



Biblioteca INFOTEC

Ciudad de México, a 10 de abril de 2025

## VISTO BUENO DE TRABAJO TERMINAL

Técnico Superior Universitario en Operación de Centro de Datos

### UNIDAD DE POSGRADOS PRESENTE

Por medio de la presente se hace constar que el **Reporte final** desarrollado por la alumna: **Laura Vertiz López** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que la alumna no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias  
Subgerente de Innovación Gubernamental

Jah

JAVG/jah

C.c.p. Mtra. Anely Mendoza Rosales. - Encargada de la Gerencia de Capital Humano. - Para su conocimiento.  
Laura Vertiz López. - Alumna Técnico Superior Universitario en Operación de Centro de Datos.- Para su conocimiento.



2025  
Año de  
La Mujer  
Indígena



## Reporte final

Datos eliminados: matrícula, correo, celular; con fundamento en lo establecido en los artículos 65, fracción II, 98, fracción III, 113, fracción I y último párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública, 44, fracción II, 106, fracción III y 116 de la Ley General de Transparencia y Acceso a la Información Pública, así como a lo establecido en los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, por tratarse de datos personales concernientes a una persona física identificada, en la modalidad de confidencial. Área Dirección Adjunta de Innovación y Conocimiento. Periodo indefinido, toda vez que no está sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma. Aprobada en la Primera Sesión Extraordinaria del Comité de Transparencia de INFOTEC ejercicio 2025.

## Índice

<b>Introducción</b> .....	3
<b>Práctica profesional</b> .....	4
<b>Estructura organizacional</b> .....	5
<b>Informe de la práctica profesional</b> .....	6
<b>Conclusiones</b> .....	8
<b>Cuadro CQA de mi estancia en la organización</b> .....	9
<b>Evaluación de desempeño</b> .....	10
<b>Referencias</b> .....	11



## Introducción

El presente documento es el reporte final de mi estancia profesional realizada en **Main Core S.A. de C.V.**, en el área de **Operación de Centros de Datos**. Este reporte tiene como objetivo documentar las actividades realizadas, describir las habilidades desarrolladas y evaluar mi desempeño profesional.

La práctica tuvo una duración de 260 horas y se enfocó en actividades como el diseño de un Plan de Recuperación ante Desastres (DRP), optimización de Procedimientos Operativos Estándar (SOP), mantenimiento preventivo y correctivo, y la implementación de controles de ciberseguridad.

El reporte incluye una descripción de la organización, las funciones asignadas, la bitácora de actividades semanales, y un análisis de cómo estas experiencias contribuyeron al desarrollo de habilidades técnicas y blandas, fundamentales para mi formación como Técnico Superior Universitario en Operación de Centros de Datos.

## Práctica profesional

Datos personales del estudiante			
Nombre completo:	Laura Vertiz López		
Matrícula:	Eliminado	Teléfono:	
Correo:	Eliminado		
Especialidad de TSU:	Operación de Centro de Datos		
Año:	2024	Celular:	Eliminado
Número de horas de práctica profesional:	260 horas		

Datos de la institución	
Nombre de la institución:	Main Core S.A. de C.V.
Departamento en el que realizarás tus prácticas:	Dirección de Operaciones
Nombre de la persona responsable del departamento:	Adrián Medina Hernández

# Estructura organizacional

- El sector de actividad

**Main Core S.A. de C.V.** es una empresa orientada a brindar soluciones tecnológicas integrales, con especialización en la operación de centros de datos, ciberseguridad y la implementación de infraestructura tecnológica. La organización se caracteriza por su capacidad para responder a las necesidades cambiantes del mercado y por su compromiso con la calidad en sus proyectos.

- Presentación de la empresa e historia de la empresa

**Main Core S.A. de C.V.** tiene como misión implementar soluciones tecnológicas que maximicen los resultados de sus clientes mediante el uso óptimo de recursos y estrategias innovadoras.

Su visión es posicionarse como líder global en innovación tecnológica, destacándose por sus altos estándares de seguridad y su enfoque en la sostenibilidad.

Desde su fundación, **Main Core S.A. de C.V.** ha desarrollado proyectos significativos en diversos sectores, consolidándose como un referente en la industria tecnológica. Entre sus logros se encuentra la implementación de soluciones de alta disponibilidad para centros de datos y el diseño de planes estratégicos para la continuidad del negocio.

- La organización de la empresa (incluir organigrama)



# Informe de la práctica profesional

- **Descripción de las funciones**

En mi estancia profesional, las principales funciones asignadas fueron:

**Monitoreo de infraestructura crítica:** Supervisión diaria de servidores, redes y sistemas críticos para garantizar la disponibilidad y el rendimiento óptimo de los recursos.

**Mantenimiento preventivo y correctivo:** Diagnóstico y solución de problemas en hardware y software para prevenir interrupciones.

**Gestión de capacidad:** Evaluación y planificación de recursos para optimizar el uso de infraestructura.

**Desarrollo de DRP:** Diseño y validación del Plan de Recuperación ante Desastres, incluyendo simulaciones de incidentes críticos.

**Actualización de SOP:** Documentación y revisión de Procedimientos Operativos Estándar para reflejar las mejores prácticas operativas.

Implementación de ciberseguridad: Colaboración en la instalación y configuración de sistemas de detección y prevención de intrusos (IDS/IPS).

**Implementación de ciberseguridad:** Colaboración en la instalación y configuración de sistemas de detección y prevención de intrusos (IDS/IPS).

**Transferencia de conocimientos:** Capacitación del equipo interno para asegurar la continuidad operativa y la correcta implementación de los cambios realizados.

- **Desglose de actividades**

**Capacitación inicial y familiarización:** Aprendí sobre herramientas de monitoreo y gestión de incidentes, así como sobre ciberseguridad.

Optimización de operaciones: Documenté y ajusté SOP existentes para garantizar eficiencia y agilidad operativa.

**Gestión de desastres:** Diseñé y probé un Plan de Recuperación ante Desastres mediante simulaciones, incorporando ajustes según resultados.

Mantenimiento y análisis: Realicé mantenimiento avanzado y analicé métricas para optimizar la capacidad del centro de datos.

**Cierre de proyectos:** Supervisé el cierre de actividades operativas, documenté resultados y elaboré recomendaciones finales para futuros proyectos.

- **Bitácora de prácticas**

<b>Semanas</b>	<b>Actividades realizadas</b>	<b>Observaciones</b>
1 a 2	Capacitación en ciberseguridad y herramientas de monitoreo. Supervisión inicial de la infraestructura del centro de datos.	Se realizó un análisis básico de herramientas como IDS/IPS y se implementaron monitoreos iniciales.
3 a 4	Documentación de Procedimientos Operativos Estándar (SOP). Optimización de procesos operativos. Implementación de controles de seguridad.	La documentación incluyó ajustes sugeridos para mejorar la eficiencia y seguridad de las operaciones.
5 a 6	Diseño del Plan de Recuperación ante Desastres (DRP). Simulaciones de recuperación y ajustes al plan. Capacitación del personal en mejores prácticas operativas.	Los resultados de las simulaciones ayudaron a identificar áreas críticas para reforzar el DRP.
7 a 8	Mantenimiento avanzado de hardware crítico. Análisis de métricas para optimizar el rendimiento y prevenir fallos en infraestructura clave.	Se identificaron cuellos de botella en el uso de recursos y se implementaron mejoras.
9 a 10	Pruebas de redundancia en sistemas críticos. Validación de sistemas de respaldo y ajustes en procedimientos operativos.	Se realizaron simulaciones de fallos eléctricos para validar la continuidad operativa.
11 a 12	Supervisión del cierre de proyectos operativos. Documentación de resultados finales y elaboración de recomendaciones estratégicas en ciberseguridad y operación.	Se generaron reportes detallados con propuestas de mejora para proyectos futuros.

## Conclusiones

La estancia profesional en **Main Core S.A. de C.V.** representó una experiencia significativa que fortaleció tanto mis habilidades técnicas como las blandas necesarias en el ámbito de operación de centros de datos. A lo largo de este periodo, participé en actividades clave como el diseño y validación del Plan de Recuperación ante Desastres (DRP), la optimización de Procedimientos Operativos Estándar (SOP), el mantenimiento avanzado de hardware crítico y la implementación de controles de ciberseguridad. Estas tareas no solo me permitieron aplicar conocimientos adquiridos durante mi formación académica, sino también adaptarme a retos reales en un entorno dinámico y colaborativo.

Destacó la importancia de la planificación estratégica y el trabajo en equipo, ya que fueron fundamentales para garantizar la continuidad operativa y la seguridad de los sistemas críticos. Además, la transferencia de conocimientos al equipo interno y la documentación de resultados finales contribuyeron a crear un impacto duradero en las operaciones de la organización.

Esta experiencia no solo consolidó mi perfil profesional, sino que también me preparó para enfrentar retos futuros en el ámbito tecnológico, demostrando la relevancia de la capacitación continua, la atención al detalle y la capacidad de adaptación ante cambios en las demandas del sector.



## Cuadro CQA de mi estancia en la organización

C ¿Qué <b>C</b> onozco?	Q ¿Qué <b>Q</b> ué aporte?	A ¿Qué <b>A</b> prendí?
Aprendí a implementar y gestionar procedimientos operativos de manera eficiente, garantizando la continuidad operativa incluso en situaciones críticas.	Aporté al equipo técnico con la optimización de los Procedimientos Operativos Estándar (SOP) y el diseño del Plan de Recuperación ante Desastres (DRP).	Aprendí a implementar y gestionar procedimientos operativos de manera eficiente, garantizando la continuidad operativa incluso en situaciones críticas.
Tengo conocimientos en ciberseguridad, incluyendo la instalación y configuración de sistemas IDS/IPS para proteger la infraestructura.	Implementé controles de seguridad para mejorar la protección de los activos tecnológicos, asegurando la integridad de los datos y sistemas.	Aprendí sobre la integración de soluciones de ciberseguridad y cómo prevenir vulnerabilidades que puedan comprometer la operación del centro de datos.
Sé cómo realizar evaluaciones de métricas de rendimiento y analizar el uso de recursos para optimizar la infraestructura tecnológica.	Aporté al análisis de métricas de rendimiento, identificando áreas de mejora y optimizando el uso de recursos críticos.	Aprendí a analizar datos de rendimiento de servidores y redes para identificar cuellos de botella y proponer soluciones eficientes.
Conozco los procesos de simulación de recuperación ante desastres, que ayudan a garantizar la continuidad del negocio en caso de fallos.	Aporté en la validación y ejecución de simulaciones del Plan de Recuperación ante Desastres (DRP), garantizando que el sistema esté preparado para eventos críticos.	Aprendí a realizar simulaciones de desastres y evaluar la eficacia de las soluciones implementadas, mejorando la capacidad de respuesta ante incidentes.
Conozco las mejores prácticas en la capacitación del personal en temas de seguridad y operaciones de centros de datos.	Aporté en la creación y ejecución de un programa de capacitación en ciberseguridad y mejores prácticas operativas para el personal del centro de datos.	Aprendí a diseñar e impartir programas de capacitación que aseguren la correcta implementación de protocolos de seguridad y operativos.



## Evaluación de desempeño

Durante mi estancia en **Main Core S.A. de C.V.**, evaluó mi desempeño como positivo y alineado con los objetivos establecidos para la práctica profesional. A lo largo de las semanas, pude aplicar de manera efectiva los conocimientos adquiridos en los ciclos previos de mi formación en **Operación de Centros de Datos**, especialmente en áreas clave como la gestión de infraestructura, mantenimiento preventivo y correctivo, y ciberseguridad.

El conocimiento obtenido en los cursos anteriores me proporcionó una base sólida para realizar tareas complejas, como la supervisión de servidores y redes, el diseño del Plan de Recuperación ante Desastres (DRP), y la optimización de los Procedimientos Operativos Estándar (SOP).

Además, la formación en análisis de métricas y gestión de capacidad fue fundamental para identificar y mitigar riesgos en el centro de datos, garantizando así la continuidad operativa.

Mi capacidad para gestionar proyectos, como la actualización de SOP y la implementación de controles de ciberseguridad, fue respaldada por las habilidades de organización y resolución de problemas que adquirí en ciclos anteriores. En particular, los conocimientos sobre ciberseguridad me permitieron colaborar en la instalación de sistemas IDS/IPS y realizar simulaciones de recuperación ante desastres con éxito.

Estas actividades contribuyeron al fortalecimiento de la infraestructura tecnológica de la organización, el conocimiento técnico adquirido en mis estudios previos, junto con el enfoque práctico durante la estancia, me permitió desempeñar mis funciones con confianza y eficiencia. La experiencia no solo consolidó mi perfil profesional, sino que también me brindó herramientas y competencias adicionales que seguiré desarrollando en mi futuro profesional.

## Referencias

Procedimiento Operativo Estándar (SOP): Definición, Ejemplos, Plantilla. (s/f). Getguru.com. Recuperado el 3 de abril de 2025, de <https://www.getguru.com/es/reference/what-is-an-sop-definition-examples-how-to-make-one>

ONE Project. (s/f). Oneproject.com. Recuperado el 3 de abril de 2025, de <https://www.oneproject.com/#/>

Atlassian. (s/f). Recuperación ante desastres de TI: estrategias y prácticas recomendadas. Atlassian. Recuperado el 3 de abril de 2025, de <https://www.atlassian.com/es/incident-management/itsm/disaster-recovery>