Biblioteca INFOTEC

Ciudad de México, a 22 de abril de 2025

VISTO BUENO DE TRABAJO TERMINAL

Técnico Superior Universitario en Ciberseguridad

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el **Reporte final** desarrollado por el alumno: **Héctor Manuel Monroy Silvestre** 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 el alumno 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

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Héctor Manuel Monroy Silvestre. – Alumno Técnico Superior Universitario en Ciberseguridad.- Para su conocimiento.

Reporte final

Datos eliminados: matrícula, correo, celular, teléfono; 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

Introducción

El presente informe tiene como objetivo documentar las actividades realizadas durante mi estancia profesional en Business Conexión México, una empresa destacada en el sector tecnológico que ofrece soluciones integrales en consultoría y servicios de TI. Este periodo representó una oportunidad para aplicar los conocimientos adquiridos en el programa de Técnico Superior Universitario en Ciberseguridad y desarrollar habilidades técnicas y profesionales dentro de un entorno laboral real.

A lo largo de este proceso, se realizaron diversas tareas relacionadas con la gestión de riesgos de seguridad de la información, como la identificación de activos críticos, análisis de vulnerabilidades y la implementación de controles de seguridad, siempre en estrecha colaboración con los líderes de área y bajo la supervisión de la Dirección de TI.

Este informe detalla la estructura organizacional de la empresa, una descripción de las funciones desempeñadas, un desglose de las actividades realizadas y una bitácora de estas. Finalmente, se incluye una reflexión sobre mi desarrollo profesional durante este periodo, así como un cuadro CQA que resume mi evolución personal y profesional.

Práctica profesional

Datos personales del estudiante			
Nombre completo:	Héctor Manuel Monroy Silvestre		
Matrícula:	Eliminado	Teléfono:	Eliminado
Correo:	Eliminado		
Especialidad de TSU:	Ciberseguridad		
Año:	2024	Celular:	Eliminado
Número de horas de práctica profesional:		280	

Datos de la institución	
Nombre de la institución:	Business Conexión México
Departamento en el que realizarás tus prácticas:	IT Transformation
Nombre de la persona responsable del departamento:	Hugo Martin

Estructura organizacional

- **El sector de actividad**

Business Conexión México brinda consultoría calificada y asesoría especializada en todas las áreas de Tecnología de la Información, como:

- Infraestructura
- Consolidación
- Virtualización
- Storage
- Renovación tecnológica
- Administración de TI
- Data Center
- Redes
- Business Continuity CLIENT COMPUTING
- Implementación de soluciones tecnológicas
- Servicios de TI a lo largo del Ciclo de Vida de los Equipos
- Soluciones Digitales y Servicios On-line
- Comunicaciones Inteligentes
- Inteligencia de Negocios

- **Presentación de la empresa e historia de la empresa**

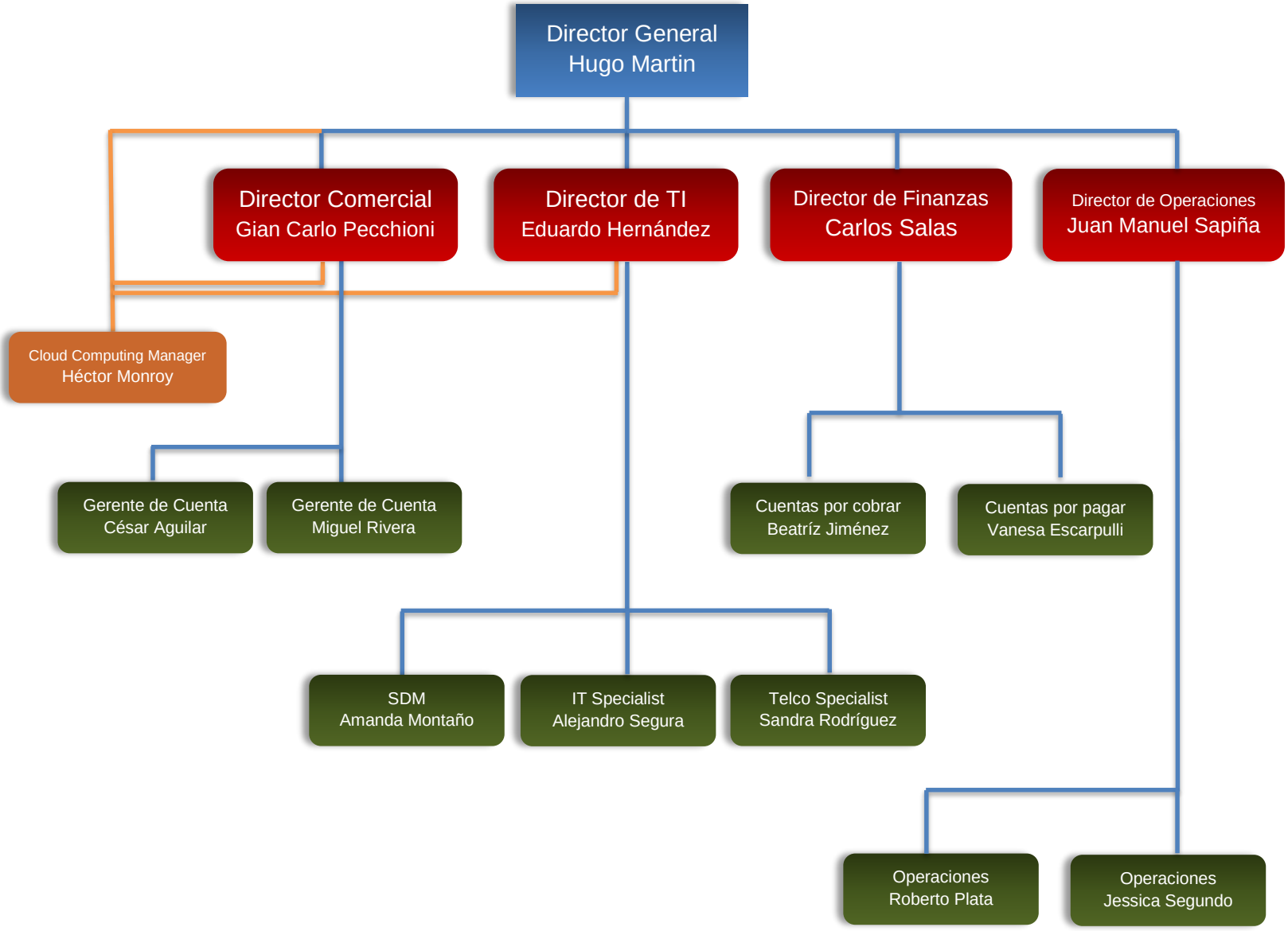
Business Conexión México es una empresa que se especializa en ofrecer Soluciones Integrales en Tecnologías de Información y Comunicaciones Unificadas.

Su filosofía de valor para los clientes se basa en tres principios básicos:

- Transformar la manera de usar la tecnología a través de la implementación de las mejores prácticas de TI en infraestructura y comunicaciones.

- Conectar a las empresas con soluciones digitales de telecomunicación, usando software y a través del internet.
- Y con esas herramientas a la mano, Decidir y tomar acciones a través de software de Inteligencia de Negocios.

- **La organización de la empresa**



Informe de la práctica profesional

- **Descripción de las funciones**

- Identificación, evaluación, análisis, tratamiento y monitoreo de riesgos.
- Procedimiento para la evaluación del impacto y las consecuencias de que una amenaza o grupo de amenazas exploten las vulnerabilidades de los activos de la organización.
- Definición del contexto de riesgo basado en la misión y visión de la organización.
- Implementación de la Gestión de Riesgos.

- **Desglose de actividades**

Fase 1 – Contexto de la Gestión de Riesgos

El objetivo de esta fase es identificar las condiciones bajo las cuales se debe desarrollar el trabajo metodológico de la gestión de riesgos y que pueden determinar el curso de esta, definiendo los siguientes aspectos:

- Condiciones iniciales de la administración de riesgos
- Criterios de riesgo
- Estrategia de comunicación
- Riesgos del proyecto
- Plan de trabajo

Fase 2 – Identificación de Activos

La identificación de los activos debe considerar los sistemas de información como hardware, software, aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información, que soportan los procesos de negocio, o componentes críticos para el cumplimiento de los objetivos estratégicos de la organización.

La identificación de activos debe realizarse a un adecuado nivel de detalle que proporcione información suficiente para una evaluación de riesgos efectiva.

Se pueden identificar, entre otros, los siguientes activos:

- Hardware
- Software
- Sitios web
- Personal
- Oficinas
- Estructura Organizacional
- Documentación

Fase 3 – Identificación de Amenazas y Vulnerabilidades

El objetivo durante esta fase es generar una lista completa de las amenazas y vulnerabilidades que existan sobre la base de aquellos eventos que se pueden mejorar, prevenir, degradar o retrasar el logro de los objetivos estratégicos de la organización.

Se define el escenario de riesgo asociado a cada activo que fue seleccionado en la fase anterior, a fin de definir la vulnerabilidad asociada y la amenaza que provocaría el evento.

Una amenaza tiene la característica de dañar los activos, procesos y sistemas de información y por consiguiente a la organización. Las amenazas pueden ser originadas por medios naturales o humanos y estas pueden ser accidentales o deliberadas.

Una vulnerabilidad se considera como la debilidad que hace a un sistema más propenso al ataque de una amenaza y que sea más probable que este tenga éxito impactando a la organización.

Fase 4 – Evaluación de Riesgos

El objetivo durante la fase de evaluación de riesgos es realizar la medición de las amenazas y vulnerabilidades, así como aquellas condiciones y factores que puedan afectar los activos de la organización.

Los tres principales objetivos en esta fase son los siguientes:

- Cálculo de métricas mediante la medición del impacto de cada una de las vulnerabilidades encontradas en los activos dentro del alcance acordado.
- Cálculo de nivel de los riesgos identificados.
- Elaborar reporte de los riesgos identificados.

Fase 5 – Análisis de Riesgos

El objetivo principal de esta fase es analizar los riesgos identificados y elaborar las opciones de tratamiento de riesgos, en esta etapa se analizan los niveles de riesgo obtenidos durante la fase anterior, las amenazas y vulnerabilidades, su importancia, criticidad de sus procesos, aplicaciones, servicios soportados y los factores internos que determinarán con mayor precisión el tipo de tratamiento.

En esta fase se ponderan y priorizan los riesgos según los criterios establecidos por la organización y cada una de sus Direcciones y se identifican los riesgos sujetos a tratamiento.

Fase 6 – Tratamiento de Riesgos

El objetivo del tratamiento de riesgos es definir, documentar e implementar las acciones de tratamiento de riesgos que se deben llevar a cabo para cada uno de los riesgos identificados, considerando los factores del impacto y costo de implementación de las medidas sugeridas.

La administración de los recursos asignados para el tratamiento de riesgos, así como la prioridad de cada uno es una tarea que requiere de una coordinación estrecha con cada uno de los responsables definidos.

Fase 7 – Comunicación y presentación de resultados

La comunicación durante el procedimiento de riesgos asigna una gran importancia al diálogo con las partes interesadas que pueden verse afectadas ante un evento.

Informar los riesgos identificados para que determine el tratamiento que se debe aplicar a cada uno de ellos.

- **Bitácora de prácticas**

Semanas	Actividades realizadas	Observaciones
1 a 2		
3 a 4		

5 a 6

FASES	SEMANA 5 30 sep - 06 oct 2024 L	M	M	J	V	S	D	SEMANA 6 07 - 13 oct 2024 L	M	M	J	V	S	D
Planeación														
Preparación														
Ejecución														
Identificación de amenazas y vulnerabilidades														
Determinación de vulnerabilidades por escaneos														
Escaneo de dispositivos tecnológicos														
Determinación de vulnerabilidades por Entrevistas	4													
Sesión con área operativa		4												
Sesión con área financiera			4											
Sesión con área de RH				4										
Sesión con área de proveedores					4									
Sesion con área de TI								4	4					
Evaluación de Riesgos										4	4	4		

7 a 8

FASES	SEMANA 7 14 - 20 oct 2024 L	M	M	J	V	S	D	SEMANA 8 21 - 27 oct 2024 L	M	M	J	V	S	D
Planeación														
Preparación														
Ejecución														
Evaluación de Riesgos														
Definir Riesgos en Documento	4	4												
Ponderación de Riesgos			4	4										
Análisis de Riesgos					4			4	4					
Carta de Aceptación de Riesgos con los responsables										4	4	4		

9 a 10

FASES	SEMANA 9 28 oct - 03 nov 2024 L	M	M	J	V	S	D	SEMANA 10 04 - 10 nov 2024 L	M	M	J	V	S	D
Planeación														
Preparación														
Ejecución														
Carta de Aceptación de Riesgos con los responsables														
Definir controles de seguridad para mitigar Riesgos	4	4	4	4	4									
Definir fecha compromiso para mitigar Riesgos								4						
Implentación de controles de seguridad para mitigar Riesgos									4	4	4	4		

11 a 12		

Conclusiones

El tiempo ha transcurrido con notable rapidez, y en más de una ocasión llegué a pensar que no lograría concluir mi proyecto en tiempo y forma. Sin embargo, tras una revisión con la Dirección General, confirmé que mi avance está alineado con los tiempos establecidos en el plan de trabajo inicial. Esto me brinda una gran tranquilidad y confianza, especialmente considerando la carga de trabajo, las responsabilidades personales y las presiones cotidianas. Estoy por culminar una etapa trascendental en mi desarrollo profesional.

En enero de 2023 tomé la decisión de aprovechar la extraordinaria oportunidad que INFOTEC ofrece. Obtener una beca en la actualidad es un desafío, y costear una carrera profesional requiere un esfuerzo significativo. Aunque enfrenté tropiezos y en ocasiones consideré abandonar debido a la acumulación de actividades, mi determinación de crecer y sobresalir prevaleció. Hoy, estoy a un mes de finalizar mi Técnico Superior Universitario (TSU) en Ciberseguridad.

La confianza depositada por Business Conexión México fue clave para ejecutar un proyecto que había visualizado por mucho tiempo. Los conocimientos adquiridos en el TSU, junto con la experiencia acumulada en mi trayectoria laboral, me permitieron materializar esta idea y demostrar el valor que puedo aportar a la organización.

Tras recibir el visto bueno de la Dirección General, elaboré un plan de trabajo y preparé una presentación para la sesión de kick-off con toda la organización. Desde ese momento, dediqué tiempo considerable al proyecto, sacrificando parte de mi jornada laboral y, en gran medida, utilizando noches y fines de semana para alcanzar mi objetivo.

Uno de los hitos más importantes fue la creación del comité interno de riesgos, que contó con el respaldo del Director de TI y el Director de Finanzas. Su retroalimentación constante fue fundamental para validar mi avance.

A partir de ahí, inicié con las entrevistas necesarias para identificar los activos y mapear los posibles riesgos de seguridad de la información. Estas entrevistas resultaron desafiantes, ya que implicaron comprender procesos en áreas fuera de mi especialidad. Durante las pruebas de penetración, disfruté mucho la oportunidad de explorar a fondo el entorno Linux, uno de mis sistemas favoritos, y aprender comandos que posteriormente implementé en scripts para detectar vulnerabilidades en activos tecnológicos.

La elaboración del documento de riesgos y su ponderación fue una de las tareas más complejas, ya que requería un equilibrio entre conocimientos técnicos en seguridad y una evaluación precisa para identificar objetivamente puntos críticos de vulnerabilidad. Una vez presentado el reporte a la Dirección General, se realizaron algunos ajustes, pero el proyecto fue aprobado para avanzar en la implementación de acciones de tratamiento y mitigación de riesgos.

Actualmente, estoy en la fase de implementación de controles de seguridad en colaboración con los responsables de cada área. Mi próxima meta es asegurar que estos controles se apliquen de manera efectiva, recabar las evidencias correspondientes y preparar el reporte final del análisis de riesgos.

Cuadro CQA de mi estancia en la organización

C ¿Qué **C**onozco?	Q ¿**Q**ué aporté?	A ¿Qué **A**prendí?
Antes de iniciar mi estancia profesional, contaba con conocimientos teóricos sobre seguridad de la información, herramientas básicas de ciberseguridad, análisis de riesgos, y habilidades en Linux, adquiridos durante mi formación académica y vida laboral. También tenía experiencia limitada en el análisis de vulnerabilidades y experiencia de un proyecto previo en el que participé como apoyo para certificar a una empresa en ISO 27001.	Durante mi estancia profesional, contribuí al desarrollo de un plan de análisis de riesgos alineado con las necesidades de la empresa, así como a la creación de un comité interno de riesgos. Implementé scripts personalizados para detectar vulnerabilidades, elaboré un documento de riesgos con propuestas de mitigación y colaboré en la implementación de controles de seguridad junto con los responsables de cada área. Mi enfoque proactivo permitió optimizar recursos y generar valor para la organización.	Adquirí experiencia práctica en la identificación y análisis de riesgos, la ejecución de pruebas de penetración y la gestión de proyectos de seguridad. Aprendí a trabajar en equipo con áreas multidisciplinarias, a comunicar hallazgos técnicos de manera comprensible para la dirección y a gestionar mi tiempo de forma eficiente para equilibrar múltiples responsabilidades. También mejoré mis habilidades técnicas en scripting y herramientas de análisis de vulnerabilidades.

Evaluación de desempeño

Durante mi estancia profesional en Business Conexión México (BCM), considero que mi desempeño fue positivo y enfocado en cumplir los objetivos planteados desde el inicio del proyecto. La experiencia me permitió aplicar los conocimientos adquiridos en ciclos anteriores, los cuales fueron fundamentales para llevar a cabo mis tareas con éxito y adaptarme a las necesidades de la organización.

Uno de los aspectos clave que influyó en mi desempeño fue el aprendizaje sobre metodologías de gestión de riesgos y análisis de vulnerabilidades. Estos conocimientos me permitieron abordar el proyecto con una estructura clara, desde la identificación de activos y amenazas hasta el desarrollo de un plan de mitigación de riesgos. Además, mi experiencia previa en el manejo de herramientas en entornos Linux me brindó una ventaja significativa al ejecutar pruebas de penetración y automatizar procesos mediante scripts.

Evaluando mi desempeño, destaco mi capacidad para comunicar el objetivo del proyecto de manera efectiva, lo que fue clave para ganar la confianza y el respaldo del comité interno de riesgos, así como de dirección general. Mi habilidad para adaptarme a las dinámicas de una organización multidisciplinaria y para identificar áreas de mejora en tiempo real también contribuyó a optimizar los tiempos del proyecto.

Sin embargo, identifico como área de mejora mi gestión del tiempo, ya que las múltiples responsabilidades laborales y académicas a veces generaron presión adicional. A pesar de esto, implementé estrategias que me permitieron avanzar de manera constante y cumplir con los plazos establecidos en el plan de trabajo.

Además del fortalecimiento de mis competencias técnicas, tuve la oportunidad de fortalecer habilidades blandas que fueron clave para el éxito del proyecto. Aprendí a trabajar bajo presión y a mantener un enfoque claro en la resolución de problemas, incluso en situaciones desafiantes. Desarrollé habilidades de negociación y empatía

al interactuar con diversas áreas de la empresa, lo que me permitió integrar sus necesidades y expectativas en las soluciones propuestas.

También reforcé mi capacidad para gestionar equipos de trabajo, promoviendo la colaboración y creando un ambiente de confianza que facilitó la implementación de los controles de seguridad. Estas experiencias me ayudaron a entender la importancia de las relaciones interpersonales y el impacto de una comunicación asertiva en el logro de objetivos comunes. Este aprendizaje complementa mi formación técnica y me prepara para enfrentar nuevos desafíos en mi desarrollo profesional.

En conclusión, la integración de conocimientos técnicos y habilidades prácticas, sumados al aprendizaje obtenido durante la estancia, me han permitido no solo completar un proyecto relevante, sino también fortalecer mi perfil profesional en un área tan dinámica como la ciberseguridad.

Referencias

Business Conexión México (**septiembre, 2024**) Descripción de los servicios de la empresa. Sitio web: https://www.dconexion.mx/

Business Conexión México (**septiembre, 2024**) Descripción de los servicios de la empresa. Sitio web: https://www.businessconexion.com.mx/

Héctor Monroy (**septiembre, 2024**) "Kick off Gestión de Riesgos" (Presentación a toda la organización)

Héctor Monroy (**septiembre, 2024**) "Organigrama creado para el reporte final"

Business Conexión México (**septiembre, 2024**) "Contexto del Riesgo" (Parte de la metodología para la gestión de riesgos)

Business Conexión México (**septiembre, 2024**) "Metodología para la Gestión de Riesgos"

Business Conexión México (**agosto, 2024**) "Presentación de firma" (Descripción de la empresa)

Felipe Hernández (**septiembre, 2015**) "Referencia para elaborar el Cuadro CQA" Sitio web:https://prezi.com/vcj6scj4ddek/cuadro-cqa/

Anáhuac Puebla (**noviembre, 2022**) "Habilidades blandas y duras: ¿cuál es su diferencia?" (Apoyo para reforzar conceptos) Sitio web: https://puebla.anahuac.mx/licenciaturas/blog/habilidades-blandas-y-duras-diferencias

Uvirtual (**enero,2024**) "Habilidades blandas y duras: diferencias y cómo desarrollarlas" (Apoyo para reforzar conceptos) Sitio web: https://blog.uvirtual.org/diferencias-entre-habilidades-blandas-y-duras

Editorial Etecé (**marzo, 2024**) "Estructura organizacional" Sitio web: https://concepto.de/estructura-organizacional/