la declaración del desastre hasta que el sitio web WordPress esté completamente funcional y accesible para los usuarios es de **4 horas**. Este RTO corto refleja la importancia del sitio para las operaciones diarias y la imagen de la empresa.
- **Objetivo de Punto de Recuperación (RPO):** La pérdida máxima de datos aceptable (medida en tiempo desde el último backup válido) es de **1 hora**. Esto implica que, en el peor de los casos, se podría perder hasta 1 hora de contenido o cambios realizados en el sitio web. Este RPO requiere una estrategia de backup frecuente para la base de datos.

4. Equipo de Recuperación y Responsabilidades

La ejecución exitosa de este plan depende de la coordinación del siguiente equipo:

Rol	Nombre	Responsabilidades Clave Durante la Recuperación
Coordinador DRP	Ana García	Activar el plan, supervisar progreso, tomar decisiones críticas, gestionar comunicaciones internas/externas.
Admin. de Sistemas	Carlos Pérez	Provisionar/restaurar infraestructura (VM/servidor), restaurar SO base y configuraciones de servicios (Apache, PHP, SSH, UFW, Fail2ban), asegurar conectividad de red del servidor.
Admin. de Base Datos	Sofía Moreno	Validar integridad del último backup de BD, restaurar la base de datos MariaDB/MySQL, verificar consistencia post-restauración.
Admin. Aplicación Web	David Ruiz	Restaurar archivos WordPress desde backup, verificar la integridad de temas/plugins, realizar pruebas funcionales completas del sitio web.
Equipo de Redes	Infraestructura TI	Asegurar la conectividad de red general, realizar ajustes de DNS necesarios si la IP pública cambia, monitorizar tráfico de red post-recuperación.

5. Estrategia de Copias de Seguridad (Backups)

La estrategia de backup es el pilar de este DRP y debe ser rigurosamente implementada y verificada.

- **Componentes a Respaldar y Justificación:**
    - **Base de Datos** wordpress**:** Contiene todo el contenido dinámico; su pérdida es crítica. Se respalda para cumplir el RPO.
    - **Archivos** /var/www/html/**:** Contiene el código de la aplicación, temas, plugins y medios subidos; esencial para la funcionalidad y apariencia del sitio.
    - **Configuraciones del Servidor:** (/etc/apache2/, /etc/mysql/, /etc/php/, /etc/ssh/sshd_config, /etc/ufw/, /etc/fail2ban/, crontab, lista de paquetes dpkg --get-selections): Necesarias para reconstruir rápidamente el entorno operativo endurecido en un nuevo servidor.
    - **(Recomendado) Imagen/Snapshot de la VM Base:** Una imagen completa del sistema operativo Debian ya instalado, actualizado y endurecido (sin datos de aplicación) acelera significativamente la restauración del entorno base.
- **Frecuencia (Mínima):**
    - **Base de Datos: Cada hora** (para cumplir RPO de 1 hora).
    - **Archivos WordPress: Diariamente** (ej. durante la noche).
    - **Configuraciones/Imagen Sistema: Semanalmente** y después de cada cambio de configuración relevante.
- **Método y Automatización:**
    - **Base de Datos:** Script automatizado (ej. en Bash) usando mysqldump con credenciales dedicadas de backup (solo permisos SELECT, LOCK TABLES), comprimido con gzip, y ejecutado vía cron cada hora. El nombre de archivo debe incluir timestamp preciso.
    - **Archivos WordPress:** Script automatizado usando tar con compresión gzip para crear un archivo único del directorio /var/www/html/, ejecutado vía cron diariamente. Alternativamente, rsync a un destino de backup si se prefiere sincronización incremental.
    - **Configuraciones:** Script que copie los directorios/archivos listados a un repositorio de backup versionado (idealmente Git privado) o los empaquete con tar.

    - **Imagen Sistema:** Funcionalidad de snapshots del hipervisor (VMware, VirtualBox, Proxmox) o herramientas de imagen de disco (Clonezilla) ejecutadas manualmente o programadas según la plataforma.

- **Almacenamiento y Seguridad:**
    - Los backups se generarán en un área de staging local (/mnt/backups_staging/ por ejemplo).
    - **Inmediatamente después**, se transferirán de forma **automatizada y cifrada** (ej. usando rsync sobre SSH, scp, o herramientas específicas de cloud) a **dos ubicaciones adicionales**:
        1. Un NAS seguro en una ubicación física diferente dentro de la empresa (On-site secundario).
        2. Un servicio de almacenamiento en la nube **seguro y externo** (Off-site, ej. AWS S3 Glacier/Standard, Google Cloud Storage Coldline/Standard, Azure Blob Storage Cool/Hot) en una región diferente.
    - Los backups almacenados off-site **deben estar cifrados en reposo** usando las capacidades del proveedor cloud o herramientas como gpg antes de la subida. El acceso a los buckets/contenedores de almacenamiento debe estar estrictamente controlado.
- **Retención:**
    - **Base de Datos (horarios):** Retener por 3 días.
    - **Archivos (diarios) / BD (fin de día):** Retener por 14 días.
    - **Semanales (Archivos+BD+Config):** Retener por 8 semanas.
    - **Mensuales (Archivos+BD+Config):** Retener por 12 meses.
    - **Anuales (Archivos+BD+Config):** Retener por 3-7 años (según requisitos legales/auditoría).
- **Verificación:**
    - **Automatizada:** Scripts de backup deben verificar códigos de salida y enviar notificaciones (email, Slack) en caso de éxito o fallo.
    - **Manual/Periódica:** Al menos **trimestralmente**, realizar una **restauración completa** de los backups (SO base, configuraciones, archivos, BD) en un **entorno de pruebas aislado** para verificar la

integridad de los datos y la viabilidad del proceso de recuperación. Documentar los resultados.

---

6. Procedimientos de Recuperación Detallados

1. **Evaluación Inicial y Activación (T0):**
    - El equipo técnico detecta/recibe notificación de fallo crítico del servidor 10.0.2.11.
    - Se realiza una evaluación rápida (ping, SSH, acceso web, consola de hipervisor si es VM) para confirmar inaccesibilidad/corrupción.
    - Se notifica al Coordinador DRP (Ana García).
    - **Decisión (Máx. 30 min desde detección):** Ana García evalúa la situación. Si la recuperación local rápida no es viable, declara formalmente el desastre y activa este DRP, convocando al Equipo de Recuperación. Se inicia la comunicación interna según plan de crisis.
2. **Preparación de Infraestructura de Reemplazo (T0 + 1 hora):**
    - Carlos Pérez (Admin. Sistemas) provisiona la infraestructura de reemplazo según el escenario:
        - Si es VM: Crear nueva VM con especificaciones (CPU, RAM, Disco) iguales o superiores en el hipervisor de contingencia.
        - Si es Cloud: Lanzar instancia predefinida (ej. Debian 12 en AWS EC2/GCP Compute Engine/Azure VM) con tipo y tamaño adecuados.
    - Configurar red básica (IP interna, acceso a internet).
3. **Restauración del Sistema Operativo y Hardening (T0 + 2 horas):**
    - **Opción Preferida:** Carlos Pérez restaura la última **imagen/snapshot válida** del SO Debian 12 base endurecido sobre la nueva infraestructura.
    - **Opción Alternativa:** Carlos Pérez realiza una instalación limpia de Debian 12. Aplica inmediatamente la configuración de red, instala paquetes esenciales (apache2, mariadb-server, php, libapache2-mod-php, ufw, fail2ban, rsync, gzip, etc.) y aplica **todas las configuraciones de hardening documentadas** (incluyendo usuarios, grupos, seguridad SSH, etc.).

- Se restaura la configuración de servicios clave (Apache, PHP, MySQL, SSH, UFW, Fail2ban) desde el último backup válido de configuraciones. Se verifican rutas y adaptan si es necesario.

4. **Restauración de la Base de Datos WordPress (T0 + 2.5 horas):**
    - Sofía Moreno (Admin. BD) obtiene acceso seguro al **último backup horario válido** de la BD (.sql.gz) desde el almacenamiento off-site o secundario.
    - Transfiere el backup al nuevo servidor.
    - Asegura que el servicio MariaDB/MySQL esté corriendo.
    - Crea la base de datos wordpress y el usuario wordpressuser con su contraseña segura y permisos correctos (si no se restauró desde imagen).
    - Importa la base de datos: gunzip < /ruta/backup/db/wordpress_AAAAMMDD_HHMMSS.sql.gz | mysql -u root wordpress
    - Verifica la importación (ej. SHOW TABLES;, SELECT count(*) FROM wp_posts;).
5. **Restauración de Archivos WordPress (T0 + 3 horas):**
    - David Ruiz (Admin. Web) obtiene acceso seguro al **último backup diario válido** de los archivos (.tar.gz o repositorio rsync).
    - Transfiere el backup al nuevo servidor.
    - Restaura los archivos en /var/www/html/, asegurando la estructura correcta (ej. sudo tar -xzf /ruta/backup/files/wordpress_AAAAMMDD.tar.gz -C / si el tar incluye la ruta completa, o -C /var/www/html si no).
    - **Verificación Crítica:** Aplica los permisos y propiedad correctos inmediatamente después de restaurar:

Bash

```
sudo find /var/www/html/ -type d -exec chmod 755 {} \;

sudo find /var/www/html/ -type f -exec chmod 644 {} \;

sudo chmod 600 /var/www/html/wp-config.php

sudo chown -R www-data:www-data /var/www/html/
```

6. **Configuración Final y Pruebas (T0 + 3.5 horas):**
    - Equipo de Redes verifica la configuración de red final. Configura UFW y Fail2ban (si no se restauró desde imagen/config). Habilita UFW (sudo ufw enable).
    - Reiniciar servicios clave: sudo systemctl restart apache2 mariadb fail2ban sshd.
    - David Ruiz y Carlos Pérez realizan pruebas funcionales:
        - Acceso al sitio vía HTTP y HTTPS (si aplica).
        - Navegación por páginas principales y posts.
        - Login de administrador (/wp-admin/).
        - Creación/edición de un post de prueba.
        - Funcionamiento de formularios de contacto (si aplica).
        - Verificación de carga de imágenes/medios.
    - Sofía Moreno verifica la conexión de la aplicación a la BD y la integridad de datos básicos.
    - Carlos Pérez verifica acceso SSH con clave y que el firewall/fail2ban estén activos (sudo ufw status, sudo fail2ban-client status sshd).
7. **Actualización DNS y Puesta en Producción (T0 + 4 horas - RTO):**
    - Si la IP pública ha cambiado, el Equipo de Redes actualiza los registros DNS para apuntar el dominio corporativo a la nueva IP.
    - Se realiza una monitorización intensiva inicial del rendimiento, logs y funcionalidad.
    - Ana García (Coordinador DRP) declara formalmente la finalización de la recuperación y comunica la restauración del servicio a las partes interesadas.

---

7. Mantenimiento y Pruebas del Plan

- **Revisión del Plan:** El DRP será revisado y actualizado por el Equipo de Seguridad y Operaciones TI cada **6 meses**, o antes si ocurren cambios significativos en la infraestructura, aplicaciones, estrategia de backup o personal clave.

- **Pruebas de Recuperación:** Se realizarán pruebas de restauración completas en un entorno aislado (sandbox) de forma **trimestral**. Estas pruebas verificarán la validez de los backups, la precisión de los procedimientos de restauración y el cumplimiento de los RTO/RPO definidos. Los resultados, problemas encontrados y lecciones aprendidas se documentarán y usarán para actualizar el plan.
- **Formación del Equipo:** El Equipo de Recuperación recibirá formación sobre este plan y sus roles específicos anualmente.

Este plan ahora incluye más detalles contextuales y procedimentales. Recuerda adaptarlo aún más a las herramientas y políticas específicas de "Innovatech Solutions EU".