UNIVERSIDAD IBEROAMERICANA

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial
Del 3 de abril de 1981

“Vigilancia tecnológica e Inteligencia Competitiva para sitios web en instituciones educativas a nivel superior”

TESIS

Que para obtener el grado de

MAESTRA EN GESTIÓN DE LA INNOVACIÓN TECNOLÓGICA

P r e s e n t a

VIRIDIANA VOLANTÍN VENEGAS

Director: Mtro. Antonio Carlos Cardeña Matamoros

Ciudad de México, 2025

Índice

Introducción 4
1. Descripción del problema, objetivo(s) y justificación. 5
1.1 Problema 5
1.1.1 Factores que detonaron el problema 5
1.2 La importancia de resolver el problema 6
1.3 Objetivos del proyecto 6
2. El contexto y la situación actual. 7
2.1 Análisis del contexto externo 7
2.2 Análisis del contexto interno 8
2.3 Análisis del problema dentro de la organización 11
3. Marco teórico y conceptual 14
3.1 Enfoque conceptual desde la gestión de la innovación tecnológica 14
3.1.1 Vigilancia tecnológica 16
3.1.2 Inteligencia Tecnológica Competitiva 17
3.1.3 Ciclo de la Vigilancia tecnológica e Inteligencia Tecnológica Competitiva. 17
3.2 La Inteligencia Competitiva y su impacto en la estrategia 18
3.3 ¿Cuál es el rol de la ITC en la empresa? 19
3.4 Modelos teóricos 20
3.4.1 Modelo de Difusión de Innovaciones 20
3.4.2 Modelo de COTEC 21
3.4.3 Modelo de Vigilancia Tecnológica según Norma UNE 166.006 22
3.5 Modelo de vigilancia e inteligencia de Godet 23
3.6 Casos documentados 27
3.6.1 Caso 1: Vigilancia Tecnológica en el sector Financiero (Gutiérrez, Cidei, 2023) 28
3.6.2 Caso 2: Inteligencia Tecnológica Competitiva para fortalecer la Innovación (Petróleo, 2017) 29
3.6.3 Caso 3: Caso de éxito: Análisis de vigilancia tecnológica e inteligencia competitiva en el sector de las criptomonedas (e-intelligent, 2022) 30
4. Alternativas de solución 34
4.1 Restricciones o limitaciones del Modelo de Vigilancia Tecnológica según Norma UNE 166.006 35
4.2 Restricciones o limitaciones del Modelo COTEC 35
4.3 Restricciones o limitaciones del Modelo Nacional de Gestión de Tecnología e Innovación 36
4.4 Comparativa de modelos 37
4.5 Alternativa de la solución 38
4.6 Fases para la creación de la Unidad 42
5. Metodología de trabajo 45
5.1 Descripción del problema, objetivos y justificación 46
5.2 Contexto actual de la organización 46

5.3 Marco teórico y conceptual 46
5.4 Alternativas de solución 47
5.5 Metodología del trabajo 47
5.6 Proceso de validación y aplicación de propuesta en el caso 47
5.7 Plan de implementación 48
5.8 Limitaciones y recomendaciones 48
5.9 Conclusiones 48
6. Proceso de validación y aplicación de propuesta en el caso 48
6.1 Proceso de validación 48
6.1.1 Focus group 48
Resultados de los *focus group* 49
6.2 Mejoras en la propuesta inicial 51
7. Plan de implementación 53
7.1 Implementación a alto nivel 53
7.2 Plan de trabajo 54
7.2.1 Diagrama WBS 54
7.2.2 Diagrama de Gantt 55
7.3 Retos que representan a la DIT 56
7.4 Gestión de riesgos 57
7.5 Costos 59
8. Limitaciones y recomendaciones 59
Recomendaciones a los lectores 60
9. Conclusiones 61
10. Anexos 62
Bibliografía 65

Introducción

Dentro de un escenario de acelerada transformación digital y cambio tecnológico, las instituciones universitarias se ven obligadas a adaptarse continuamente y anticipar tendencias emergentes para preservar su relevancia en los ámbitos académico, investigativo y social. El sector de la informática, en particular, se halla en constante evolución debido al desarrollo vertiginoso de tecnologías como la inteligencia artificial, la ciberseguridad, la computación en la nube y el Internet de las cosas (IoT), entre otros avances. En este contexto, la gestión eficiente de los entornos digitales universitarios —especialmente los sitios web institucionales— se vuelve una tarea crítica, tanto para la operación cotidiana como para la proyección estratégica de la universidad.

Actualmente, en la Dirección de Innovación Tecnológica (DIT) de una universidad privada, se ha identificado una problemática significativa derivada de la administración de más de 200 sitios web, desarrollados con plataformas y tecnologías heterogéneas. Esta situación ha generado dificultades en la actualización oportuna, en la implementación de medidas de ciberseguridad, y en la alineación con los estándares institucionales de identidad digital. Asimismo, la ausencia de un sistema estructurado para anticipar cambios tecnológicos y coordinar decisiones estratégicas ha derivado en un entorno fragmentado, reactivo y expuesto a riesgos crecientes de obsolescencia y vulnerabilidad operativa.

Frente a este escenario, la instauración de una Unidad de Vigilancia Tecnológica (VT) e Inteligencia Competitiva (IC) se plantea como una estrategia fundamental para fortalecer la capacidad de la universidad para identificar, analizar y aprovechar las transformaciones tecnológicas y las dinámicas competitivas que inciden en el desarrollo web institucional. Esta unidad facilitará la recolección, análisis y difusión de información estratégica que respalde la toma de decisiones en aspectos clave como la investigación, el desarrollo de plataformas, la transferencia tecnológica y la vinculación con el entorno.

La vigilancia tecnológica implica un monitoreo sistemático del entorno científico y tecnológico con el propósito de identificar oportunidades, amenazas y tendencias que puedan influir en la actividad universitaria. Por su parte, la inteligencia competitiva complementa esta labor al incorporar el análisis del mercado, la actividad de competidores, y las nuevas demandas sociales y laborales. En conjunto, ambas estrategias brindan a la institución educativa una ventaja prospectiva que permite prever cambios críticos, optimizar sus procesos de innovación y consolidar su posicionamiento en el ecosistema digital, científico y académico.

La finalidad de esta investigación es diseñar e implementar una propuesta para la creación de una Unidad de VT e IC enfocada en el ámbito de la informática, específicamente en la gestión de los sitios web de la universidad. Para ello, se plantea definir su estructura organizativa, los procesos operativos que la sustentarán, las herramientas tecnológicas requeridas, así como sus mecanismos de integración con las actividades sustantivas de la institución. El objetivo general de este estudio es fortalecer la capacidad de adaptación tecnológica de la universidad y promover una cultura organizacional centrada en la innovación, la prospectiva y el conocimiento estratégico.

Este documento se compone de diversos capítulos que abordan, en primer lugar, la problemática actual relacionada con el desarrollo, mantenimiento y seguridad de los sitios web, así como la participación de los actores responsables de estos procesos. En segundo lugar, se presentan los fundamentos teóricos de la vigilancia tecnológica y la inteligencia competitiva. Posteriormente, se realiza un diagnóstico institucional que permite identificar necesidades específicas en el ámbito de la informática. A continuación, se describe el diseño de la unidad propuesta. Finalmente, se exponen las conclusiones y recomendaciones que servirán como guía para su implementación y desarrollo futuro.

1. Descripción del problema, objetivo(s) y justificación.

Las universidades enfrentan diariamente la necesidad de mantenerse a la vanguardia tecnológica. El uso de plataformas, lenguajes de programación o librerías obsoletas no solo afecta el rendimiento de los sitios web institucionales, sino también expone a los sistemas a vulnerabilidades de seguridad, además de influir en la experiencia del usuario. La falta de planificación oportuna y la ausencia de una estrategia de detección temprana de cambios tecnológicos representan un riesgo significativo para la operación digital de la universidad.

1.1 Problema

El principal desafío radica en las dependencias de tecnologías obsoletas, las cuales impactan negativamente el rendimiento y la seguridad de los sistemas y sitios web de la universidad. La ausencia de una estrategia de innovación tecnológica impide la detección oportuna de cambios críticos en plataformas, frameworks, lenguajes de programación o librerías utilizadas por estos, lo que genera riesgos en tres áreas principales:

1) **Seguridad:** Las versiones de software son más susceptibles a ataques cibernéticos, comprometiendo la integridad de la información y la estabilidad de los sistemas web (Carmona, 2023).
2) **Experiencia del usuario:** La lentitud y las fallas en las plataformas afectan la interacción de estudiantes, docentes, administrativos y posibles aspirantes con los servicios digitales.
3) **Costos operativos:** Mantener infraestructura obsoleta implica inversiones adicionales en soporte extendido, actualizaciones urgentes y soluciones temporales que podrían evitarse con una planificación adecuada.

1.1.1 Factores que detonaron el problema

A pesar de los esfuerzos del personal de la Dirección de Informática y Telecomunicaciones (DIT) por fortalecer y optimizar la infraestructura tecnológica, la carga operativa diaria y la gestión de proyectos prioritarios desvían la atención de actualizaciones críticas. Como resultado, cuando se identifican necesidades de migración tecnológica, el tiempo disponible para implementar los cambios suele ser insuficiente, lo que obliga a tomar decisiones apresuradas y aumenta el riesgo de errores y soluciones temporales.

Además, algunas plataformas pueden quedar obsoletas o perder soporte oficial, lo que obliga a la universidad a incurrir en costos adicionales por soporte extendido o a desarrollar soluciones alternativas de emergencia. De igual manera, las versiones antiguas de los lenguajes de programación pueden volverse incompatibles con servidores modernos, y los navegadores pueden dejar de admitir ciertas librerías, afectando la funcionalidad de los sitios web.

Frente a este escenario, tres áreas clave dentro de la DIT se ven directamente impactadas:

- **Infraestructura:** Administración y mantenimiento de servidores web y de bases de datos.
- **Seguridad:** Protección de sitios web y mitigación de riesgos cibernéticos.
- **Desarrollo de plataformas:** Actualización y optimización del código y funcionalidades.

Si una plataforma web utiliza tecnologías desactualizadas o versiones obsoletas de lenguajes de programación, su rendimiento se percibe como lento para los usuarios, y la infraestructura no puede actualizarse debido a incompatibilidades con servidores más recientes. Esto, a su vez, abre brechas de seguridad que pueden ser explotadas por ciberdelincuentes, obligando al área de seguridad a reforzar sus esfuerzos para mitigar riesgos y prevenir ataques.

Una de las responsabilidades clave de la DIT es fortalecer, mejorar y mantener la infraestructura tecnológica, además de monitorear los cambios generados por factores externos, como actualizaciones de seguridad o la obsolescencia de funcionalidades en navegadores como Chrome. Si estos cambios no se gestionan de manera oportuna, las áreas involucradas se ven obligadas a trabajar bajo presión para cumplir con los requerimientos, lo que limita la evaluación de alternativas y, en muchos casos, conduce a la implementación de soluciones temporales que no resuelven el problema de fondo.

1.2 La importancia de resolver el problema

Abordar este problema es crucial por dos razones principales:

1) Impacto en los usuarios:
    a. Sitios web lentos o inoperables pueden provocar que aspirantes aborden el proceso de consulta y pierdan interés en la universidad.
    b. Los administrativos pueden enfrentar dificultades en sus labores cotidianas, afectando la operatividad de la universidad.
    c. Los estudiantes pueden experimentar problemas al realizar trámites en línea, generando inconformidad con los servicios universitarios, ya que buscan experiencias digitales positivas, por ejemplo, que los trámites que requieran realizar sean de manera ágil desde una plataforma (base22, s.f.).
2) Seguridad y estabilidad tecnológica
    a. La infraestructura se vuelve vulnerable a posibles ciberataques, causando así un retraso operativo. Además, las brechas de seguridad pueden comprometer información delicada de la universidad.
    b. La falta de una planificación adecuada limita la capacidad de respuesta ante emergencias tecnológicas.

Adicionalmente, se suma el factor de la pérdida de confianza y prestigio para la universidad, lo cual podría afectar su posicionamiento en las búsquedas digitales, apareciendo por debajo de sus competidores.

Asimismo, la falta de planificación de actualización de plataformas obliga a los equipos de TI a responder de manera reactiva. Esto genera una carga de trabajo considerable, lo que puede provocar desgaste físico y mental, además de un mayor margen de error en las soluciones implementadas.

En el artículo de "*Los riesgos del estrés laboral para la salud*", se destaca que la sobrecarga de tareas rutinarias puede provocar sentimientos constantes de tensión, impotencia y frustración, generando un estado de estrés persistente. Esta situación conduce al desgaste físico y mental, manifestándose en trastornos digestivos, aumento en la tensión arterial y dolor de cabeza. Además, se menciona un estudio de la Academia Americana de Neurología, el cual indica que las personas con trabajos demandantes y poco control sobre sus actividades tienen 58 % más probabilidades de sufrir una isquemia y un 22 % más de riesgo de padecer una hemorragia cerebral. (Instituto Nacional de Salud Pública, s.f.).

1.3 Objetivos del proyecto

El objetivo principal de este proyecto es diseñar y proponer la creación de un área especializada dentro de la DIT de la universidad, con el propósito de fortalecer la gestión tecnológica institucional a través de un enfoque estratégico e integral. Esta área tendrá como función principal el monitoreo constante de los cambios tecnológicos en plataformas, infraestructura y ciberseguridad. Lo que permitirá anticipar tendencias y responder oportunamente ante los desafíos que impone el entorno digital (Observa, s.f.). Asimismo, se busca implementar mecanismos de detección temprana de factores internos y externos que puedan impactar negativamente en los sistemas web universitarios, como fallas técnicas, amenazas cibernéticas o cambios normativos, permitiendo así una intervención proactiva.

El área propuesta también estará encargada de diseñar e implementar estrategias de actualización tecnológica que minimicen riesgos, optimicen recursos y garanticen la estabilidad, funcionalidad y seguridad de los sitios web institucionales, mejorando con ello la experiencia del usuario final. Además, se incorporarán herramientas de análisis estratégico como FODA, PESTEL, Porter y CAME, las cuales permitirán a la universidad evaluar su posicionamiento en el entorno competitivo, identificar oportunidades de mejora, anticipar amenazas y diseñar planes de acción que respalden la toma de decisiones informadas (Buzzi, 2023).

Este proyecto también considera que la adopción de una estrategia de innovación tecnológica no solo debe responder a necesidades inmediatas, sino también orientarse al mediano y largo plazo (Roberto Marijuán, 2015). En ese sentido, se plantea que dicha estrategia contribuya a la optimización del presupuesto destinado a infraestructura tecnológica, así como a la introducción de buenas prácticas en el uso de las tecnologías de la información (Observatorio Virtual de Transferencia de Tecnología, 2025). Finalmente, se espera que esta área facilite la colaboración con socios estratégicos externos, identificando oportunidades de cooperación beneficiosas para la universidad en el marco de una transformación digital sostenible.

2. El contexto y la situación actual.

En el entorno universitario actual, los sitios web institucionales han adquirido un papel estratégico fundamental. No solo representan el rostro digital de la universidad ante aspirantes, estudiantes, docentes y la sociedad en general, sino que también operan como herramientas clave para la gestión académica, administrativa y de comunicación (Impactum, 2023). La experiencia del usuario en estas plataformas impacta directamente en la percepción de la calidad institucional, y, por tanto, en la competitividad de la universidad dentro del mercado educativo. Sin embargo, mantener estos entornos digitales en condiciones óptimas plantea grandes retos técnicos, de seguridad y de actualización tecnológica.

En el caso específico de la Dirección de Innovación Tecnológica (DIT) de una universidad privada, se enfrenta actualmente una situación crítica derivada del uso de tecnologías obsoletas, la diversidad de plataformas, y la carencia de un área especializada que dé seguimiento continuo a los cambios tecnológicos. La universidad gestiona más de 200 sitios web, tanto públicos como de intranet, lo que complica su mantenimiento oportuno y seguro. Esta complejidad se ve agravada por prácticas descentralizadas, donde usuarios internos recurren a proveedores externos sin seguir lineamientos institucionales, generando retrasos, inconsistencias en la identidad digital y riesgos de ciberseguridad.

Además, el contexto externo impone presiones significativas: los ciberataques en el sector educativo aumentan cada año, y la falta de actualizaciones incrementa la vulnerabilidad de los sistemas. A nivel interno, las migraciones de plataformas como PHP o ColdFusion se vuelven procesos prolongados, a menudo interrumpidos por prioridades operativas urgentes. Ante este escenario, se vuelve imperativo implementar una estrategia estructurada y proactiva que permita a la DIT anticiparse a los riesgos tecnológicos, optimizar recursos y garantizar la seguridad de sus sitios web. Esta tesis propone, por tanto, la creación de un área especializada dentro de la DIT que atienda dichos desafíos, mediante un enfoque estratégico, analítico y orientado a la innovación tecnológica institucional.

2.1 Análisis del contexto externo

En la actualidad, el posicionamiento web juega un papel importante, ya que les permite ser de las primeras opciones al momento que el usuario final busca información relacionada con algún tema en particular, es por ello por lo que es importante destacar el impacto de un sitio web, ya que según estadísticas de WebFX (*Digital Marketing that Drives Revenue*, 2025), se tiene que considerar que:

- ⇨ El **21 %** de las pequeñas empresas citan el bajo tráfico como el mayor de los desafíos de un sitio web.
- ⇨ El **50 %** de los consumidores dicen que sus impresiones de una empresa dependen del diseño del sitio web de la empresa.
- ⇨ El **42 %** de las personas abandonarían un sitio web debido a una funcionalidad deficiente.

Además, los sitios web no solo son utilizados para dar información general a los estudiantes o aspirantes, también son parte fundamental del núcleo de la universidad, existe una gran variedad de sitios web que son utilizados por los administrativos, profesores o alumnos para llevar a cabo actividades cotidianas, por ejemplo:

- Dar de alta materias a cursar
- Evaluar a los profesores y alumnos en evaluaciones aplicadas durante el semestre
- Cargar CV para obtener oportunidades laborales
- Portal de Recursos Humanos para que los interesados y con la autorización previa puedan ver información de su interés

Si los sitios web son lentos o no permiten trabajar de manera óptima, puede retrasar tareas, que, en corto o mediano plazo, pueden causar molestia de la comunidad en general.

La DIT, está comprometida con el correcto funcionamiento y protección de los sitios, actualmente la universidad cuenta con más de 200 sitios, entre sitios intranet y sitios públicos, con tecnologías e infraestructura diversa, esto obstaculiza poder actualizar de manera oportuna a cada uno de ellos, además de los sitios que surgen en el transcurso de un año.

Dado lo anterior, la DIT enfrenta un problema cuando los usuarios, en su afán por encontrar soluciones rápidas, recurren a sus propios proveedores para el desarrollo de sus sitios web, sin considerar la infraestructura institucional, manual de identidad digital o el uso correcto de los logos institucionales, así como la tipografía y los colores correctos a utilizar. Como resultado, al intentar alojar estos sitios web en la infraestructura institucional, a menudo no cumplen con los requisitos establecidos, lo que genera retraso en la publicación de estos, debido a que se requieren hacer ajustes y pasar por el escaneo de vulnerabilidades.

Desde el panorama de los estudiantes, las plataformas pueden ser tan extensas que no saben dónde pueden localizar la información que requieren, lo que puede hacerlos caer en páginas maliciosas, que su único fin es robar la información importante y no solo obtener información del alumno, sino también credenciales válidas para poder ingresar a los sistemas digitales de la universidad, lo que puede generar una brecha de seguridad para los sistemas de la universidad.

La DIT enfrenta un gran desafío al atender diversos usuarios, los cuales requieren diversos servicios, por ejemplo, la creación, actualización o alojamiento de sitio web. Todo esto sin olvidar su misión, la cual es garantizar que los sitios web de la universidad sean óptimos y seguros. Sin embargo, el uso de tecnología obsoleta, como Drupal versión 7.x.x, complica más dicha tarea,

2.2 Análisis del contexto interno

La presencia de tecnología obsoleta representa un gran desafío crítico para la DIT, ya que afecta directamente el rendimiento, la ciberseguridad y la competitividad de la universidad.

Según Cloudflare, en México el sector educativo recibió el 3.2 % de los ciberataques registrados en el 2024 (Redacción Portal ERP México, 2024). Este dato resalta la importancia de contar con herramientas de seguridad actualizadas y aplicar los parches necesarios, de lo contrario, los sistemas digitales podrían convertirse en vulnerabilidades críticas para la universidad.

A continuación, se presenta un panorama actualizado de la infraestructura de la DIT, la cual cuenta con servidores web y de base de datos que operan bajo distintos sistemas operativos, entre ellos:

- Red Hat 7.x.x., 8.x.x y 9.x.x
- Windows Server 2016 Std.
- Windows Server 2019

Esta diversidad responde a la variedad de plataformas y tecnologías en uso, algunas de las cuales se encuentran en proceso de migración. Entre las principales tecnologías utilizadas se incluyen.

- PHP 7.x.x, 8.x.x
- Coldfusion 2021
- React
- Angular
- Los Sistemas de Gestión de Contenido (SGC), también conocidos como CMS, como WordPress, Drupal, entre otros.

La heterogeneidad de estos entornos hace que la protección de los distintos sitios web sea una tarea compleja. El equipo de seguridad debe aplicar medidas específicas para cada tecnología, lo que requiere un enfoque especializado. Para mitigar riesgos, se emplean herramientas como Imperva, que brinda protección avanzada contra amenazas web.

Asimismo, la diversidad de plataformas e infraestructura, sumada a las tareas operativas diarias, dificulta la atención oportuna a actualizaciones y el seguimiento de fechas clave, como el fin del soporte de determinadas tecnologías. Esta situación se agrava cuando no existe un equipo designado para monitorear y gestionar los cambios tecnológicos, lo que aumenta el riesgo de obsolescencia y vulnerabilidades en los sistemas.

Un ejemplo de ello, es que la DIT actualmente lleva poco más de un año tratando de migrar sitios informativos de una versión de PHP a otra, considerando el análisis de vulnerabilidad aplicado por parte del equipo de seguridad, el cual puede llevarse un tiempo considerable de aproximadamente un mes, todo esto sin descuidar la operación diaria, tal como la actualización de sitios, agregar nuevas sesiones a sitios, publicar nuevos sitios desarrollados por proveedores, los cuales ya pasaron por la aprobación de seguridad, así como la generación de nuevos sitios, lo que implica a realizar las migraciones de forma pausada y en caso de que lleguen proyectos con mayor prioridad, incluso se pueden poner en pausa, hasta que el proyecto concluya.

Tomando en cuenta los tiempos que puede tardar una migración, puede pasar que cuando se está concluyendo o a mitad de la migración ya se cuente con nueva versión de PHP o que seguridad indique que es necesario migrar de versión dado que la actual tiene una vulnerabilidad, lo que hace que la tarea de migración de sitios informativos se vuelva una tarea infinita.

En el caso de los sitios web realizados con tecnología Coldfusion es mucho más controlada la migración, ya que esta puede tardar un año en concluir, pero la plataforma da cinco años de soporte, lo que le da a la DIT una ventaja de cuatro años, en los que solo se tiene que preocupar por actualizaciones de la misma plataforma o del sistema operativo, según sea el caso.

Adicionalmente, Kaspersky, en su informe de “Cómo las empresas pueden minimizar el costo de una brecha de seguridad”, el 47 % de las empresas latinoamericanas utiliza algún tipo de tecnología obsoleta dentro de su infraestructura de TI. Esta práctica pone a las compañías en riesgo de sufrir más daños financieros en caso de una brecha de seguridad, un 51 % más para las pymes y un 77 % más para las empresas, en comparación con aquellas que actualizan a tiempo. (Kaspersky, 2021)

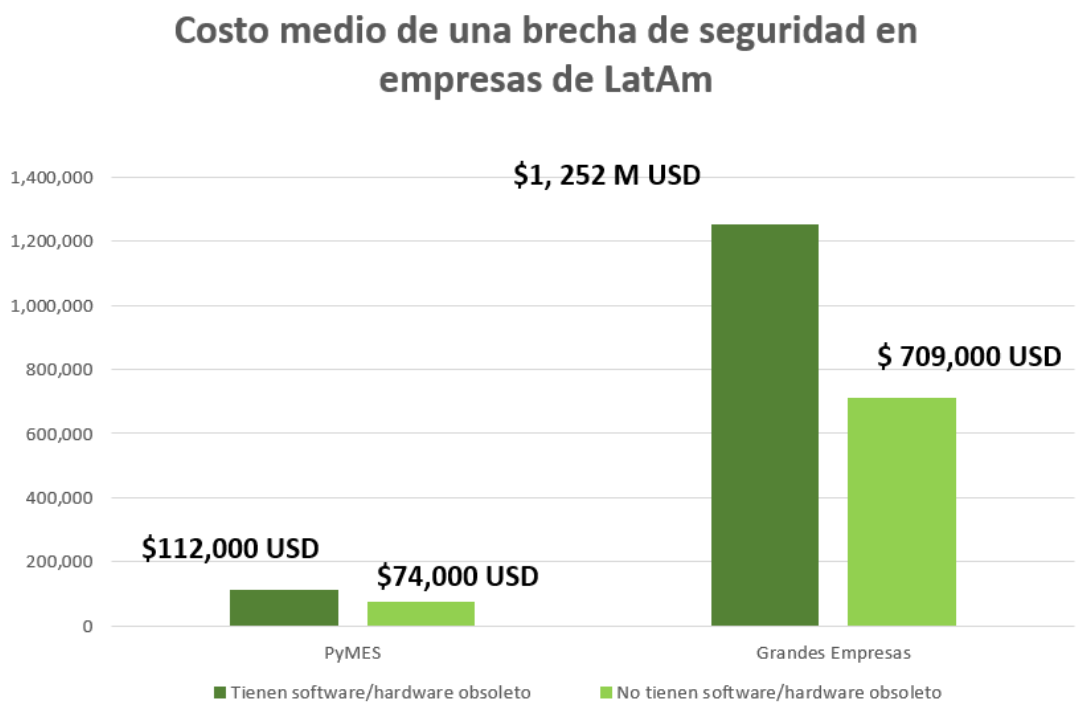


Ilustración 1. Costo medio de una brecha de seguridad en empresas de LatAm, obtenido de Kaspersky, 2021

La Ilustración 1, tomada del informe de Kaspersky, muestra el impacto económico que puede generar una brecha de seguridad en grandes empresas latinoamericanas que utilizan tecnología obsoleta. Esto incluye sistemas operativos sin parches de seguridad, software desactualizado o dispositivos móviles incompatibles. En estos casos, los daños financieros pueden alcanzar un promedio de 1,252,000 dólares, lo que representa un 77 % más que las pérdidas registradas por empresas con tecnología completamente actualizada, cuyo promedio es de 709,000 dólares.

En cuanto a las pequeñas y medianas empresas (pymes) de la región, aquellas que operan con tecnología obsoleta enfrentan un promedio de pérdidas de 112,000 dólares, es decir, un 51 % más que las que mantienen su infraestructura tecnológica al día, cuya media de daños asciende a 74,000 dólares en caso de una brecha de seguridad.

El informe también identifica las principales razones por las cuales las organizaciones no realizan actualizaciones tecnológicas oportunas. Entre las más destacadas se encuentran:

- Incompatibilidad con aplicaciones desarrolladas internamente (49 %): Este factor puede ser crítico para las organizaciones que han desarrollado software a medida para satisfacer necesidades específicas del negocio.
- Resistencia del personal a utilizar nuevas versiones de software (47 %): Muchos empleados enfrentan dificultades para adaptarse a nuevas herramientas y metodologías, lo cual puede traducirse en una menor productividad temporal y rechazo al cambio.

Finalmente, el análisis subraya la importancia de mantener la infraestructura tecnológica actualizada como una medida fundamental para reducir los riesgos financieros derivados de incidentes de ciberseguridad. En este sentido, las empresas deben considerar la actualización de sus sistemas no como un gasto, sino como una inversión estratégica para protegerse de posibles amenazas cibernéticas.

De las razones previamente mencionadas, el caso de estudio abordado en este trabajo la DIT presenta una situación particular: una gran parte de sus desarrollos web transaccionales ha sido

realizada de manera interna. Por otro lado, aproximadamente el 80 % de sus sitios web informativos están construidos sobre CMS ampliamente conocidos, como Drupal o WordPress, los cuales operan con distintas versiones de CMS, sistemas operativos o PHP, especialmente en los sitios externos.

En contraste, los sitios transaccionales suelen desarrollarse utilizando una misma versión tecnológica en la mayoría de los casos. Sin embargo, las prácticas de desarrollo empleadas o la forma en que fueron implementados pueden representar una potencial brecha de seguridad.

Además, en muchas ocasiones, los nuevos desarrollos deben integrarse con sistemas previamente existentes, lo que obliga a mantener compatibilidad con soluciones heredadas. Esta necesidad de adaptación puede limitar la adopción de tecnologías más seguras y actualizadas, y comprometer la protección de los sistemas críticos de la universidad.

2.3 Análisis del problema dentro de la organización

Para entender qué áreas sería necesario involucrar en este proceso, es indispensable entender el cómo se encuentra organizada la DIT de una universidad privada actualmente, lo cual nos lleva a presentar el siguiente organigrama:

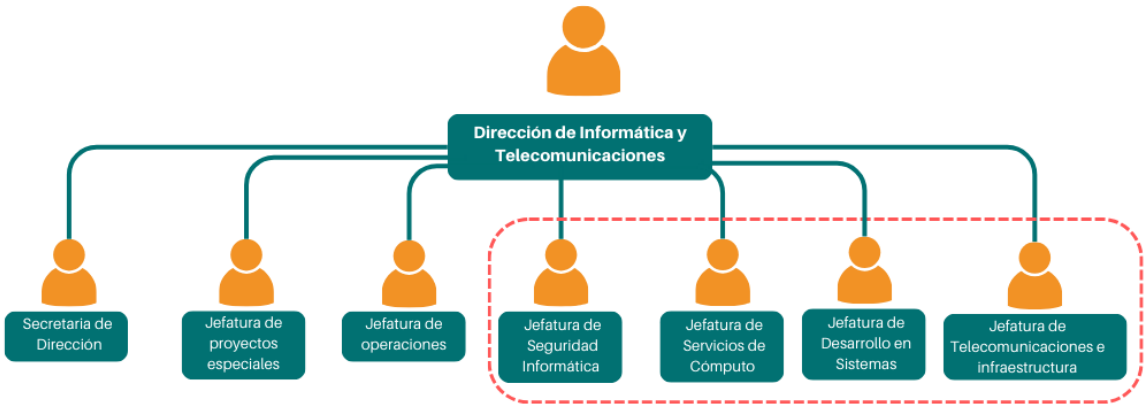


Ilustración 2. Organigrama actual de la DIT

Fuente: Elaboración propia, con apoyo de Canvas

En la Ilustración 2, se puede apreciar que la DIT se puede dividir en seis jefaturas, las cuales abarcan cada uno de los diferentes aspectos, los cuales se enumeran los siguientes:

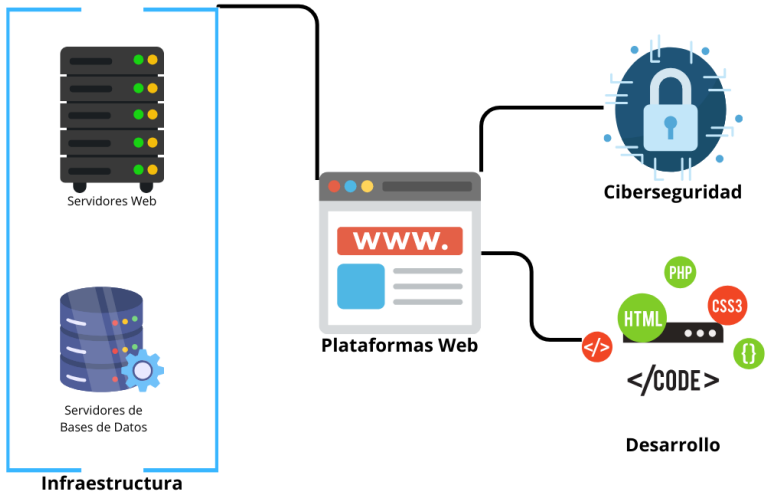
1) Jefatura de proyectos especiales: Se encarga de analizar los requerimientos de nuevas solicitudes dentro de la DIT, así como medir los alcances del proyecto y tiempos de entrega.
2) Jefatura de operaciones: Su función principal es atender las solicitudes de la comunidad, por ejemplo, problemas con las impresoras, o problemas particulares de los sitios web.
3) Jefatura de Seguridad de Informática: Su principal función es la protección de todas las plataformas digitales, no solo web, sino también en la comunicación entre servidores o equipos de cómputo.
4) Jefatura de Servicios de Cómputo: Esta área es de servicio para el área de Desarrollo, ya que le provee apoyo con el soporte de aplicaciones de los sistemas transaccionales y en la realización de pruebas de garantía de calidad (QA, por siglas en inglés *Quiality Assurance).* Estas pruebas aseguran que los sistemas cumplen con los requisitos establecidos. Además, de generar sitios informativos, así como el apoyo con los servidores web y de base de datos, tanto en su mantenimiento, como en su puesta a punta de cada uno.
5) Jefatura de Desarrollo de Sistemas: Su principal función es generar sistemas transaccionales de la universidad, es decir, sistemas que requieran información de la universidad, como nombre, número de cuenta, etc., para facilitar las actividades de la comunidad universitaria.

6) Jefatura de Telecomunicaciones e Infraestructura: Se encarga de proporcionar los servidores requeridos, hacer copias de respaldo de todos los servidores de manera periódica, la conectividad vía Ethernet o Wifi de la universidad, así como el monitoreo de los sitios web.

Tal como se muestra en la imagen anterior, de las seis jefaturas que conforman la DIT, cuatro de ellas participan activamente en la publicación, actualización y mantenimiento de los sitios web, cada una con distintos niveles de involucramiento. Esta participación inicia desde la solicitud o creación del sitio web, ya que actualmente existen dos canales principales para solicitar un nuevo sitio: Servicios de Cómputo o Desarrollo.

Ambos canales terminan por canalizar las solicitudes hacia los equipos adecuados dentro de la DIT, que pueden incluir personal con roles híbridos, como el experto web o los líderes de desarrollo, quienes forman parte tanto del equipo de desarrollo como del de servicios. Estos actores son los encargados de definir el tipo de sitio web a desarrollar, en función del objetivo y del público al que se desea llegar.

En la Ilustración 3 se presenta, de forma simplificada, qué áreas están involucradas en el proceso. A continuación, se describe cómo interactúa cada una de ellas dentro del ciclo de vida de los sitios



web.

Ilustración 3. Áreas involucradas de la DIT

Fuente: Elaboración propia, con apoyo de Canvas.

A continuación, se describen las principales actividades relacionadas con los sitios web que realiza cada una de estas jefaturas:

1. Jefatura de Desarrollo

   Es responsable de construir sitios web dirigidos principalmente a alumnos, personal administrativo o aspirantes que requieren realizar trámites como el pago de colegiaturas, actividades extracurriculares, inscripción a eventos, exámenes, entre otros.
   También se encarga de atender las observaciones del equipo de seguridad, derivadas de escaneos o cambios en políticas de ciberseguridad que puedan afectar el funcionamiento de los sistemas.

2. Jefatura de Servicios de Cómputo (Servidores Web, Plataformas Web, Servidores de base de datos)

   Tiene la responsabilidad de aplicar actualizaciones necesarias relacionadas con parches del sistema operativo y motores de base de datos, con el fin de reducir las brechas de seguridad.

Asimismo, realiza pruebas de aseguramiento de calidad (QA) y colabora en el desarrollo de sitios informativos cuyo objetivo es brindar información general al público en general.

3. Jefatura de Infraestructura (Servidores)

   Proporciona los servidores requeridos para alojar los sitios web y se encarga de aplicar parches y actualizaciones periódicas en los servidores, contribuyendo así a la estabilidad y seguridad de los sistemas.

4. Jefatura de Seguridad (Ciberseguridad)

   Se encarga de habilitar puertos de comunicación, proteger los sitios web y realizar escaneos de seguridad tanto proactivos como bajo demanda. Además, notifica sobre nuevas vulnerabilidades que puedan impactar los desarrollos existentes, como cambios en las versiones de PHP u otros componentes tecnológicos.

Además, la DIT de manera interna tiene diferentes categorías de sus sistemas web, los cuales son:

- ⇒ Micrositios: Sitios web informativos, los cuales su principal función es proporcionar al público en general información relacionada con departamentos o iniciativas, etc.
- ⇒ Sitios transaccionales: Sitios que permiten que la comunidad universitaria inicie sesión y puede llevar a cabo acciones como inscripciones, evaluaciones, firmar recibos de nómina en el caso de los administrativos.
- ⇒ Portales principales: Sitio web principal de la universidad en la que se publica información relevante para los interesados y la comunidad universitaria.

Las categorías también le permiten saber al departamento de seguridad, cuál es el grado de severidad que puede involucrar la protección de los sitios y cuáles son los que pueden ser focos rojos para atacantes, pero esto no quita severidad al resto, puesto que los atacantes pueden estar monitoreando cualquier vulnerabilidad en el ecosistema web de la universidad y en cualquier momento utilizar dicha brecha para saltar entre los sistemas y servidores.

En conclusión, comprender qué áreas deben involucrarse en la gestión, mantenimiento y seguridad de los sitios web institucionales implica, en primer lugar, conocer cómo está estructurada la DIT. De acuerdo con el organigrama presentado, cuatro jefaturas participan de forma directa en el ciclo de vida de los sitios web: Desarrollo, Servicios de Cómputo, Infraestructura y Seguridad.

Cada una de estas áreas desempeña funciones específicas que, en conjunto, garantizan tanto el funcionamiento adecuado como la protección de los sitios web de la universidad. Desde la solicitud y creación del sitio, pasando por su despliegue y mantenimiento técnico, hasta su protección ante vulnerabilidades, la colaboración entre estas jefaturas resulta esencial para mantener una presencia digital segura, funcional y alineada con las necesidades institucionales.

El ecosistema web universitario se compone, además, de diferentes tipos de sitios: micrositios, sitios transaccionales y portales principales, cada uno con públicos, objetivos y niveles de criticidad distintos. Esta clasificación permite a la jefatura de Seguridad priorizar acciones y estrategias de protección, sin dejar de lado que cualquier vulnerabilidad, por mínima que sea, puede convertirse en un punto de entrada para amenazas más complejas que afecten a sistemas críticos.

En este contexto, la coordinación interdepartamental, la estandarización de procesos y la actualización continua de la infraestructura tecnológica se consolidan como pilares estratégicos para reducir riesgos, fortalecer la ciberseguridad institucional y ofrecer servicios digitales confiables y sostenibles a toda la comunidad universitaria.

3. Marco teórico y conceptual

En un entorno donde la tecnología evoluciona de forma acelerada, los ciclos de vida de las herramientas digitales se acortan significativamente, lo que obliga a las organizaciones a adaptarse con rapidez para no perder competitividad. Sin embargo, muchas empresas e instituciones educativas enfrentan una brecha tecnológica considerable, causada por factores como la resistencia al cambio, la falta de capacidades para actualizar desarrollos internos, o la ausencia de estrategias claras para la gestión de su infraestructura tecnológica (Goya Soluciones, s.f.). Esta situación compromete no solo el rendimiento de sus plataformas digitales, sino también su posicionamiento en un mercado que valora la innovación, la seguridad y la eficiencia operativa.

Ante este panorama, la vigilancia tecnológica y la inteligencia tecnológica competitiva emergen como herramientas fundamentales para anticipar tendencias, mitigar riesgos y fortalecer la toma de decisiones estratégicas. Estos enfoques permiten a las instituciones no solo identificar tecnologías emergentes o cambios regulatorios relevantes, sino también analizar su entorno interno y externo a través de metodologías como el análisis FODA, PESTEL y CAME. En este capítulo se presentan los principales conceptos que sustentan la propuesta de esta investigación, así como antecedentes teóricos y casos de aplicación que permiten contextualizar la relevancia de crear un área especializada en la DIT orientada a enfrentar los desafíos de la obsolescencia y fortalecer la gestión de los sitios web institucionales.

3.1 Enfoque conceptual desde la gestión de la innovación tecnológica

La estrategia de innovación ha sido ampliamente reconocida como una herramienta fundamental para el desarrollo organizacional y la adaptación ante escenarios cambiantes. De acuerdo con Henderson (Henderson, 2023), retomando a Cooper y Edgett, una estrategia de innovación efectiva permite alinear los esfuerzos de desarrollo tecnológico y creativo con los objetivos generales de la organización. Esta alineación estratégica facilita una asignación más eficiente de recursos, mejora los procesos de priorización y fortalece la toma de decisiones basada en criterios objetivos y orientados al valor. En este sentido, la planificación estratégica en materia de innovación no solo se limita a definir lineamientos operativos, sino que establece una visión estructurada para fomentar la generación de nuevas soluciones, mejorar la capacidad de respuesta frente a la adversidad y garantizar un crecimiento sostenido en el tiempo.

En la siguiente figura 4, se presentan tres tipos de innovación junto con una breve descripción de cada uno. Cabe destacar que la innovación radical es la más utilizada en las organizaciones. Esto se debe a que ayuda a efectuar cambios en la empresa, en cómo trabaja, sus procesos, en los servicios que ofrece y cómo trata al cliente:

Ilustración 4. Tipos de innovación

Fuente: (SYDLE, 2023)

Teniendo en cuenta lo anterior y centrándose en la estrategia de innovación, la cual puede adoptar diversas formas, de las cuales en este caso se enfocará en la innovación tecnológica, la cual es un proceso en el que la organización puede crear, transformar o mejorar los servicios productos o modelos. Adicionalmente, parte de los beneficios al implementar la innovación tecnológica, se considera la reducción de costos, la cual es el resultado de la mejora o la implementación de métodos eficientes, los cuales logran la optimización de recursos (García, 2023).

Para lograr un proceso de innovación tecnológica que permita impulsar proyectos tecnológicos, tanto en plataformas tecnológicas, herramientas de seguridad y mejores prácticas de desarrollo, así como la optimización de los recursos, se debe utilizar una serie de fases que ayude con lo mencionado anteriormente, es por ellos que en la Universidad, se considera como base el Modelo Nacional de Gestión de Tecnología, dicho modelo tiene como propósito impulsar el desarrollo de las empresas mediante una gestión de tecnología explicita, sostenida y sistemática. (Fundación Premio Nacional de Tecnilogía, 2015). El modelo se compone de actividades o procesos que las organizaciones deben de realizar para la implementación de la innovación tecnológica. Las actividades se agrupan para poder eficientizar la gestión de estas. La agrupación de las actividades se puede categorizar con base en sus funciones.

Otro punto clave del modelo es la integración de la gestión tecnológica con los procesos de la organización, así como los resultados que la misma aporta a la organización con el fin de poder tener un enfoque más centralizado y que permita optimizar la toma de decisiones y la implementación de su tecnología.

¿Cuáles son las funciones del modelo de Gestión de la Tecnología?

Las tareas del modelo de gestión de la tecnología incluyen: "*vigilar, planear, habilitar, proteger e implantar*".

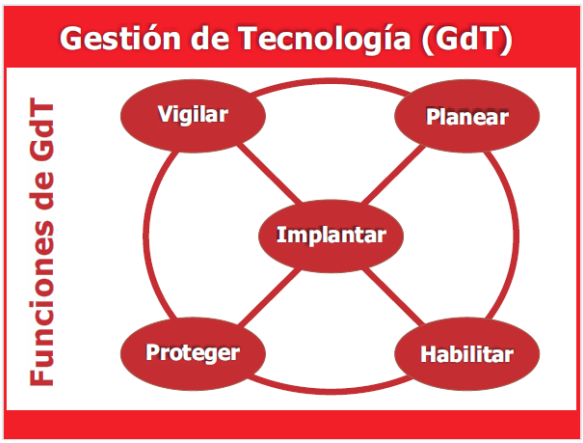


Ilustración 5. Modelo de Gestión de Tecnología (GdT)

Fuente: Premio Nacional de Gestión de Tecnología e Innovación.

Cada una de las funciones se explica en la siguiente tabla:

Tabla 1. Funciones del Modelo de Gestión de Tecnología

Funciones del GDT	Significado
Vigilar	Es la búsqueda en el entorno de señales e indicios que permitan identificar amenazas y oportunidades de desarrollo e innovación tecnológica que impacten en el negocio.
Planear	Es el desarrollo de un marco estratégico tecnológico que le permite a la organización seleccionar líneas de acción que deriven en ventajas

	competitivas. Implica la elaboración de un plan tecnológico que se concreta en una cartera de proyectos.
Habilitar	Es la obtención, dentro y fuera de la organización, de tecnologías y recursos necesarios para la ejecución de los proyectos incluidos en la cartera.
Proteger	Es la salvaguarda y cuidado del patrimonio tecnológico de la organización, generalmente mediante la obtención de títulos de propiedad intelectual.
Implantar	Es la realización de los proyectos de innovación hasta el lanzamiento final de un producto nuevo o mejorado en el mercado, o la adopción de un proceso nuevo o sustancialmente mejorado.

Fuente: Premio Nacional de Gestión de Tecnología e Innovación.

Además de la vigilancia tecnológica, en este trabajo se complementará con la inteligencia tecnológica competitiva. Este último es el proceso de análisis, interpretación, difusión y utilización de la información para la toma de decisiones estratégicas (Herrera-Mendoza, 20223).

Pero ¿qué es lo que hace la vigilancia tecnológica y la vigilancia tecnológica competitiva?, ¿cómo puedo distinguirlos?, ¿cómo pueden ayudar a la DIT? Todo esto se ve con mayor profundidad en los siguientes puntos.

3.1.1 Vigilancia tecnológica

Se denomina Vigilancia tecnológica como el proceso sistemático de recopilación, análisis y difusión de información sobre desarrollos científicos y tecnológicos relevantes para una organización o industria. Su principal objetivo es anticipar los cambios, identificar oportunidades de innovación y reducir los riesgos.

La definición de la Vigilancia Tecnológica se encuentra en la familia de normas UNE 166000, la cual menciona la siguiente definición: (LISA Institute, s.f.)

"Proceso organizado, selectivo y sistemático, para captar información del exterior y de la propia organización sobre ciencia y tecnología, seleccionarla, analizarla, difundirla y comunicarla, para convertirla en conocimiento con el fin de tomar decisiones con menor riesgo y poder anticiparse a los cambios"

De acuerdo con (Herrera-Mendoza, 20223), en donde hace referencia al (FPNTI, 2014), se menciona que la vigilancia tecnológica se realiza mediante los siguientes procesos:

a) Monitoreo tecnológico. Proceso por el cual se identifican tecnologías iguales o similares a las que se pretende desarrollar. Asimismo, en esta fase se encuentran tecnologías que pueden tener diferencias en su forma y en su funcionalidad.
b) El análisis competitivo de las tecnologías encontradas en el monitoreo tecnológico. Especialmente, si puede representar una amenaza actual o potencial en el futuro. El análisis tiene como base las cualidades y debilidades de las tecnologías y se centra en el usuario o cliente que está dispuesto a pagar para utilizarlos.
c) Estudios de mercado y de competitividad. Son medios organizados para analizar e identificar el perfil del usuario, a los competidores y a todos los involucrados que sea relevante. Además, proporciona información relevante sobre las oportunidades y amenazas que estén presentes en la actualidad o en un futuro.

La vigilancia tecnológica (VT) proporciona una ventaja estratégica al permitir la identificación de oportunidades de desarrollo, colaboraciones potenciales y amenazas emergentes. Además, facilita la toma de decisiones basada en datos y la optimización de recursos en proyectos de investigación y desarrollo (I+D).

3.1.1.1 Herramientas para la Vigilancia Tecnológica

Ilustración 6. Herramientas para la VT

Fuente: Elaboración propia, basada en (LISA Institute, s.f.)

Existen diversas herramientas para realizar una VT adecuada, de las cuales se pueden visualizar en la ilustración 6, tal es el caso de los diversos análisis, por ejemplo, el análisis de mercado, el cual permite conocer las tendencias de los usuarios en el mercado en el que se encuentre la organización. El análisis de la competencia, el cual analiza los movimientos de los competidores, así como prevenir cambios en el mercado. Otro tipo de análisis es el de patentes, el cual permite obtener información oportuna de tecnologías emergentes o existentes en las que se puedan adquirir.

El Benchmarking tecnológico consiste en analizar las mejores prácticas de la industria, esto con el fin de utilizarlas en la mejora de la organización.

La minería de textos se basa en las tecnologías emergentes para la búsqueda de conocimientos en una gran colección de documentos no estructurados. Finalmente, las bases de datos son la utilización de información publicada, por ejemplo, revistas especializadas, artículos, etc.

3.1.2 Inteligencia Tecnológica Competitiva

La inteligencia tecnológica competitiva (ITC) es un proceso sistemático de recopilación, análisis y difusión de información sobre avances tecnológicos y tendencias del mercado con el fin de mejorar la toma de decisiones empresariales. Su aplicación permite a las organizaciones anticipar cambios en su entorno, identificar oportunidades de innovación y fortalecer su competitividad. La ITC no solo ayuda a reducir la incertidumbre, sino que también facilita el desarrollo de estrategias basadas en el conocimiento. (Villalpando, 2023)

3.1.3 Ciclo de la Vigilancia tecnológica e Inteligencia Tecnológica Competitiva.

En la figura 6 se muestra el ciclo de vigilancia e inteligencia tecnológica competitiva, que al ser implementado permite realizar un proceso de trabajo enfocado, cíclico, sistematizado y colaborativo, el cual esté compuesto por las siguientes etapas.

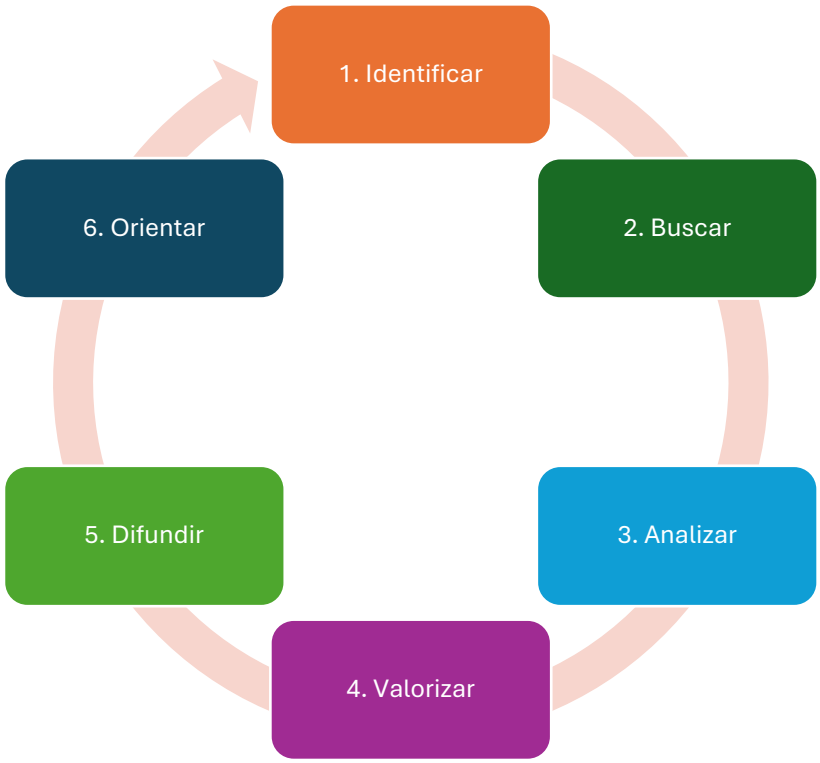


Ilustración 7. Ciclo de la Vigilancia e Inteligencia

Fuente: Elaboración propia con base en (Guía de Vigilancia e Inteligencia Tecnológica, s.f.)

Las etapas del proceso se pueden mostrar en la ilustración 7. Se describirá como:

1.) Diagnóstico y priorización: Se identifican las tecnologías a vigilar y las necesidades de información mediante los Factores Críticos de Vigilancia (FCV) o *Key Intelligence Topics* (KIT). Estos pueden enfocarse en decisiones estratégicas, señales tempranas o actores clave.
2.) Búsqueda y captura de información: Se diseña una estrategia de recopilación de información con objetivos claros, utilizando palabras clave, fuentes relevantes y herramientas digitales para gestionar la sobrecarga informativa.
3.) Análisis de información: Se procesan y filtran los datos mediante herramientas como mapas tecnológicos, software de patentes y gestores bibliográficos para extraer información relevante.
4.) Valorización de información relevante: Se elaboran productos estratégicos como boletines tecnológicos, estudios de mercado o informes de vigilancia para facilitar la toma de decisiones.
5.) Difusión y comunicación: Se establecen estrategias de comunicación interna para distribuir la información y asegurar que toda la organización aproveche los resultados.
6.) Toma de decisiones y acciones: Se interpretan los hallazgos para apoyar la toma de decisiones estratégicas, promoviendo la innovación y la competitividad empresarial.

3.2 La Inteligencia Competitiva y su impacto en la estrategia

De acuerdo con la Agencia de Innovación (BAI Agencia de Innovación., 2007), en la ilustración 8 se puede apreciar la relación perfecta entre el *Businness Intelligence* y la Inteligencia Competitiva, en el cual la diferencia del BI y la IC, se da, ya que el BI da solución a la parte táctica de la organización, a resolver la parte operativa de la organización, a gestionar los recursos internos de la misma, mientras que en la IC, se enfoca en resolver lo que está fuera de la organización, en un entorno desconocido, obteniendo y analizando información relevante para facilitar la toma de decisiones al momento de la incertidumbre, además de considerar la estrategia.

La Agencia de Innovación, también destaca que la parte táctica de una organización puede ser perfecta, pero si su aspecto estratégico no es el correcto, no se podrán alcanzar los objetivos.

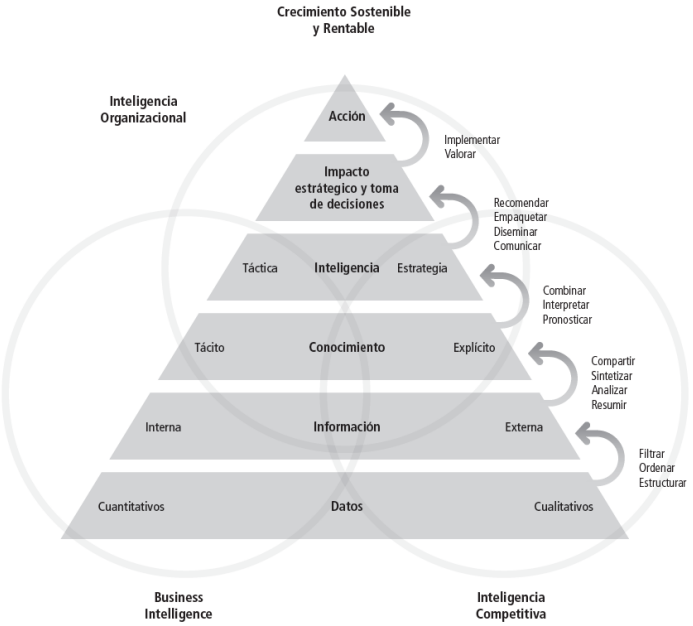


Ilustración 8. Relación entre el Bussiness Intelligence y la Inteligencia Competitiva

Fuente: (BAI Agencia de Innovación., 2007)

3.3 ¿Cuál es el rol de la ITC en la empresa?

De acuerdo con Joshua Henderson, (Villalpando, 2023), el rol de la ITC es:

"La ITC busca proveer conocimiento sobre tecnologías, las actividades de los proveedores y competidores, para su manejo oportuno e influyente.

Típicamente, los esfuerzos de ITC se enfocan en las tecnologías relacionadas con el negocio principal de la empresa y donde hay mayores inversiones de capital.

La ITC no es solamente la recopilación de datos; debe contrastarse la información recopilada con la situación interna de la empresa.

La ITC contempla la búsqueda, recolección y análisis de información técnica de manera sistemática y organizada para su uso oportuno. Su objetivo es dar seguimiento al estado del arte y analizar datos para la toma de decisiones y el reforzamiento de la competitividad de la empresa."

Además, Joshua Henderson (Villalpando, 2023), el cual hace referencia a García Vergara, indica que existen tres tipos de estructuras organizacionales para la ITC, de las cuales se describen a continuación:

Tabla 2 Estructuras organizacionales para ITC

Estructura centralizada	Estructura distribuida	Estructura híbrida
Beneficios: La ITC es una función reconocida por dirección general, lo que la hace	**Beneficios:** Tiene un conjunto de expertos encargados de la recolección y distribución de la información,	**Beneficios:** Combina un sistema formal centralizado con gatekeepers, lo que permite una distribución

acreedora a un presupuesto definido y personal de tiempo completo. Las actividades de ITC están centralizadas, lo que evita duplicar esfuerzos. Se enfoca en la información solicitada por la dirección o el área tecnológica. **Contras:** No permite una participación de varios investigadores o colaboradores, lo que la comunicación puede ser lenta.	lo cual promueve la comunicación dentro de la empresa (llamados gatekeepers). **Contras:** Hay poca integración y coordinación de esfuerzos y es difícil hacer análisis integrales.	de la información y administración de recursos más eficientes. **Contras:** Costos más elevados en comparación con las estructuras centralizadas y distribuida. Requiere grandes esfuerzos para la coordinación, gestión y conexión jerárquica difusa con los otros departamentos de la empresa.

Fuente: (Henderson, 2023)

3.4 Modelos teóricos

Para analizar y abordar la problemática de la obsolescencia tecnológica y la falta de actualización oportuna, se pueden considerar tres modelos teóricos fundamentales:

3.4.1 Modelo de Difusión de Innovaciones

Este modelo explica cómo las innovaciones tecnológicas son adoptadas por individuos y organizaciones en diferentes etapas

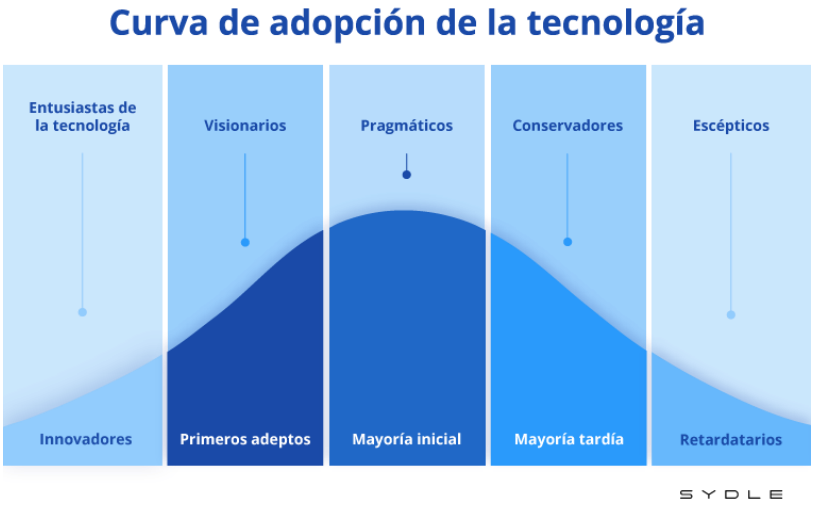


Ilustración 9. Curva de adopción de la tecnología

Fuente: (SYDLE, 2023)

En la ilustración 9 muestra las diferentes etapas de la curva de adopción de la tecnología, en la cual se categoriza por cinco: los innovadores, los primeros adeptos, mayoría inicial, mayoría tardía y retardados. Los innovadores, los cuales representan un 2.5 %, son los primeros en probar nuevos productos, asumiendo riesgos. Los primeros adeptos tienen el 13 %, son también llamados *early adopter*, son más selectivos y crean tendencias haciendo que influya en otros y su toma de decisiones. Mientras que la categoría de la mayoría inicial, que representa el 34 %, son los consumidores de tecnología que esperan la validación de los primeros adeptos antes de decidir elegir un nuevo producto. La mayoría tardía, que representa el otro 34 %, son los más conservadores, esto se debe a que solo aceptan productos cuando están ampliamente adoptados y, por último, los

retardatarios, que son el 16 % restante, son los que adquieren la tecnología cuando es imprescindible. (SYDLE, 2023)

De acuerdo con las categorías antes mencionadas, la universidad se encuentra en la mayoría tardía, ya que prefiere consumir productos que ya tengan un soporte robusto o, en el caso de ser requerido, se tenga una mayor documentación sobre posibles afectaciones al momento de su implementación.

3.4.2 Modelo de COTEC

De acuerdo con (Gtz, s.f.) el modelo de Temaguide, más conocido como modelo de COTECT, fue fundado en 1998, por la Fundación COTEC, el cual consiste en cinco elementos claves que facilitan el proceso de innovación.

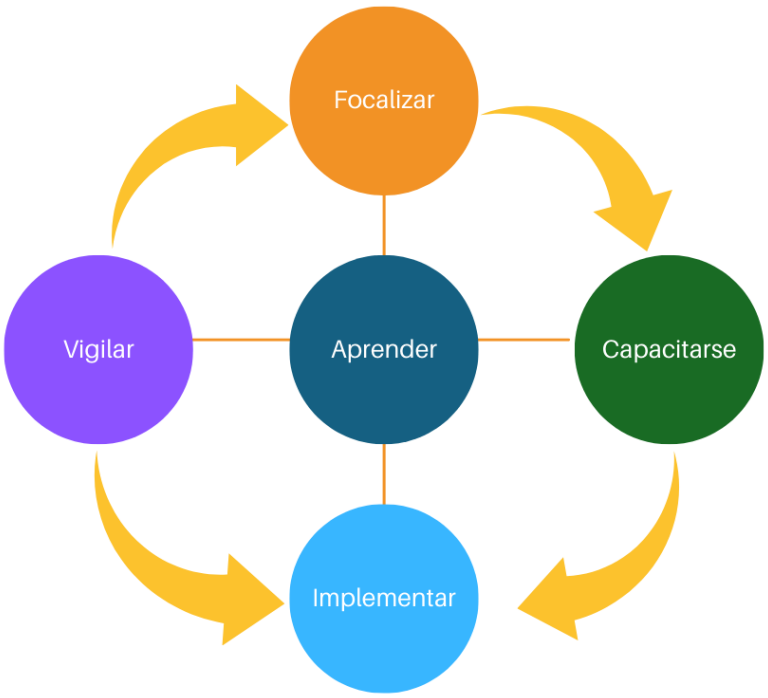


Ilustración 10. Modelo de COTEC

Fuente: Elaboración propia, con base en (Gtz, s.f.)

La ilustración 10 muestra los pasos del modelo de COTEC. Su primera fase es la **vigilancia**, en este paso se observa el entorno externo e interno de la organización, esto con el fin de identificar las necesidades de innovación y las oportunidades potenciales. Dentro de los de las señales que se pueden mencionar son: cambios o nuevas legislaciones, nuevas demandas de los consumidores, avances tecnológicos, etc. En la segunda fase se tiene la **focalización**, la cual se dirigen los esfuerzos hacia estrategias específicas de innovación que fortalezcan la ventaja competitiva y le ayuden en su posicionamiento en el mercado.

La fase de **capacitación** es donde consiste en adquirir y gestionar el conocimiento necesario para el desarrollo de la alternativa seleccionada, esto con el fin de que la organización cuente con la capacidad necesaria para llevar a cabo la innovación en la fase de **implementación**, esta etapa abarca desde la generación de ideas hasta el lanzamiento del producto o servicio al mercado, así como también la incorporación de nuevos procesos en la organización.

En la fase del **aprendizaje**, implica la difusión del conocimiento adquirido a partir de experiencias previas, lo que permite visualizar puntos de mejora y generar nuevos procesos. Es fundamental que el aprendizaje sea continuo para mantener la competitividad de la organización y el desarrollo de nuevos productos, servicios o negocios.

La filosofía del modelo de COTEC es “organización que aprende”, destacando la importancia de la adaptación y la mejora continua en la gestión de la tecnología y la innovación.

3.4.3 Modelo de Vigilancia Tecnológica según Norma UNE 166.006

La Norma UNE 166.006, en el año 2018 sufre una actualización (Obsera, Observatorio Tecnológico UA, s.f.), esto con el fin de mejorar la gestión de los sistemas de vigilancia e inteligencia en la organización como parte de la gestión de la investigación (I), desarrollo (D) e innovación (i), denominada gestión de la I+D+i. Su objetivo es estandarizar procesos y terminologías para facilitar la toma de decisiones estratégicas en un entorno en el que el cambio es constante.

El enfoque de esta versión es la captura, análisis, difusión y uso estratégico de la información, esto con el fin de anticipar los cambios, reducir los riesgos e identificar las oportunidades de innovación.

La Norma se compone de cinco etapas, que se describen a continuación:

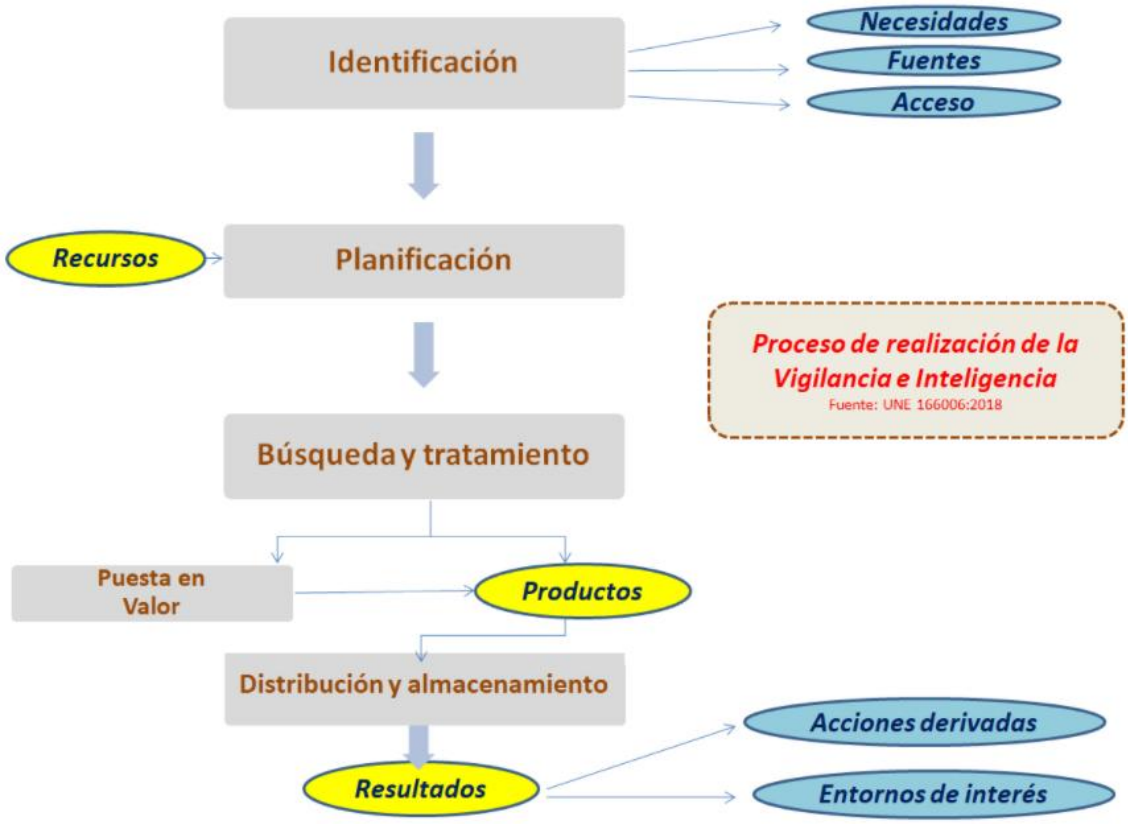


Ilustración 11. Modelo de vigilancia tecnológica Norma UNE 166.006. 2018

Fuente: (Ardiles Briones, 2021)

En la ilustración 11 se muestran dichas etapas, las cuales se pueden definir como (Ardiles Briones, 2021):

1) Identificación y planificación: En esta etapa se definen los objetivos de la vigilancia tecnológica, las áreas de interés. Además de identificarse las principales fuentes de información, así como los recursos disponibles que tiene la organización.
2) Búsqueda y tratamiento: Se recopila la información relevante mediante diversas fuentes, posteriormente se evalúa la pertinencia, fiabilidad, relevancia y calidad de la información, tomando en cuenta la opinión de los expertos. Finalmente, el tratamiento o validación,

permitirá seleccionar los datos que cumplen con los requisitos de fiabilidad, oportunidad y utilidad para la toma de decisiones.

3) Puesta de valor: En esta etapa se requiere un análisis más profundo, que pueden acaparar desde expertos de diversas áreas que evalúan la información recolectada para identificar oportunidades, reducir riesgos e impulsar la innovación, alineándolo a la estrategia organizacional.
4) Distribución y almacenamiento: En esta etapa, la organización define los formatos de distribución de la información, según sean las necesidades, clasificándolos en:

    a. Bajo análisis: Alertas, noticias y RSS.
    b. Análisis medio: Boletines, informes, estudios biográficos y de patentabilidad
    c. Análisis profundo: Informes detallados y estudios estratégicos para la toma de decisiones.

5) Resultados: La información que se obtuvo y el proceso se convierte en conocimiento estratégico, permitiendo que la organización se anticipe a cambios y a su vez reducir riesgos en la toma de decisiones.

Cabe destacar que este modelo garantiza que la VT sea un proceso sistemático y eficiente, el cual está alineado a los objetivos estratégicos de la organización.

3.5 Modelo de vigilancia e inteligencia de Godet

En el artículo “MICHEL GODET: EL PROSPECTIVISTA DE LA PROSPECTIVA Y LA PERMANENTE EFECTIVIDAD DE SU MÉTODO EN EL SIGLO XXI. ", publicado en la revista TAMBARA, (Armijos Ortega, 2019) se aborda el modelo de prospectiva estratégica desarrollado por Michel Godet, en el cual destaca la relevancia y aplicación en el ámbito empresarial.

El modelo de vigilancia e inteligencia de Godet, basado en la prospectiva estratégica, es un enfoque muy poderoso para que las organizaciones se puedan anticipar al futuro y, así, preparar decisiones estratégicas en escenarios inciertos.

En la ilustración 12, se muestran las técnicas que ayudan con el modelo de vigilancia e inteligencia de Godet.

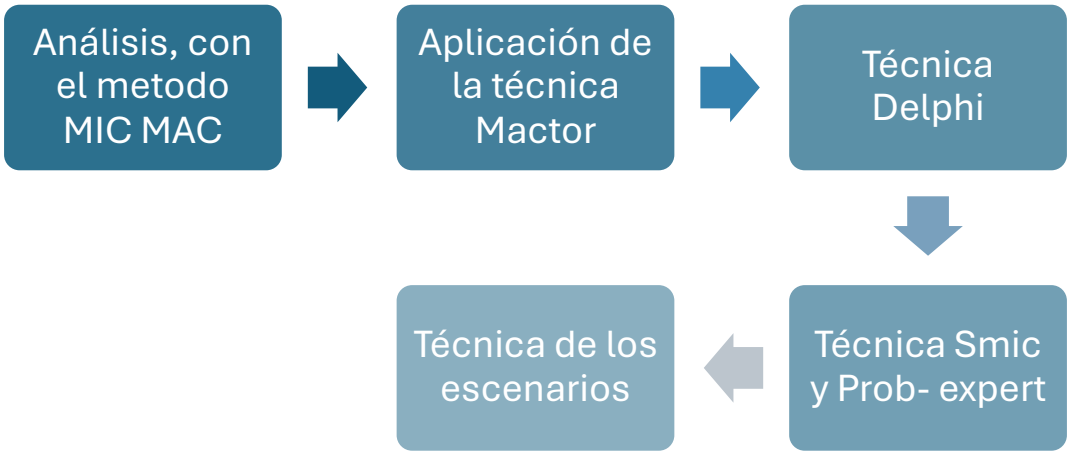


Ilustración 12. Técnicas para los estudios prospectivos

Fuente: Elaboración propia, con base a (Armijos Ortega, 2019)

La descripción de cada una de las técnicas se presenta a continuación:

Método MIC MAC (Matriz de Impactos Cruzados-Multiplicación Aplicada a una Clasificación)

De acuerdo con el artículo anteriormente mencionado (Armijos Ortega, 2019), este método se analiza las diferentes variables de entorno que influyen, cuáles son sus dependencias y la relación entre ellas. Para ello, se divide en tres fases, las cuales son:

- ⇒ Fase uno, lista de las variables: En esta fase, se enlistan todas las variables, tanto externas como internas, las cuales se obtienen de entrevistas con las personas involucradas en los procesos.
- ⇒ Fase dos, la descripción de las relaciones entre ellas: En esta fase, participan las personas que definieron la lista en la fase uno, esto con el objetivo de que entre los mismos categoricen, qué detona y cuáles con las variables consecutivas.
- ⇒ Fase tres: Identificación de variables claves: En esta fase, con base en los análisis previos, se puede identificar cuáles son las variables que son fundamentales considerarse, gracias a estos análisis y pueden ver incluso variables que no se tenían contempladas.

Técnica Mactor

En primera instancia, se define como Matriz de Alianzas y conflictos: tácticas, objetivos y recomendaciones. En una definición simple y concreta, se toma como base la propuesta en el artículo de Armijos Ortega, del 2019.

"*Es una herramienta que permite valorar las diferentes posturas de los actores y poder analizar divergencias y convergencias para guiar la toma de decisiones. (Rivera & Malaver, 2006) (p.263)."*

Las etapas que componen la técnica Mactor son 5 fases (Armijos Ortega, 2019):

"Fase 1. Definir los actores e identificar la estrategia

Fase 2. Establecer la matriz de posiciones, es decir, situar a cada actor en relación

con los objetivos.

Fase 3. Realizar la matriz de posiciones evaluadas, es decir jerarquizar los objetivos

para cada actor y evaluar la relación de fuerza de los actores.

Fase 4. Reconocer las convergencias y divergencias entre actores.

Fase 5. Formular las estrategias y finalmente las preguntas claves del futuro (Rivera

& Malaver, 2006) (p.269)."

Técnica Delphi

De acuerdo con (Velázquez, s.f.), el modelo de Delphi es una técnica de comunicación desarrollada para obtener información y opiniones cualitativas de manera sistemática e interactiva, basada en la consulta a un panel de expertos.

Dentro de sus características principales se encuentra el anonimato de los participantes, ya que los expertos no conocen la identidad de los demás, haciendo que las respuestas proporcionadas sean honestas y sin interferencias tales como la jerarquía o personas dominantes. Además, se realiza un itinerario de rondas, lo que permite a los participantes revisar y ajustar sus respuestas basándose en el resumen de las respuestas del grupo anterior. Con las respuestas proporcionadas al finalizar cada una de las rondas, se les proporciona a los expertos un resumen, lo que les facilita la reflexión y a realizar el ajuste de opiniones en las siguientes rondas, lo que proporciona una retroalimentación controlada.

Asimismo, sucede la agregación de respuestas. Las cuales son analizadas y sintetizadas para identificar consensos y divergencias, proporcionando una visión colectiva del tema en cuestión.

Técnica Smic y Prob- expert

Esta técnica se refiere a los métodos de impacto cruzados probabilistas, cuyo objetivo es evaluar los cambios en las probabilidades que se definieron. Esto se realiza mediante hipótesis, las combinaciones de estas y la vigilancia estrecha de dichas (Prospektiker, 2007), además, se cuenta con apoyo de expertos para el descarte de hipótesis. Esta técnica consta de tres fases (Armijos Ortega, 2019):

- Fase 1, hipótesis: En esta fase se realiza el planteamiento de 5 o 6 hipótesis fundamentales y algunas hipótesis complementarias. El cómo son seleccionadas estas hipótesis es mediante la elección correcta de las variables principales.
- Fase 2, elección de expertos**:** Se selecciona a las personas expertas que son las que se deben de formular las preguntas correctas para la selección de los posibles escenarios más adecuados. Para este paso, se debe considerar un mes mínimo, y el número de expertos debe superar los 100 y se les pide que se categorice de la siguiente manera (Prospektiker, 2007):
  - "*Evaluar la probabilidad en la que es simple de realización de una hipótesis desde una probabilidad 1 (muy débil) hasta una probabilidad 5 (acontecimiento muy probable).""*
  - *"Evaluar bajo forma de probabilidad condicional la realización de una hipótesis en función de todas las demás (en este caso la nota 6 significa la independencia de las hipótesis); habida cuenta de todas las preguntas que el experto debe plantearse, se le exige revelar la coherencia implícita de su razonamiento."*
- Fase 3, evaluación de los escenarios posibles: En esta etapa se establece qué escenarios son los más probables que ocurran, esto utilizando el programa de SMIC (programa clásico de minimización de una forma cuadrática con límites lineales). Dicho programa permite el análisis del grupo de expertos, ya que permite la corrección de los expertos para así obtener resultados coherentes, que permitan ser utilizados para las estadísticas de escenarios y de esta manera posicionar las hipótesis y sus escenarios. En la ilustración 13, se da una muestra de dicho software.

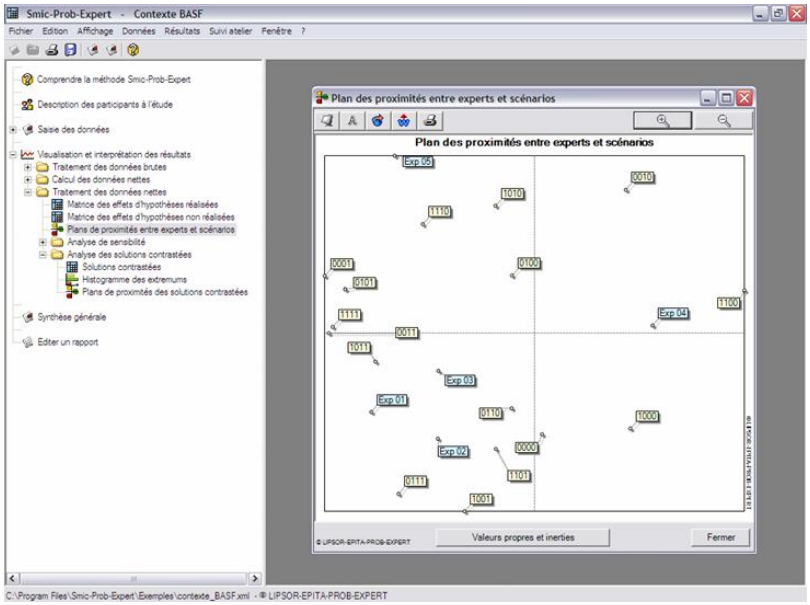


Ilustración 13. programa SMIC-PROB-EXPERT

Fuente: (Prospektiker, 2007)

Técnica de los escenarios

La técnica de los escenarios se enfoca en construir todos los escenarios posibles, las consecuencias que este tendría y el camino que conduce a este. Para ello, se debe tener en claro que es un escenario, Goret (como lo sitio en Prospeltiker, 2007), indicó que:

"Un escenario es un conjunto formado por la descripción de una situación futura y de la trayectoria de eventos que permiten pasar de una situación origen a una situación futura."

Con base en la definición Goret, propone dos tipos de escenarios, (Armijos Ortega, 2019):

- Exploratorios: Se originan a partir de tendencias históricas y actuales, conduciendo a futuros plausibles.
- Previas o regulaciones: Estos se diseñan con base en las representaciones alternativas del futuro: estos pueden ser deseables o no. Además, se representa como modo retrospectivo. También se debe considerar que, mediante las evoluciones, los escenarios pueden ser tendenciosos o contrastados.

Para la elaboración de dichos escenarios se deben considerar 3 fases, las cuales son (Prospektiker, 2007):

- Fase 1. Construir la base: Se lleva a cabo un análisis profundo de cómo está la organización, tanto de manera externa como de manera interna, para lo cual es conveniente delimitar el análisis, así como las variables esenciales, además de analizar las estrategias que cada actor puede realizar.
- Fase 2. Identificar variables y reducir la incertidumbre: Una vez identificadas las variables claves y analizados los juegos de los actores, es posible construir las hipótesis, así como su importancia. Es por ello por lo que es importantes las técnicas antes mencionadas y que se ven en una representación gráfica en la ilustración 14.
- Fase 3. Elaboración e implementación de los escenarios: En esta etapa se planean los escenarios y objetivos a alcanzar. Es necesario describir la estrategia que se llevará a cabo en cada situación, así como su análisis correspondiente, para posteriormente proceder con la toma de decisiones.

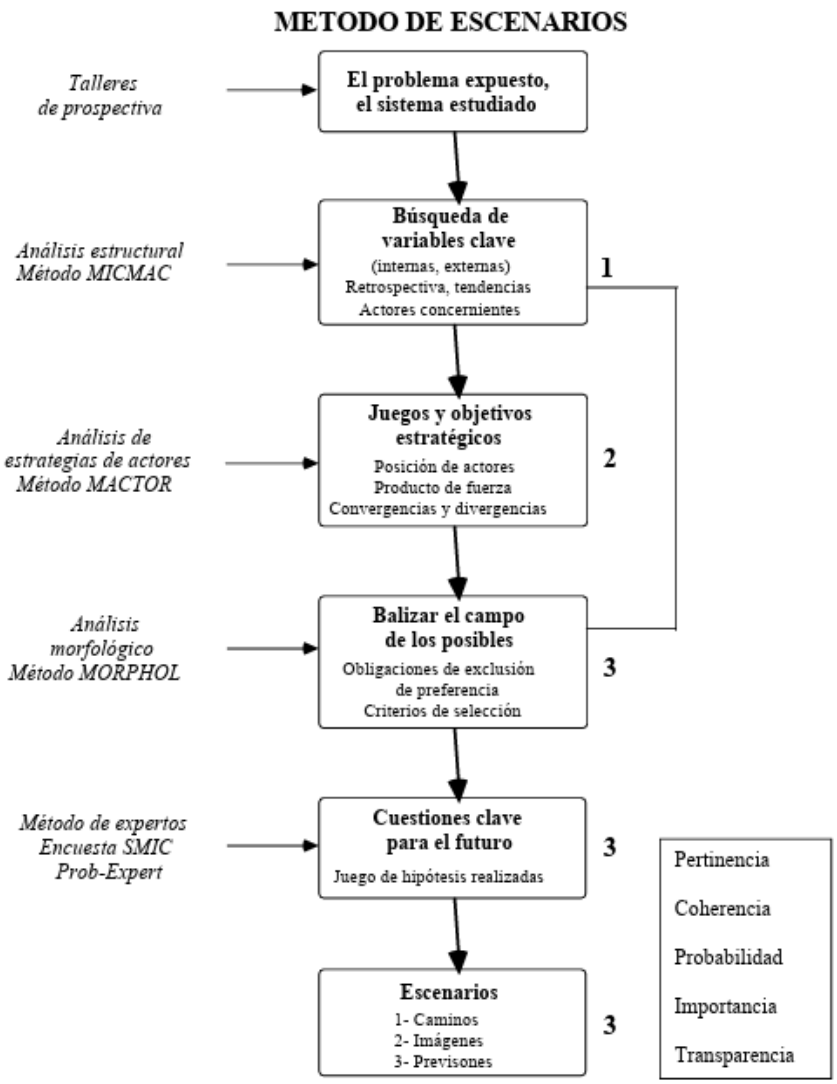


Ilustración 14. Metodo de escenarios

Fuente: (Prospektiker, 2007)

3.6 Casos documentados

Dentro de las investigaciones realizadas para esta tesis, se identificaron tres casos relevantes en los que la implementación de estrategias de vigilancia e inteligencia tecnológica competitiva permitió a diferentes organizaciones enfrentar problemáticas específicas relacionadas con la innovación, la toma de decisiones estratégicas y la adaptación tecnológica. Los casos muestran que herramientas especializadas pueden contribuir de forma significativa al fortalecimiento organizacional, al permitir la identificación oportuna de amenazas y oportunidades en entornos complejos y cambiantes.

La vigilancia tecnológica y la inteligencia competitiva se han consolidado como prácticas clave para transformar información dispersa del entorno científico, tecnológico y comercial en conocimiento estratégico. La aplicación de estas metodologías en distintos sectores como el educativo, el

energético y el financiero ha facilitado la anticipación a cambios del mercado, la mitigación de riesgos operativos, y la optimización de recursos. En esta sección se presentan tres estudios de caso documentados, cuyo análisis permite extraer aprendizajes relevantes para sustentar la propuesta de creación de un área especializada dentro de la Dirección de Innovación Tecnológica (DIT) de la universidad.

3.6.1 Caso 1: Vigilancia Tecnológica en el sector Financiero (Gutiérrez, Cidei, 2023)

En el caso de éxito presentado por Cidei sobre la implementación de vigilancia tecnológica en el sector financiero, se identificó una problemática central que impulsó esta iniciativa: las instituciones enfrentaban una creciente dificultad para adaptarse a los acelerados cambios tecnológicos, responder a las amenazas en ciberseguridad y mantener su competitividad frente a un entorno altamente dinámico. Esta situación evidenció la necesidad de contar con mecanismos sistemáticos que permitieran anticipar tendencias, detectar riesgos emergentes y aprovechar oportunidades de innovación.

Las entidades financieras se encontraban ante múltiples desafíos: la detección temprana de innovaciones disruptivas, la comprensión de las expectativas cambiantes de los clientes, la presión por cumplir normativas en constante evolución y la necesidad de vigilar las estrategias de la competencia. Además, el aumento en la frecuencia y sofisticación de ciberataques y fraudes representaba una amenaza crítica para la seguridad operativa y la confianza de los usuarios.

Frente a este contexto, la implementación de la vigilancia tecnológica se consolidó como una herramienta estratégica clave. A través de un proceso sistemático de monitoreo, recopilación, análisis y difusión de información relevante del entorno, las instituciones pudieron fortalecer su capacidad de toma de decisiones con base en datos actualizados y fiables.

Entre los principales beneficios derivados de esta práctica, destacan los siguientes:

- Identificación de oportunidades y tendencias emergentes: La vigilancia tecnológica permitió a la institución financiera mantenerse al tanto de soluciones innovadoras, tecnologías disruptivas y cambios regulatorios. Esta capacidad de anticipación le otorgó ventajas competitivas al permitirle actuar antes que sus competidores frente a nuevas dinámicas del mercado.

- Mejora de la experiencia del cliente: Al analizar comportamientos y preferencias de los usuarios, se identificaron áreas de mejora en productos y servicios. Esto permitió una mayor personalización de la oferta, alineándola con las expectativas reales de los clientes y mejorando su nivel de satisfacción.

- Análisis estratégico de la competencia: La vigilancia constante del entorno competitivo proporcionó información clave sobre las acciones y posicionamientos de otras instituciones. Esto permitió evaluar fortalezas y debilidades internas, identificar brechas de mercado y sustentar decisiones estratégicas con mayor precisión.

- Gestión de riesgos y amenazas: La identificación anticipada de riesgos, especialmente en temas de ciberseguridad y fraudes, facilitó la elaboración de estrategias preventivas. Esto fortaleció la protección de los activos digitales, así como la confianza de los usuarios en la seguridad de sus operaciones financieras.

- Cumplimiento normativo oportuno: Dado que el sector financiero opera bajo estrictas regulaciones, la vigilancia tecnológica permitió identificar de manera temprana nuevas normativas y adaptarse a ellas de forma oportuna. Esto no solo evitó sanciones, sino que también reforzó la reputación institucional en cuanto a cumplimiento y responsabilidad.

En síntesis, la vigilancia tecnológica no solo respondió eficazmente a la problemática inicial detectada, sino que también permitió transformar esa debilidad en una fortaleza competitiva. Su implementación ayudó a las instituciones financieras a enfrentar un entorno cambiante con mayor preparación, agilidad y visión estratégica.

3.6.2 Caso 2: Inteligencia Tecnológica Competitiva para fortalecer la Innovación (Petróleo, 2017)

En el documento titulado “Inteligencia Tecnológica Competitiva para fortalecer la innovación”, publicado por el Instituto Mexicano del Petróleo (IMP), se identifica una problemática central que motivó la implementación de estrategias de vigilancia tecnológica: la necesidad de mejorar los procesos de toma de decisiones en un entorno energético nacional caracterizado por cambios acelerados en la estructura de la industria, en las regulaciones y en la evolución de tecnologías competidoras. La apertura del mercado derivada de la Reforma Energética incrementó el interés de diversas empresas en invertir recursos en nuevas tecnologías y servicios dirigidos a resolver problemáticas específicas del sector energético nacional. No obstante, la carencia de un sistema estructurado para transformar información no sistematizada proveniente de fuentes científicas, tecnológicas y comerciales en conocimiento útil para la toma de decisiones dificultaba la planificación tecnológica y la adquisición de soluciones adecuadas.

Ante esta situación, el IMP formalizó la aplicación de la inteligencia tecnológica competitiva mediante la creación de su Unidad de Inteligencia Tecnológica Competitiva, establecida originalmente en 1998 con el Programa Estratégico de Inteligencia Tecnológica. Esta unidad se convirtió en un pilar fundamental para mejorar los procesos decisionales, brindando asesoría tanto a Petróleos Mexicanos (Pemex) en sus procesos de adquisición y planeación tecnológica, como a la Secretaría de Energía (Sener) en la definición de planes tecnológicos para nuevas iniciativas, como los Centros Mexicanos de Innovación en Energía (CEMIEs). La aplicación de metodologías como los mapas de ruta tecnológicos y el método Delphi permitió acelerar los procesos de innovación, reducir la incertidumbre en decisiones estratégicas y garantizar que los resultados generaran valor conforme a los objetivos establecidos.

El documento también aborda el Proceso de Innovación, estructurado en cuatro fases principales, como se muestra en la Ilustración 15:

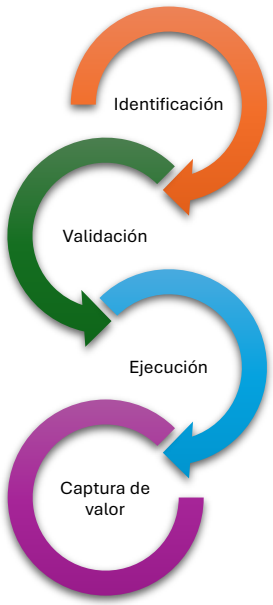


Ilustración 15. Fases del Proceso de Innovación

Fuente: Elaboración propia, con base a (Petróleo, 2017)

- Fase de **identificación de oportunidades**: En esta etapa se generan insumos para detectar tecnologías o productos ya disponibles en el mercado, así como para identificar innovaciones potenciales. Para ello, se emplean metodologías como los mapas de rutas tecnológicas y el método Delphi.
- Fase de **validación**: Se evalúa el valor comercial de las innovaciones identificadas, utilizando el análisis de casos de negocio.
- Fase de **ejecución**: Se lleva a cabo el monitoreo continuo del entorno con el fin de adaptarse oportunamente a cambios tecnológicos y regulatorios.
- Fase de **captura de valor**: Finalmente, se implementan estrategias comerciales y ejercicios de *benchmarking* que permiten comparar la oferta del IMP frente a productos o servicios existentes en el mercado.

Gracias a la experiencia acumulada por la Unidad de Inteligencia Tecnológica Competitiva, y al conocimiento especializado en gestión de tecnología, el IMP ha logrado consolidar esta función como una línea de negocio estratégica, fortaleciendo así la competitividad del sector energético nacional, particularmente en el ámbito de los hidrocarburos. Para un mejor entendimiento de qué son los mapas de rutas tecnológicas, se describen a continuación:

¿Qué es un mapa de ruta tecnológico?

Un mapa de ruta tecnológico es una herramienta que ayuda a planear estratégicamente el uso de tecnología en una empresa o sector. (miro, s.f.) Además, entre sus beneficios se encuentran que proporciona un camino claro para la empresa, alinea los equipos, ayuda a la toma de decisiones y motiva al equipo.

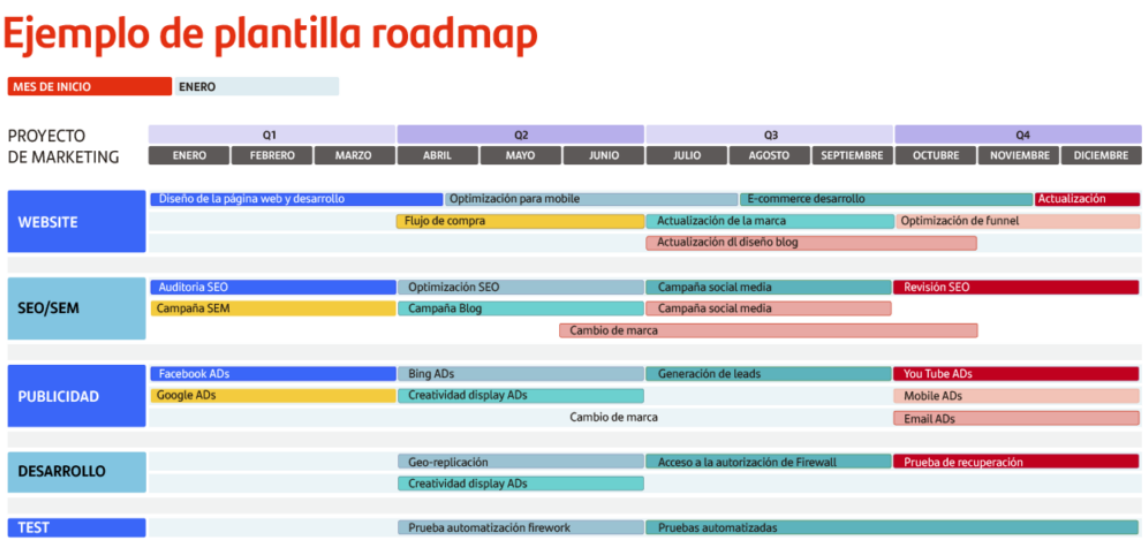


Ilustración 16. Ejemplo de plantilla, ruta tecnológica

Fuente: (Roadmap: Qué es, tipos y cómo hacerlo, 2024).

La ilustración 16, es un ejemplo del cómo se realiza una ruta tecnológica, en el cual se muestra los equipos a los que pertenece que actividad, así como las fechas en las que se tiene prevista la realización de cada una de ellas.

3.6.3 Caso 3: Caso de éxito: Análisis de vigilancia tecnológica e inteligencia competitiva en el sector de las criptomonedas (e-intelligent, 2022)

El artículo “Caso de éxito: Análisis de vigilancia tecnológica e inteligencia competitiva en el sector de las criptomonedas” presenta un estudio colaborativo entre e-intelligent y la Universidad Politécnica de Madrid (UPM), cuyo objetivo fue analizar el impacto actual y las tendencias futuras de las

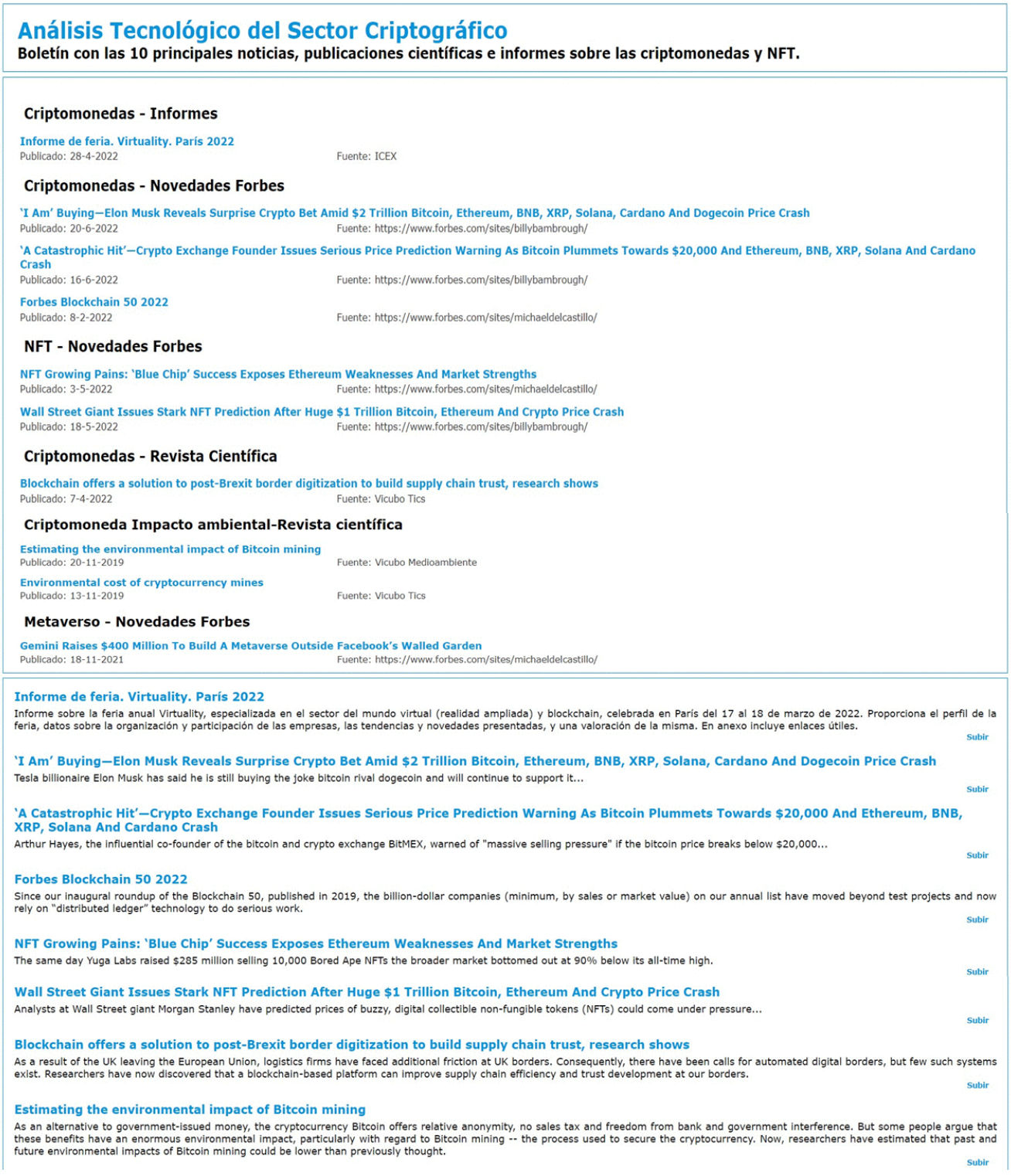
criptomonedas en la economía global. La necesidad de implementar vigilancia tecnológica surgió a partir de una problemática clara: el sector de las criptomonedas se caracteriza por su alta volatilidad, rápida evolución tecnológica, escasa regulación y abundancia de fuentes de información dispersas y de calidad variable. Este entorno dificultaba la toma de decisiones estratégicas fundamentadas y exigía una sistematización del conocimiento emergente. Para abordar esta situación, e-intelligent proporcionó a la UPM su plataforma **Vicubo Cloud**, a través de la cual se diseñó un Observatorio Tecnológico de Criptomonedas. Este observatorio permitió automatizar procesos clave como la filtración de información, la priorización de contenidos relevantes, el análisis estructurado de tendencias y la mejora en la calidad de los datos utilizados para el estudio. Gracias a esta solución, se logró superar las limitaciones derivadas de las búsquedas aleatorias y se facilitó una visión clara y analítica del entorno competitivo, permitiendo anticipar oportunidades y amenazas en un sector altamente dinámico.

La metodología del estudio que se aplicó fue la siguiente:

1) Recopilación de la información
    a. Se seleccionaron exhaustivamente diversas fuentes, incluyendo patentes, artículos científicos, revistas y portales especializados, para obtener diversos datos de los avances tecnológicos, encuestas, opiniones y cotizaciones relacionadas con las criptomonedas
2) Análisis realizado:
    a. Análisis del mercado criptográfico: En este análisis se evaluó la posición de las criptomonedas en el mercado financiero, así como el impacto en la economía mundial, su aceptación social, así como también el ámbito de los tokens no fungibles (NFT, por sus siglas en inglés *Non -Fungible Token*).
    b. Análisis tecnológico criptográfico: Se llevó a cabo el estudio del desarrollo y posición de las tecnologías de las criptomonedas y criptoarte, en el cual se identifican las principales líneas de investigación en curso.
    En la Ilustración 17, se puede visualizar parte del análisis de la Vigilancia Tecnológica realizado para este caso.

    c. Análisis competitivo: En este análisis se detectan las fuerzas externas, tales como la baja regulación y análisis de empresas líderes en criptomonedas y NFT.

Además, en dicho análisis se identificaron las principales tendencias de las criptomonedas, su crecimiento en el sector financiero, su adopción geográfica, el perfil de los usuarios y la publicación de las patentes. Asimismo, se destacó la necesidad constante de la vigilancia tecnológica y la inteligencia competitiva, esto para comprender la evolución del sector criptográfico y los futuros avances, manteniendo así la competitividad en el ámbito en el que se tienen cambios constantes.



Análisis Tecnológico del Sector Criptográfico

Boletín con las 10 principales noticias, publicaciones científicas e informes sobre las criptomonedas y NFT.

Criptomonedas - Informes

Informe de feria. Virtuality. París 2022
Publicado: 28-4-2022 Fuente: ICEX

Criptomonedas - Novedades Forbes

'I Am' Buying—Elon Musk Reveals Surprise Crypto Bet Amid $2 Trillion Bitcoin, Ethereum, BNB, XRP, Solana, Cardano And Dogecoin Price Crash
Publicado: 20-6-2022 Fuente: https://www.forbes.com/sites/billybambrough/

'A Catastrophic Hit'—Crypto Exchange Founder Issues Serious Price Prediction Warning As Bitcoin Plummets Towards $20,000 And Ethereum, BNB, XRP, Solana And Cardano Crash
Publicado: 16-6-2022 Fuente: https://www.forbes.com/sites/billybambrough/

Forbes Blockchain 50 2022
Publicado: 8-2-2022 Fuente: https://www.forbes.com/sites/michaeldelcastillo/

NFT - Novedades Forbes

NFT Growing Pains: 'Blue Chip' Success Exposes Ethereum Weaknesses And Market Strengths
Publicado: 3-5-2022 Fuente: https://www.forbes.com/sites/michaeldelcastillo/

Wall Street Giant Issues Stark NFT Prediction After Huge $1 Trillion Bitcoin, Ethereum And Crypto Price Crash
Publicado: 18-5-2022 Fuente: https://www.forbes.com/sites/billybambrough/

Criptomonedas - Revista Científica

Blockchain offers a solution to post-Brexit border digitization to build supply chain trust, research shows
Publicado: 7-4-2022 Fuente: Vicubo Tics

Criptomoneda Impacto ambiental-Revista científica

Estimating the environmental impact of Bitcoin mining
Publicado: 20-11-2019 Fuente: Vicubo Medioambiente

Environmental cost of cryptocurrency mines
Publicado: 13-11-2019 Fuente: Vicubo Tics

Metaverso - Novedades Forbes

Gemini Raises $400 Million To Build A Metaverse Outside Facebook's Walled Garden
Publicado: 18-11-2021 Fuente: https://www.forbes.com/sites/michaeldelcastillo/

Informe de feria. Virtuality. París 2022
Informe sobre la feria anual Virtuality, especializada en el sector del mundo virtual (realidad ampliada) y blockchain, celebrada en París del 17 al 18 de marzo de 2022. Proporciona el perfil de la feria, datos sobre la organización y participación de las empresas, las tendencias y novedades presentadas, y una valoración de la misma. En anexo incluye enlaces útiles.
Subir

'I Am' Buying—Elon Musk Reveals Surprise Crypto Bet Amid $2 Trillion Bitcoin, Ethereum, BNB, XRP, Solana, Cardano And Dogecoin Price Crash
Tesla billionaire Elon Musk has said he is still buying the joke bitcoin rival dogecoin and will continue to support it...
Subir

'A Catastrophic Hit'—Crypto Exchange Founder Issues Serious Price Prediction Warning As Bitcoin Plummets Towards $20,000 And Ethereum, BNB, XRP, Solana And Cardano Crash
Arthur Hayes, the influential co-founder of the bitcoin and crypto exchange BitMEX, warned of "massive selling pressure" if the bitcoin price breaks below $20,000...
Subir

Forbes Blockchain 50 2022
Since our inaugural roundup of the Blockchain 50, published in 2019, the billion-dollar companies (minimum, by sales or market value) on our annual list have moved beyond test projects and now rely on "distributed ledger" technology to do serious work.
Subir

NFT Growing Pains: 'Blue Chip' Success Exposes Ethereum Weaknesses And Market Strengths
The same day Yuga Labs raised $285 million selling 10,000 Bored Ape NFTs the broader market bottomed out at 90% below its all-time high.
Subir

Wall Street Giant Issues Stark NFT Prediction After Huge $1 Trillion Bitcoin, Ethereum And Crypto Price Crash
Analysts at Wall Street giant Morgan Stanley have predicted prices of buzzy, digital collectible non-fungible tokens (NFTs) could come under pressure...
Subir

Blockchain offers a solution to post-Brexit border digitization to build supply chain trust, research shows
As a result of the UK leaving the European Union, logistics firms have faced additional friction at UK borders. Consequently, there have been calls for automated digital borders, but few such systems exist. Researchers have now discovered that a blockchain-based platform can improve supply chain efficiency and trust development at our borders.
Subir

Estimating the environmental impact of Bitcoin mining
As an alternative to government-issued money, the cryptocurrency Bitcoin offers relative anonymity, no sales tax and freedom from bank and government interference. But some people argue that these benefits have an enormous environmental impact, particularly with regard to Bitcoin mining -- the process used to secure the cryptocurrency. Now, researchers have estimated that past and future environmental impacts of Bitcoin mining could be lower than previously thought.
Subir

Ilustración 17. Análisis Tecnológico del Sector Criptográfico

Fuente: "Análisis de Vigilancia Tecnológica e Inteligencia Competitiva en el Sector de las Criptomonedas" de la Universidad Politécnica de Madrid/, Janet Fernández Ibáñez. Vicubo Cloud.

3.7 Conclusión del capitulo

A partir del análisis detallado de conceptos como la vigilancia tecnológica, la inteligencia competitiva, la innovación estratégica y la obsolescencia tecnológica, se evidencia que el entorno digital actual exige respuestas institucionales organizadas, sistemáticas y basadas en datos. Estas respuestas deben permitir una toma de decisiones informada frente al dinamismo del cambio tecnológico y a la creciente complejidad en la gestión de infraestructuras web, especialmente en instituciones con alta dependencia tecnológica, como las universidades.

La vigilancia tecnológica se define como un proceso organizado y permanente de recolección, análisis y difusión de información del entorno científico, tecnológico y competitivo, cuyo objetivo es generar conocimiento útil para la toma de decisiones estratégicas. Esta herramienta se convierte en un recurso fundamental para instituciones que, como las universidades, dependen de plataformas digitales funcionales, seguras y actualizadas para mantener su competitividad, cumplir su misión educativa y responder adecuadamente a las demandas de su comunidad. Complementariamente, la inteligencia tecnológica competitiva permite contextualizar los hallazgos obtenidos por medio de la vigilancia, incorporando dimensiones clave como el análisis del mercado, las tendencias regulatorias, el comportamiento de competidores y la prospectiva tecnológica.

Lejos de tratarse de procesos técnicos aislados, tanto la vigilancia como la inteligencia tecnológica constituyen herramientas estratégicas orientadas a la gestión del conocimiento organizacional. En el caso particular de las universidades, su aplicación adquiere una relevancia crítica, dada la creciente dependencia de sus ecosistemas digitales. Estos abarcan desde la comunicación externa (sitios institucionales, portales de aspirantes, subsitios de eventos y departamentos) hasta procesos internos fundamentales como la inscripción académica, evaluación docente y administrativa, y servicios de gestión. La ausencia de un sistema de vigilancia tecnológica estructurado conlleva consecuencias importantes: actualizaciones reactivas, acumulación de riesgos de ciberseguridad, procesos ineficientes y una mayor exposición a la obsolescencia tecnológica.

Un valor adicional de este capítulo reside en la presentación de casos documentados en los que distintas organizaciones, una universidad pública latinoamericana, una institución financiera y el Instituto Mexicano del Petróleo, han implementado exitosamente estrategias de vigilancia e inteligencia tecnológica para enfrentar desafíos concretos, tales como la dispersión de plataformas, la falta de actualización tecnológica o la necesidad de responder en contextos altamente regulados y competitivos. Estos casos demuestran que la implementación de tales estrategias no está limitada a grandes corporaciones; por el contrario, pueden adaptarse a distintos contextos institucionales, siempre que exista voluntad organizacional y se cuente con una estructura adecuada para su ejecución. Herramientas como Vicubo Cloud, o la creación de observatorios tecnológicos institucionales, han resultado claves para dar seguimiento a tendencias emergentes, gestionar eficazmente el conocimiento interno y anticipar los ciclos de obsolescencia de tecnologías críticas.

Finalmente, los casos analizados permiten destacar una constante esencial: las decisiones tecnológicas de alto impacto no deben tomarse de forma aislada ni improvisada, sino con base en información sistematizada, verificada y contextualizada. Ya sea para llevar a cabo la migración de un CMS obsoleto, implementar nuevas medidas de ciberseguridad o seleccionar proveedores tecnológicos, contar con inteligencia tecnológica no solo fortalece la autonomía institucional, sino que también reduce el margen de error, optimiza los recursos disponibles y mejora significativamente la eficiencia del gasto, tanto en instituciones públicas como privadas.

4. Alternativas de solución

Con base a la investigación realizada en la sección anterior, se puede considerar que las siguientes metodologías son las más adecuadas con respecto a lo que se quiere lograr con este trabajo:

- Modelo de Vigilancia Tecnológica según Norma UNE 166.006
- Modelo de COTEC.
- Modelo Nacional de Gestión de Tecnología e Innovación

Además de tener en cuenta el proceso de innovación del IMP, es importante indicar que la DIT se encuentra en dos grupos del modelo de difusión de innovaciones: la mayoría inicial y la mayoría tardía. Esto se debe a que la universidad prefiere adaptar tecnologías que ya hayan sido probadas, que tengan soporte y sobre las cuales se cuente con información suficiente, especialmente para mitigar los riesgos de vulnerabilidad que pueda implicar.

Para tomar la mejor decisión de que tipo de modelo es el ideal para la DIT, o que parte de este puede ser de gran utilidad, es importante conocer cuáles son las restricciones y limitaciones de cada uno, es por ello por lo que en los siguientes subtemas se enlistarán dichas restricciones, todas enfocadas en la implementación enfocado solo en las áreas de páginas web, las cuales son:

- Jefatura de Telecomunicaciones e Infraestructura: Crear y proporciona los servidores adecuados con la versión de sistemas operativos requeridos, ya sea Linux o Windows, así como realizar periódicamente en Windows la actualización de parches. Además de programar, de acuerdo con las necesidades que se requiera, respaldos completos o parciales de cada servidor, así como el almacenamiento de estos por un tiempo determinado. Otra de las actividades que realizan son la asignación de una dirección de protocolo de internet (IP) para los sitios balanceados, así como hacer el registro en los Sistemas de Nombre de Dominio o por sus siglas en inglés *Domain Name System,* DNS externos e internos de la universidad.
- Jefatura de Desarrollo en Sistemas: Desarrolla, mantiene y modifica los sitios web transaccionales de la universidad, los cuales están desarrollados con lenguajes de programación tal como Coldfusion, PHP, ASPNET, React, etc.
  Tales lenguajes también van evolucionando y cada nueva versión tiene funciones obsoletas que son sustituidas por nuevas o inclusive que desaparecen es importante mantenerse bien informado sobre dichos cambios, además cada uno de ellos va orillando a que los desarrolladores apliquen mejores prácticas y lógica en los desarrollos para no hacerlos vulnerables ante atacantes.
- Jefatura de Seguridad Informática: En el caso de la ciberseguridad, dado que es un gran espectro todo lo que protege de la universidad y sus diferentes aplicativos, así como la protección de datos personales, en este caso se toma como consideración las siguientes áreas:
  - Escaneaos de vulnerabilidad, los cuales se realizan en dos momentos del desarrollo de los sitios, la primera vez es previo a la publicación de los sitios y no se publica algún sitio sin que pase por la aprobación del equipo de seguridad, el segundo momento es periódicamente, ya que las páginas alojadas en la infraestructura Ibero son escaneadas de manera periódica para así detectar de manera oportuna nuevas vulnerabilidades o brechas de seguridad.
  - Agentes de seguridad: A cada servidor otorgado por el equipo de infraestructura se le coloca un agente de qué seguridad con las políticas adecuadas al uso se les dará a los servidores. Por ejemplo, en los servidores de bases de datos, las políticas que se le aplican son diferentes a los servidores web.
  - Protección de puertos: Los servidores por default tienen todos los puertos habilitados y solo se habilitan los necesarios para la publicación de los sitios, así como habilitar los protocolos de comunicación entre el equipo encargado de administrar los sitios y el servidor.
  - Protección de las páginas web: aquí el equipo se encarga de que los sitios web no sean propensos a que se les incruste código malicioso, lo que provocaría que los sistemas se vean comprometidos.

- Jefatura de Servicios de Cómputo: Se encarga de adecuar, implementar y de monitorear que los servidores web y servidores de base de datos funcionen de manera adecuada, así como de la instalación de los aplicativos utilizados por el equipo de desarrollo. Además, de desarrollar, dar, mantenimiento, actualizar y aplicar medidas de seguridad a los micrositios de la universidad, con CMS tales como WordPress, Drupal o desarrollos con PHP, HTML, PYTHON, etc.
  Adicionalmente, apoya con las pruebas de QA y tiene un grupo especializado que se encarga de darle soporte a los sitios web transaccionales, esto con la finalidad de que el equipo de desarrollo continúe con la mejora continua.

En cualquiera de los modelos a considerar, se deben contemplar dichas áreas, por lo cual existen limitaciones generales, las cuales afectarían en las decisiones de la DIT para que el modelo o la creación de un modelo propio se implemente de manera adecuada. Dichas restricciones son:

- Económico
- Personal
- Tiempo

4.1 Restricciones o limitaciones del Modelo de Vigilancia Tecnológica según Norma UNE 166.006

Dado que este modelo está basado en la norma UNE 166.006, podría en algún momento la DIT perder el verdadero objetivo de la vigilancia tecnología para la universidad y su desarrollo web, lo que los obligaría a estar más atentos por cumplir con los lineamientos que se tengan que cumplir, así como las modificaciones que se realicen. Además, la vigilancia tecnológica es una tarea que requiere que tenga continuidad y una actualización constante, por lo que el encontrar tecnología que cumpla con lo requerido por la Norma puede reducir las posibilidades dado que la norma puede funcionar como una guía para la adquisición de nueva tecnología y no permitiendo ver evaluar nuevas posibilidades de tecnología o en su defecto cambios que impacten a la universidad.

Además, para que se aplique de manera adecuada se requiere personal capacitado o contratar personal especializado. Esto le llevará a la DIT a estar en una curva de adaptación, tanto para tener los elementos necesarios y saber cómo aplicar la norma de manera adecuada. Así como también llevar a cabo las evaluaciones y mediciones sin generar sesgos en la toma de decisiones a la hora de seleccionar las tecnologías, aplicaciones o mejoras que se van a implementar.

Otra de las restricciones que se podría tener, son las prioridades de cada jefatura, por ejemplo, para ciberseguridad, su prioridad puede cambiar dependiendo de nuevos ataques que hagan que requieran más atención en otro punto, restando o dejando de un lado la vigilancia, mientras que para el área de servicios de cómputo puede tener una mayor relevancia, es por ello que coordinar todas las jefaturas y que sus prioridades se vuelvan colaborativas la una con la otra puede ser un gran desafío, empezando con la coordinación de los mismos y poner las prioridades claramente establecidas.

Una limitación sería que la Norma no se aplicaría sola, se requiere ser complementada por otras normas que le ayuden a reforzar y mejorar la vigilancia tecnología, tales como la Norma ISO 27001 que su enfoque es la seguridad de la información o también las Directrices de Accesibilidad para el Contenido Web o por sus siglas en inglés WCAG (*Web Content Accessibility Guidelines*) que su principal objetivo, es aplicar herramientas para que los sitios web puedan ser accesibles para personas con capacidades diferentes, tales como visuales o auditivos.

4.2 Restricciones o limitaciones del Modelo COTEC

El Modelo COTEC es una herramienta utilizada por organizaciones para estructurar la capacitación, análisis y gestión de información. Pero la aplicación de esta puede presentar ciertas restricciones y limitaciones que pueden afectar la efectividad en la DIT, sobre todo en el desarrollo web y lo que esto implica.

Una de las limitaciones que tiene el modelo es que tiene un enfoque general, lo que implica que sería necesario un tiempo considerable para adaptarlo a las necesidades específicas de la Vigilancia

Tecnológica y la Inteligencia Tecnológica Competitiva, en el sector de plataformas web. Además, debido a la falta de directrices, no se contarían con pautas claras para la recolección de información.

Otra de las limitaciones que se tiene que considerar como importante es la necesidad de contar con personal capacitado en el análisis de la información, así como el procesamiento de esta, esto debido a que se podría tener una gran cantidad de información y el tiempo en el que se demora en poder tomar una decisión alineada a la estrategia de la DIT.

En sectores dinámicos como el desarrollo web, el modelo COTEC puede resultar poco flexible debido a su enfoque estructurado. Las metodologías ágiles, utilizadas en este sector, requieren una adaptación rápida a cambios y novedades, lo que podría verse afectado por la rigidez del modelo.

Por último, la aplicación del modelo depende de fuentes externas de información, muchas de las cuales pueden tener restricciones de acceso o requerir inversiones significativas. En industrias de evolución acelerada, la dificultad para obtener información relevante en tiempo real puede afectar la toma de decisiones estratégicas.

4.3 Restricciones o limitaciones del Modelo Nacional de Gestión de Tecnología e Innovación

En primer lugar, el modelo tiene un enfoque estructurado y normativo, lo que puede dificultar su adaptabilidad a sectores específicos como el desarrollo web o las tecnologías emergentes. Su rigidez metodológica puede hacer que su implementación sea compleja en entornos dinámicos que requieren respuestas rápidas a los cambios del mercado y la tecnología.

Otra limitación es la necesidad de contar con recursos especializados. La correcta aplicación del modelo requiere equipos con conocimientos en gestión tecnológica, investigación y desarrollo, así como en estrategias de innovación. Esto puede representar una barrera para organizaciones con capacidades limitadas en estas áreas, especialmente pymes o *startups*.

El procesamiento y acceso a la información tecnológica también supone un desafío. La implementación del modelo depende de la disponibilidad de datos actualizados y relevantes, lo cual puede verse afectado por la falta de acceso a bases de datos especializadas o la ausencia de una cultura organizacional orientada a la vigilancia tecnológica.

Asimismo, el modelo puede resultar incompatible con metodologías ágiles utilizadas en sectores como el desarrollo web. La rigidez en sus procedimientos puede generar retrasos en la adopción de nuevas tecnologías y dificultar la experimentación rápida, un factor clave en ecosistemas innovadores.

Por último, la aplicación del modelo depende de regulaciones y normativas nacionales, lo que puede generar dificultades en empresas que operan en mercados globales donde las políticas de innovación pueden diferir. Esta dependencia regulatoria podría ralentizar la adopción de tendencias tecnológicas internacional

4.4 Comparativa de modelos

En la tabla 3, se realiza la comparación de los modelos para tener una mejor visión para seleccionar la o las mejores opciones para la DIT.

Tabla 3 Comparación de Modelos de Innovación y Gestión Tecnológica

Criterio	Modelo de Vigilancia Tecnológica (UNE 166.006)	Modelo de COTEC	Modelo Nacional de Gestión de Tecnología e Innovación
Enfoque principal	Gestión sistemática de la información tecnológica y del entorno.	Promoción de la innovación en empresas y sectores productivos.	Desarrollo y gestión de tecnología e innovación a nivel nacional.
Objetivo	Identificar oportunidades tecnológicas y tendencias de mercado.	Impulsar la cultura de innovación y la competitividad.	Establecer un marco para gestionar tecnología e innovación en organizaciones.
Metodología	Recopilación, análisis y difusión de información tecnológica.	Basado en experiencias y buenas prácticas de empresas innovadoras.	Estructura procesos de gestión tecnológica desde la idea hasta la comercialización.
Aplicabilidad	Empresas que requieren vigilancia tecnológica para la toma de decisiones.	Empresas de diversos sectores, especialmente PYMES.	Organizaciones con enfoque en I+D+i, particularmente en sectores estratégicos.
Ventajas	- Proporciona información clave para la toma de decisiones. - Basado en estándares internacionales.	- Flexible y adaptable a distintos sectores. - Fomenta la cooperación entre empresas y centros de innovación.	- Estructura clara para la gestión de tecnología. - Permite la articulación entre gobierno, empresas y academia.
Limitaciones	- Alto costo de implementación. - Dependencia de herramientas especializadas.	- Modelo más general, requiere adaptación a cada empresa. - Menos énfasis en digitalización.	- Falta de reconocimiento internacional. - Depende de políticas gubernamentales y financiamiento público.
Tiempo de implementación	Mediano a largo plazo, depende del sector y herramientas utilizadas.	Corto a mediano plazo, dependiendo del nivel de madurez de la empresa.	Mediano a largo plazo, requiere compromiso institucional.
Dependencia de Recursos Públicos	Baja. Se puede implementar en empresas privadas de forma independiente.	Media. Se basa en cooperación público-privada.	Alta. Depende de las políticas de innovación del gobierno.

Énfasis en comercialización	Bajo. Se centra en la obtención de información, no en la venta de tecnología.	Medio. Busca fomentar la innovación, pero no está enfocado en la comercialización.	Alto. Considera la transferencia de tecnología y su impacto en la economía.

Fuente: Adaptado de ChatGPT (2025) con información propia.

La selección de estos modelos se realizó mediante la observación del cómo trabaja la DIT actualmente y cuales se podrían ajustar de una mejor manera al ritmo de trabajo, para que la curva de aprendizaje y ajuste de esta sea del menor tiempo posible.

4.5 Alternativa de la solución

La Gestión de Tecnología tiene una gran relevancia, esto debido a que su oportuna implementación logra que las empresas tengan una notoriedad en el mercado en el que participen, es por ello por lo que la DIT tiene la necesidad de aplicar dicho modelo, comenzando por realizar una vigilancia tecnológica, que permita identificar amenazas y oportunidades, alineados con la visión de la empresa, lo que permitirá asignar los recursos de manera adecuada.

En el análisis anterior, todos los modelos tienen una característica, se pueden moldear a lo que requiere la empresa, esto puede ser como bien se dijo, una limitante y a la vez una ventaja, ya que se puede alinear a lo requerido por parte del departamento de la DIT, además de considerar que tipo de innovadores es donde la DIT se siente cómodo para la aplicación de esta.

Parte de la solución es adecuar las características de los diferentes modelos y tomarlos y adecuarlos a lo requerido por la DIT, lo que da como resultado el modelo de la ilustración 18.

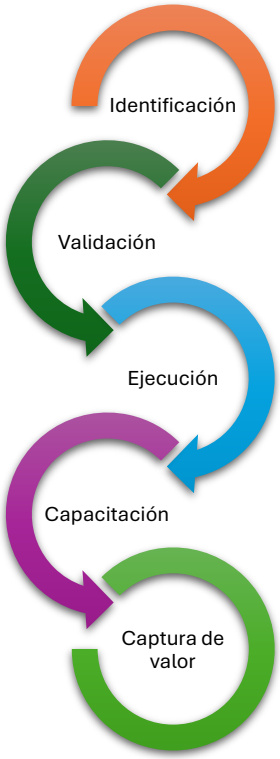


Ilustración 18. Modelo propuesto para la DIT

Fuente: Elaboración propia basada en el modelo de IMP (Petróleo, 2017)

La DIT no cuenta con un grupo de trabajo especializado para realizar la VT, enfocada en la Inteligencia tecnológica competitiva, por lo cual el primer paso previo al modelo a aplicar es buscar dentro del mismo departamento y en mercado laboral, los elementos adecuados, es importante que no todos los recursos humanos sean nuevos dentro de la DIT, ya que el aprender cómo funciona la DIT, cuáles son sus dolencias, cuáles son sus oportunidades, etc. puede ser una curva grande de aprendizaje lo cual puede llevar un tiempo considerado, en el caso de que sea todo el equipo dentro de la DIT, es importante que las personas sean personas claves que puedan aportar al proyecto y permitan ver las tecnologías que requieren un enfoque, así como impulsar el cómo se puede aplicar dicho modelo.

En el cual se tendrían 5 pasos genéricos, los cuales son:

- Identificación: En esta fase la DIT, llevará a cabo trabajo continuo de monitoreo de cambios tecnológicos en el mercado de las universidades, además de efectuar diferentes análisis, sobre todo dos análisis, los cuales son, el análisis de FODA y como complemento un análisis de CAME, dichos análisis permitirán de manera oportuna tener estrategias y desarrollo de planes basados en las fortalezas, debilidades, oportunidades y amenazas de la DIT.

  Además, se definirán los objetivos de la vigilancia y la inteligencia tecnológica competitiva, así como identificar las principales fuentes de información y los recursos que se tienen en la DIT, así como los recursos económicos, humanos, operativos que se requieran de la universidad.

- Ejecución: En esta etapa, la DIT tendrá que obtener las tecnologías y recursos necesarios para la ejecución de los proyectos, dichas tecnologías, así como la obtención de quienes impartan, en caso de ser necesario, el cómo manejar dicha tecnología o plataformas.

- Capacitación: En esta fase, la DIT adquiere y gestiona el conocimiento para el manejo de las plataformas o tecnologías seleccionadas, esto con el fin de que el personal que lo requiera pueda sacar el mayor beneficio posible.

- Captura de valor: En esta fase, la DIT, mediante infografías, en caso de ser necesario, compartirá con la comunidad universitaria el cómo puede utilizar las nuevas herramientas. Asimismo, se realizará un *benchmarking* para comparar las alternativas tecnológicas que proporciona la universidad en comparación con sus competidores en el mercado.

Adicionalmente, la aplicación de normas tecnológicas depende de las tecnologías involucradas, especialmente aquellas relacionadas con la ciberseguridad. En este sentido, tanto la universidad como la mayoría de las empresas deben enfocarse en cómo proteger a los usuarios y los datos que ingresan a los sistemas, evitando que sean vulnerables a posibles ciberdelincuentes. Esto incluye riesgos como robo de identidad, datos personales, entre otros. No solo se protegen a los sistemas que utilizan los usuarios, sino todo el ecosistema digital, ya que un sistema vulnerable puede convertirse en una puerta de entrada para los delincuentes, comprometiendo así la seguridad del entorno digital de la universidad.

La metodología de trabajo que se utilizará en este trabajo se basará en el sistema de Inteligencia Tecnológica Competitiva. (Henderson, 2023), la cual se describe en la ilustración 19.

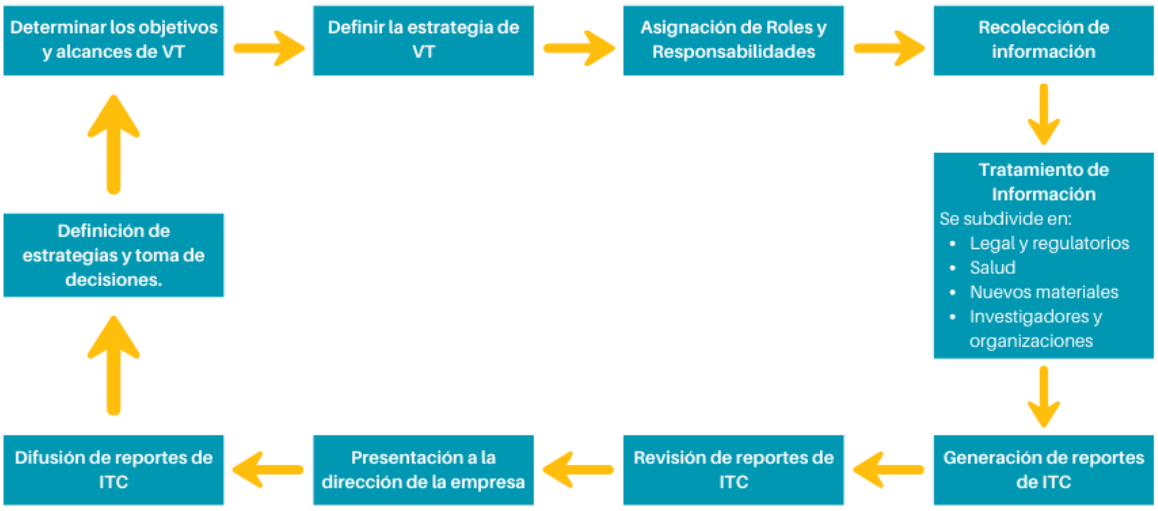


Ilustración 19. Sistema de ITC

Fuente: Elaboración propia basada en (Henderson, 2023)

Pero ¿Cómo la DIT aplicaría lo anteriormente mencionado?, con la creación de una unidad híbrida de VT e ITC, lo que permitiría la participación de diferentes participantes que permitirían aportar y filtrar la información de manera adecuada, todo esto orientado a los alcances y objetivos que se definan en un inicio de cada ciclo.

Para la formación de la unidad de VT e ITC, debe considerar los siguientes factores:

- ⇒ Contar con el Vo. Bo. Por parte de la dirección de la DIT, así como de las jefaturas que se verían involucradas, para lo cual se les dará a conocer qué es la vigilancia tecnológica, la inteligencia tecnológica competitiva, las diferencias entre ambas y cómo pueden beneficiar a la DIT.
- ⇒ El recurso humano que conforme la unidad debe contar con los conocimientos y experiencia para llevar a cabo las actividades, en caso de que no se tengan dichos elementos dentro de la DIT se pueden considerar capacitar a los participantes seleccionados o contratar los elementos necesarios para que se cuente con dicho personal.
- ⇒ Considerarse el uso de plataformas para realizar de manera continua la VT para estar informados sobre nuevas tendencias, plataformas, mejoras en los lenguajes de programación o, en su caso, nuevos lenguajes que faciliten la creación de sitios web.
- ⇒ Motivar al equipo que se ve involucrado en los sitios web a estar atentos a las nuevas tendencias y que expongan por qué les gustaría experimentar con dicha tecnología.
- ⇒ Contar con ambientes de pruebas que permitan fallar rápido en la aplicación de nuevas plataformas, lenguajes, etc.
- ⇒ La unidad debe generar reportes con datos fidedignos que permitan fomentar la confianza en los datos obtenidos, para así tomar la mejor decisión.

Otros factores que se deben considerar para el éxito de la unidad son:

- ⇒ Identificar las necesidades de los usuarios y categorizarlos por el tipo de usuario, por ejemplo: académicos, administrativos, departamentos, programas, convenios con otras universidades.
- ⇒ Identificar el público objetivo que tienen los sitios web, los cuales se pueden encontrar en las siguientes categorías: académicos, administrativos, estudiantes, público en general o comunidad universitaria.
- ⇒ Contar con un mínimo de dos fuentes de información, relacionadas con lo requerido.

- ⇒ Recurrir a información sobre métricas de Google, como lo son *TAG Manager, Analytics*, etc., que proporcionan información relevante con respecto al comportamiento de los usuarios dentro de las plataformas digitales.
- ⇒ Contar con un canal de comunicación entre la unidad de VT e ITC y el equipo de la DIT.
- ⇒ La unidad de VT e ITC, debe considerarse para tomas de decisiones estratégicas en el desarrollo, mantenimiento y actualización de los sitios web de la universidad.
- ⇒ Las jefaturas involucradas, así como la dirección, deben considerar los tiempos de advertencias proporcionados por la unidad.
- ⇒ La unidad realizará seguimiento a las alertas emitidas para que sean atendidas de manera oportuna.
- ⇒ La unidad debe categorizar las fuentes de información de acuerdo con tipo de fuente, credibilidad de estas y fecha de publicación.
- ⇒ Además, tanto la unidad como su modelo de trabajo y sus pasos a seguir pueden ser modificados conforme a las necesidades de la DIT o de la universidad y las estrategias de estas.

Esto sin olvidar los obstáculos que de acuerdo con José Luis González (Sánchez, 2023) y como cito el estudio de "*Competitive intelligence usage and understanding in USA companies, Outward insights*", señalan que la mayoría de los obstáculos que se tiene en la VT e ITC de las empresas y en LATAM, es debido a sus distintas ideologías, entre otros como se muestran en la ilustración 20:

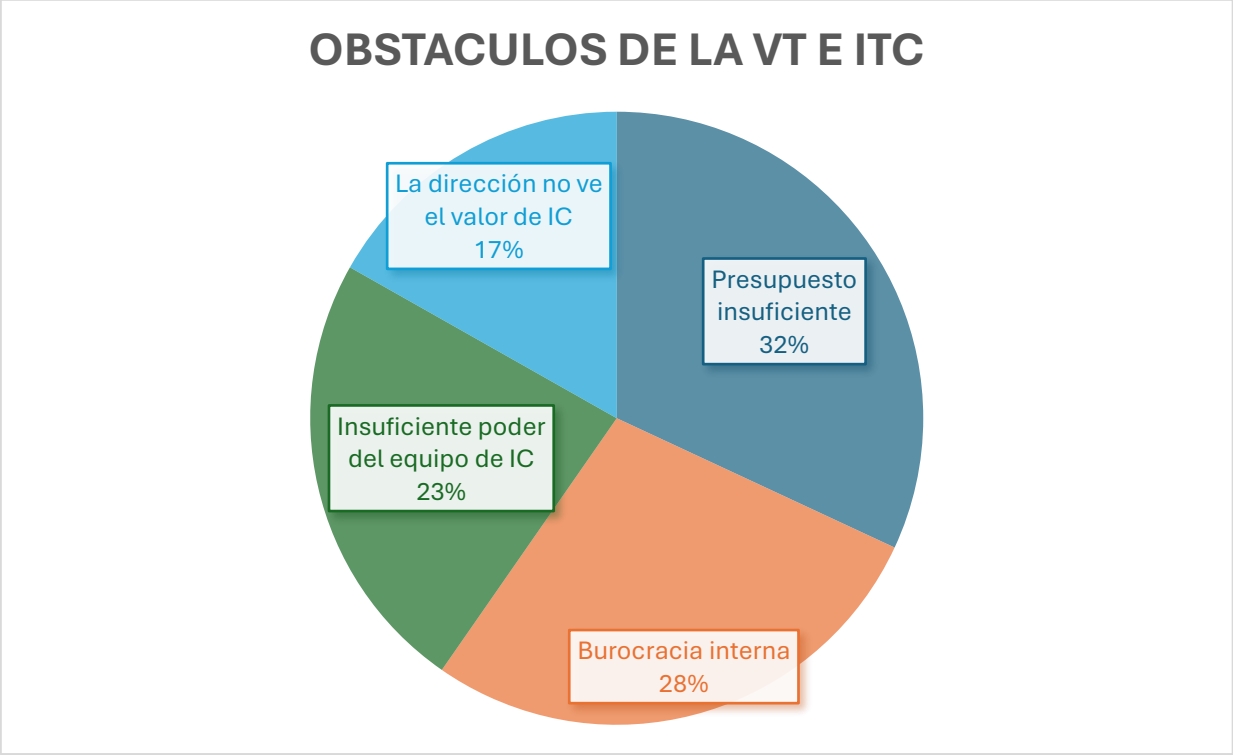


Ilustración 20. Obstáculos de la VT e ITC

Fuente: Elaboración propia, con base de José Luis González (Sánchez, 2023)

Asimismo, en dicho estudio de caso, menciona que en México y en LATAM, la VT e ITC no logran mayor impulso por motivos culturales, costumbres, prácticas, además de la resistencia al cambio, al realizar los procesos de manera diferente.

4.6 Fases para la creación de la Unidad

Para que se consolide la unida de VT e ITC se propone realizar una serie de fases, para la determinación de dichas fases se tomó como fundamento las fases que se proponen en el artículo de “El proceso de la vigilancia tecnológica y cómo implementarla” (Gutiérrez, El proceso de la vigilancia tecnológica y cómo implementarla, 2023), así como la creación de un grupo multidisciplinario el cual este compuesto por los diferentes líderes de las jefaturas, así como del director, además de personal clave que detecten necesidades de los sistemas web, así como ser los primeros en formular las preguntas iniciales con las que se iniciaría el ciclo de vigilancia tecnológica, la cual se denominará fase 1.

La **fase uno** consistiría en un análisis exploratorio en donde se utilizará la investigación realizada en este trabajo, en el cual se identificó la problemática que se tiene en los diferentes sitios web de la universidad, ya sea en el desarrollo, infraestructura o seguridad, así mismo un análisis FODA y CAME de las plataformas, lenguajes de programación o herramientas de seguridad actuales, además de identificar cuáles son los sitios web principales para la universidad, un ejemplo de ellos, el portal principal de la universidad, el cual es donde se da a conocer la oferta académica al público en general así como los enlaces a las páginas en donde se efectúa el pago de colegiaturas, o la inscripción de los alumnos, o la evaluación de los docentes.

En la ilustración 21 se muestra un FODA ejemplo, de las fortalezas, debilidades, oportunidades y amenazas de la DIT enfocada únicamente en los sistemas web.

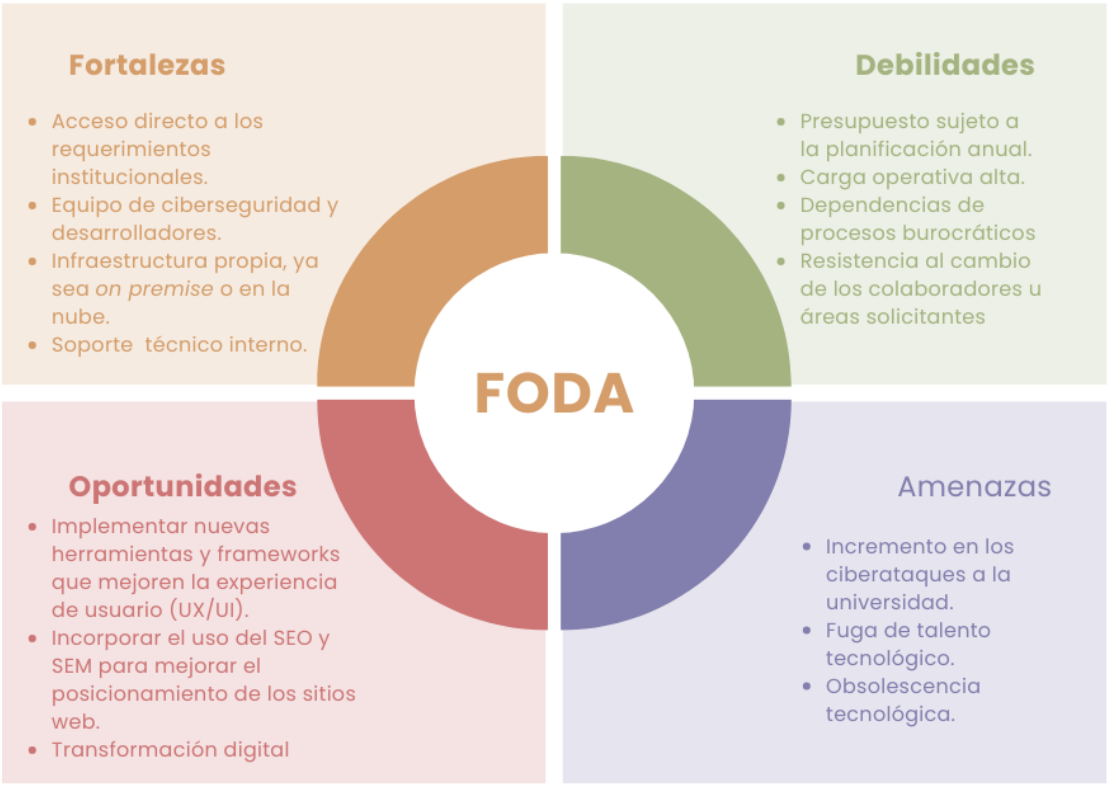


Ilustración 21. FODA de la DIT de sus sitios web

Fuente: Elaboración propia

Otro ejemplo de FODA es el que se muestra en la figura 21, en donde se un análisis del área de Servicios de Computo.

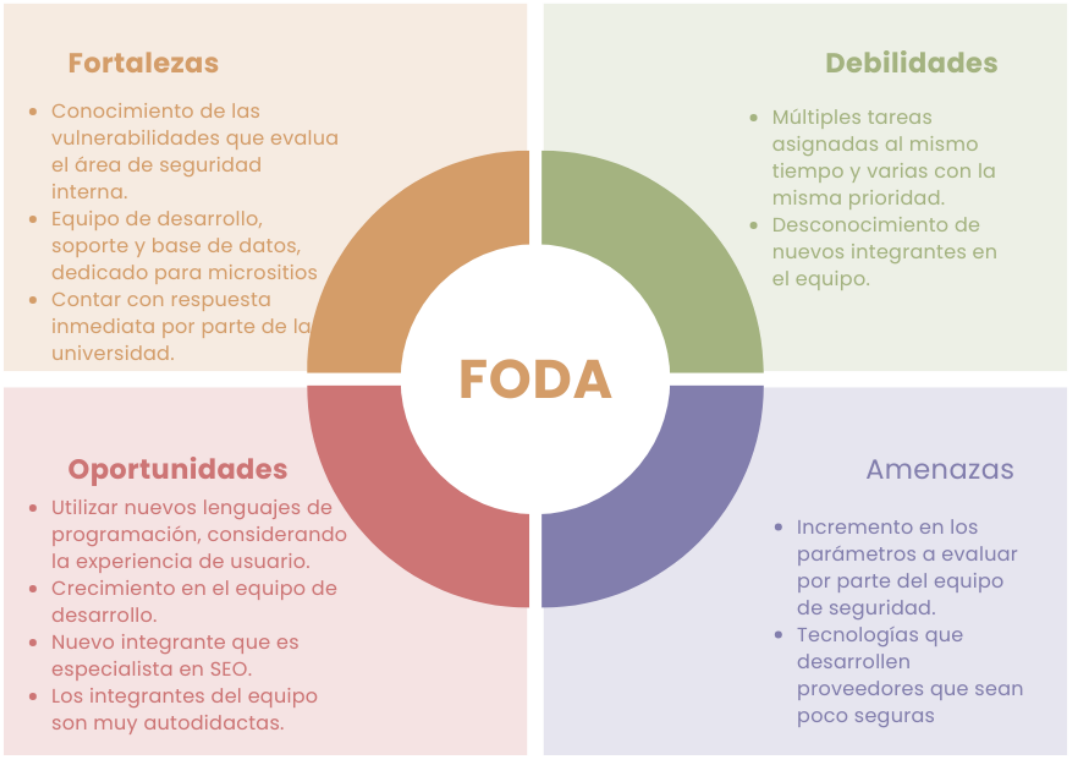


Ilustración 22. FODA de la jefatura de Servicios de Cómputo

Fuente: Elaboración propia.

Además, de dos etapas del sistema de ITC, que se muestra en la figura 16, que son la determinación de los objetivos y alcances de la vigilancia tecnológica, así como la definición de la estrategia de la VT, los cuales deben ser definidos por las diferentes jefaturas y el directo de la DIT, contemplando también el plan estratégico 2030 de la universidad. Aquí también se puede involucrar a los departamentos dueños de los procesos más relevantes, esto con el propósito de alinear los procesos digitales a las necesidades de los procesos.

La **fase dos**, consiste en formar la estructura del equipo que conforme la unidad, así como la etapa del Sistema de ITC, de la asignación de roles y responsabilidades que tendrá cada uno de los integrantes, en esta etapa se considerará los colaboradores actuales de la DIT, así como sus habilidades y experiencias y en caso de que se requiera cubrir otro perfil se tendrá la opción de contratación de personal.

Los perfiles considerados son:

- Líder de procesos: Es el encargado de formar el equipo, moderar la participación de los integrantes, coordinar los recursos y los esfuerzos.
- Los vigías: serán quienes recopilen y analicen la información sobre las tendencias, tecnologías, plataformas, lenguajes, etc. En este perfil se pueden considerar a varias personas.
- Expertos: Como su nombre lo menciona, son los líderes o referentes en una temática específica y se reúnen con regularidad con los vigías para identificar oportunidades, riesgos y acciones que se consideran para la universidad.
- Analistas de datos: Responsables de analizar la información recolectada para así poder identificar tendencias y oportunidades que permitan a la universidad mantenerse a la vanguardia tecnológica.

- Especialista en comunicación: Encargados de la comunicación para la difusión de hallazgo de la VT, dicha difusión puede ser por diferentes canales, por ejemplo: los informes o tipografías.

En un análisis realizado por la autora de este trabajo, se considera que los roles pueden asignarse a integrantes del mismo equipo de la DIT, tales como:

- Líder de programación C.
- Líderes de programación B.
- Equipo de ciberseguridad.
- Equipo de base de datos.
- Web Máster.
- Integrantes del equipo de desarrollo.
- Project Manager.

Es importante considerar que no todo el equipo cuenta con los conocimientos de cómo se realiza una vigilancia tecnológica, por lo que se debe capacitar al equipo para poder asignar los perfiles de acuerdo con las habilidades de cada uno.

En la **fase tres** se realizará la captura de información, la cual abarca la etapa de identificación del modelo propuesto en la ilustración 18 y las etapas de recolección de información y tratamiento de esta, basado en el sistema de ITC.

En esta fase también se debe considerar la adquisición de software de VT e IC el cual proporcionará información relevante sobre los avances tecnológicos, desarrollo, ciberseguridad y los puede organizar conforme sus fuentes de información.

Además, en esta etapa se realizará una categorización de VT conforme a la clasificación de las fuentes y a su vez subdividirse en el tipo de información, por ejemplo, si son notas o artículos, patentes, etc. En la ilustración 22 se muestran los tipos de fuentes.

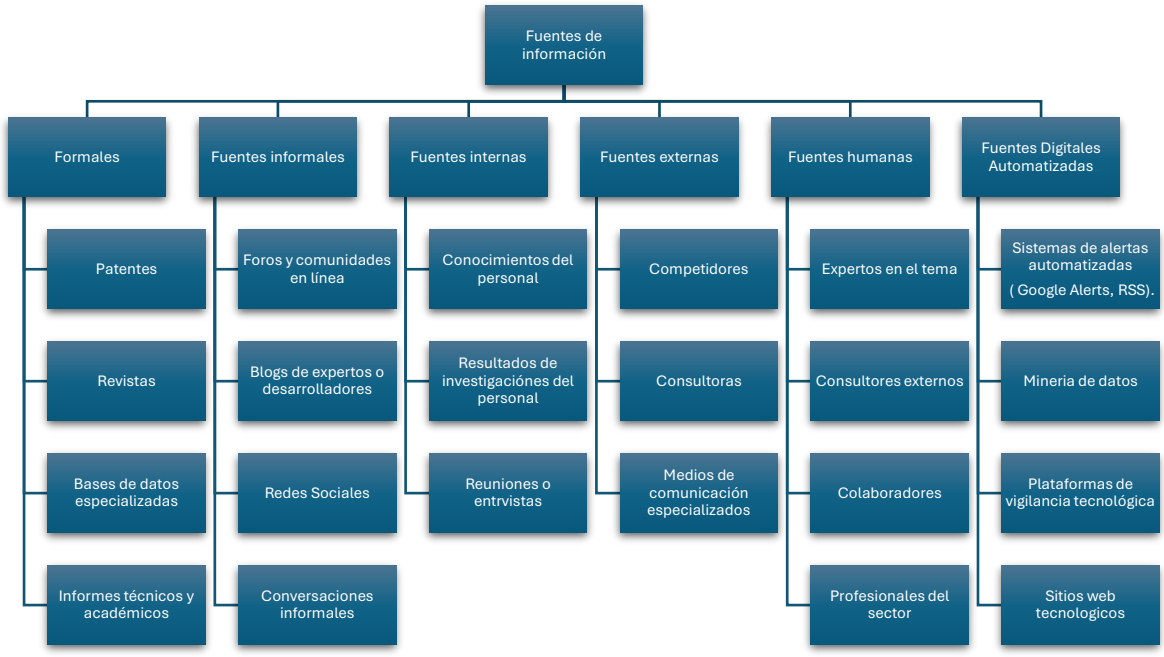


Ilustración 23. Clasificación de fuentes de información

Fuente: Elaboración propia con base de información proporcionada por ChatGPT, ChatGPT (2025).

En la **fase cuatro**, se procesaría y analizaría la información recolectada, lo que pertenece a la etapa de validación del modelo propuesto para la DIT, en esta etapa se validará que información es relevante para la DIT en cuestión de desarrollo de páginas web, aquí la recomendación de Adriana Gutiérrez (Gutiérrez, Cidei, 2023), es utilizar gestores de información:

- Mapas tecnológicos
- Software de patentes
- Gestores bibliográficos
- Visores de información
- Software de seguimiento tecnológico integral.

Dichas herramientas apoyarán a realizar los reportes que serán presentados a la dirección de la DIT y las jefaturas involucradas.

En cuanto a la **fase cinco** se presentan los reportes y se seleccionan y priorizan los hallazgos realizados, una vez priorizar las propuestas y en caso de ser necesario se solicita a proveedores una prueba de software, esto con la finalidad de saber ventajas y desventajas de las plataformas y el beneficio que le darán a la DIT, además de una capacitación al personal clave que al final son los que utilizarían la herramienta en el día a día, así como áreas involucradas que pueden tener impacto, ya sea negativo o positivo.

Además de difundir dichos reportes a los involucrados para la toma de decisiones, los cuales deben ser lo más claro posible para que puedan leerlo con facilidad y les permita tomar las decisiones.

En la **fase seis** se definen cuáles son las estrategias más adecuadas para la DIT y, además, también se toman decisiones sobre qué software se adquiere en un periodo corto y cuáles más pueden colocarse en mediano y largo plazo. Así como también aquí se considera el presupuesto que requiere cada implementación de mejora o actualización digital.

5. Metodología de trabajo

En este capítulo se mostrará la metodología del trabajo del presente, la cual se refleja en la siguiente figura:

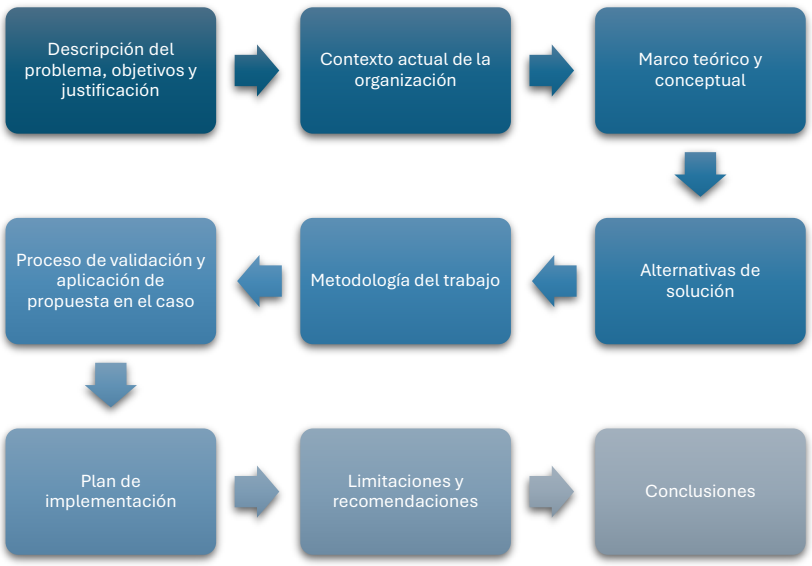


Ilustración 24. Metodología del trabajo

Fuente: Elaboración propia

La descripción de cada uno de los pasos de la ilustración 24, así como el cómo están compuestos, se describen a continuación.

5.1 Descripción del problema, objetivos y justificación

En esta sesión se plasmó la situación actual de la DIT, en la cual sus actividades del día a día les consumen a los diferentes colaboradores, lo que no permite tener una visión con antelación a cambios externos a la universidad.

Así como también la justificación del porqué, es importante contar con una unidad que permita actuar con antelación a los diferentes cambios en el entorno, así como el aprovechamiento de nuevas tecnologías que sustituyan a las tecnologías actuales con las que cuenta la universidad.

Este problema se enfoca para este trabajo en el servicio de páginas web y alojamiento de las mismas, dado que los colaboradores encargados de que los sitios web se encuentren funcionando de manera adecuada, en múltiples ocasiones se han tenido que enfrentar en tener diversos sitios web desarrollados en versiones de tecnologías diferentes, librerías obsoletas que afectan el funcionamiento adecuado de la página o el aplicar medidas de seguridad de manera inmediata, lo que hace que el equipo de trabajo trabaje de manera extra temporal o a marchas forzadas.

5.2 Contexto actual de la organización

En esta sesión se analizó como está actualmente la estructura de la DIT, el cómo diferentes jefaturas interactúan entre sí para lograr el funcionamiento adecuado de los sitios web transaccionales, informativos o portales principales, el cómo una actualización necesaria de seguridad puede afectar al funcionamiento de los sitios, o como se requiere realizar modificación en la programación para adoptar y mejorar el funcionamiento de las páginas con respecto a cambios externos de la universidad, tal es el caso de las librerías permitidas por Google o nuevas herramientas de tecnología o infraestructura que pueden impactar en el funcionamiento de los sitios web.

También es importante mencionar que las diferentes jefaturas actualmente hacen cada una sus propias investigaciones de nuevas tecnologías, herramientas o de los cambios y en ocasiones no se toma en consideración las demás áreas y cuanto se requeriría tanto de tiempo máquina y recurso humano para hacer que funcione adecuadamente, además de no poder anticiparse a los cambios externos y poder realizar una planeación estratégica adecuada.

5.3 Marco teórico y conceptual

En esta sesión se analizaron diferentes fuentes de información, lo que ayudará a darle una posible solución a la problemática, en la cual se encontraron diferentes puntos, los cuales son:

- En dónde se encuentra la universidad conforme a la curva de implementación de tecnología.
- Vigilancia tecnológica
- En esta sesión se muestra el cómo está compuesta la DIT a nivel organigrama y el cómo diferentes jefaturas interactúan entre sí para
- Inteligencia tecnológica competitiva.

Donde se habla del ciclo de la Vigilancia tecnológica y de Inteligencia tecnológica, el cómo a pesar de que pueden confundirse y parecer similares no lo son, esto debido a que la Vigilancia tecnológica sirve para la recolección de información, el filtrado y el cómo catalogar dicha información, mientras que la inteligencia tecnológica permite poner en acción la adquisición, la capacitación, la distribución de nuevas tecnologías, todas ellas alineadas a la misión, visión y el plan estratégico de la universidad.

Además, se analizaron cuáles modelos pueden ser los más adecuados de utilizar, los pros y contras de cada uno dentro de la DIT.

5.4 Alternativas de solución

En esta sección se destacaron tres posibles soluciones, así como las formas en que podrían implementarse conforme a las necesidades específicas de la DIT, considerando también las posibles restricciones asociadas a cada una al momento de su aplicación.

Cabe mencionar que también se destaca que es importante la creación de una unidad enfocada en realizar dos ciclos, los cuales son la Vigilancia tecnológica como primer ciclo, en el cual se requerirá de personas que se enfoquen en realizar la recolección de información enfocada en los temas, tales como:

- Nuevos lenguajes de programación, CMS o plataformas para el desarrollo de sitios web ágiles, con mayor seguridad y que cumplan los requisitos y cubra las necesidades de la comunidad universitaria.
- Herramientas de seguridad o aplicar nuevos filtros de seguridad que permitan proteger los servidores de posibles atacantes, así como la protección de los sitios para evitar la incrustación de código malicioso en los sitios web o el monitoreo de páginas que puedan ser falsas y que su propósito sea que los usuarios proporcionen información importante.
- Mejoras en el desarrollo de páginas web.
- Mejoras en servidores, actualización de manera oportuna o el migrar de servidores, evitando que los servidores, por ejemplo, Windows, se queden sin soporte por parte del fabricante.

Además de realizar una planeación estratégica enfocada en cumplir metas y objetivos que en un inicio se establecen, así como la integración del equipo de vigilancia tecnológica, tanto de recursos actuales de la universidad, así como la incorporación de nuevos elementos al equipo.

5.5 Metodología del trabajo

En esta sesión, se detalla la metodología que se utiliza, así como una breve explicación de qué se realizó en cada paso, esto con el fin de ser claros al momento de presentar el enfoque de dicho proyecto, además de mostrar el cómo se va adaptando a las necesidades del trabajo en sí.

5.6 Proceso de validación y aplicación de propuesta en el caso

En esta sesión se llevó a cabo la validación de la solución propuesta, identificando a los principales colaboradores que contribuirán a la implementación de la nueva metodología. Asimismo, se analizó cómo la creación de la unidad apoyará en la adecuada aplicación de la planeación estratégica y facilitará la toma de decisiones con mayor anticipación.

Para ello, se organizó un *focus group* en el que primero se expuso el objetivo de la creación de dicha unidad, su propósito, los beneficios que podría aportar, la forma en que se planea implementarla, y se solicitó retroalimentación sobre posibles mejoras. Específicamente, se pidió a los participantes que señalaran qué aspectos modificarían, qué elementos reforzarían o qué partes no consideran coherentes con los objetivos actuales de la DIT y su alineación con la visión de la universidad.

Los *focus group*, se aplicarán a las siguientes personas claves:

- Jefe de Desarrollo
- Jefe de Servicios de Cómputo
- Líder de programación C, que es el encargado de proporcionar los diferentes servidores.
- Jefe de Ciberseguridad
- Equipo de ciberseguridad
- Equipo de base de datos
- Web Máster
- Integrantes del equipo de desarrollo
- Director de la DIT.

5.7 Plan de implementación

En esta sesión, una vez realizados los *focus group* con las personas seleccionadas, tomando en consideración sus propuestas, ajustes y necesidades, se realizarían las adecuaciones necesarias.

Además, en esta fase se utilizará el sistema de ITC, el cual consta de los siguientes pasos:

- Determinar los objetivos y alcances de la Vigilancia tecnológica.
- Definir la estrategia de la vigilancia tecnológica.
- Asignar roles y responsabilidades. Este paso se validará si se cuenta con los recursos humanos propios o si se requiriese de la búsqueda de nuevo talento para dicha actividad.
- Recolección de la información: en este paso se pueden utilizar herramientas para realizar más eficientemente la recolección de información.
- Tratamiento de la información.
- Generación de reportes de Inteligencia tecnológica competitiva.
- Revisión de los reportes.
- Presentación a la dirección de la empresa.
- La difusión de reportes de ITC a las jefaturas involucradas.
- Definición de estrategias y toma de decisiones.

5.8 Limitaciones y recomendaciones

En esta sesión, se explica cuáles serían las posibles limitaciones al momento de implementar la nueva unidad de vigilancia e inteligencia tecnológica competitiva, entre los cuales existen los siguientes factores: el tiempo, el recurso económico y el personal que se requiere para la creación de dicha unidad.

Además, se realizan recomendaciones del cómo se puede aplicar no solo al servicio de páginas web, como la vigilancia, se podría utilizar poco a poco en cada uno de los servicios ofrecidos por la DIT.

5.9 Conclusiones

En esta sesión, se evaluará si la solución aplicada en el departamento de la DIT es funcional para ir aplicando en las diferentes necesidades, así como también se considerará una retroalimentación por parte de la DIT a la autora de dicha propuesta y se les solicitará que se den puntos de retroalimentación para ir mejorando a la unidad y así apoyar a la DIT en dar cada día un mejor servicio tecnológico a la comunidad universitaria.

6. Proceso de validación y aplicación de propuesta en el caso

En este capítulo, se plantea como se validará si la idea propuesta es la ideal para el equipo de la DIT, así como una propuesta de cómo aplicarlo, para eso, se realizaron *focus group* con diferentes perfiles, los cuales intervienen en la publicación, actualización, mantenimiento y el correcto funcionamiento de las páginas web de la universidad.

6.1 Proceso de validación

El propósito del *focus group* es evaluar la viabilidad de crear una unidad de vigilancia tecnológica (VT) e Inteligencia tecnológica competitiva (ITC), para esto se requiere planear cuidadosamente el objetivo, los perfiles de los participantes, la dinámica de la discusión y cómo se analizarán los resultados, para eso se realizaron los siguientes pasos.

6.1.1 Focus group

El objetivo del *focus group* es “Explorar la percepción y la disposición de los colaboradores claves para implementar una unidad de VT/ITC, así como identificar las expectativas, necesidades y posibles obstáculos”.

Los participantes que se tienen considerados para el ejercicio son los siguientes:

- Jefe de Desarrollo
- Jefe de Servicios de Cómputo

- Líder de programación C, que es el encargado de proporcionar los diferentes servidores.
- Jefe de Ciberseguridad
- Equipo de ciberseguridad
- Equipo de base de datos
- Web Máster
- Integrantes del equipo de desarrollo
- Director de la DIT.

En cada *focus group* se llevará a cabo una reunión entre 6 y 10 participantes, lo que facilitaría una conversación fluida, con diferentes puntos de opinión y sin que estos se dispersen en otros temas que no se tengan en consideración para la sesión. Además, se creó una guía de discusión para que se tenga una lista de pasos para llevar la reunión.

6.1.1.1Guía del *focus group*

Introducción

¿Conocen o han tenido experiencia con vigilancia tecnológica o inteligencia competitiva?

¿Sabe la diferencia entre vigilancia tecnológica e inteligencia competitiva?

¿Cómo se toman actualmente las decisiones estratégicas o tecnológicas enfocadas para páginas web?

Exploración del problema

¿Qué tan relevante consideran contar con información sistemática del entorno tecnológico?

¿Qué riesgos han identificado por no anticiparse a los cambios tecnológicos?

Evaluación de la idea

¿Ven viable implementar una unidad de VT/ITC dentro de la DIT?

¿Qué beneficios visualizan en el servicio de páginas web?

¿Qué barreras podrían dificultarlo (presupuesto, cultura, capacidades, etc.)?

Condiciones para el éxito

¿Qué requeriría una unidad así para tener impacto real?

¿Qué perfil debería tener el equipo?

¿Qué indicadores servirían para medir su éxito?

Cierre

¿Algo más que deseen agregar?

¿Estarían dispuestos a colaborar con una futura unidad?

Resultados de los *focus group*

A continuación, se presenta un reporte de las actividades realizadas en los dos focus group. Si bien se contaba con una guía previamente estructurada, se permitió a los participantes expresar libremente sus inquietudes, recomendaciones y observaciones, lo que enriqueció significativamente la discusión. En ambas sesiones estuvieron presentes personas clave, tanto aquellas que podrían integrarse al equipo de Vigilancia Tecnológica e Inteligencia Tecnológica Competitiva, como quienes ocupan cargos de toma de decisiones en las distintas jefaturas, además de la participación del director de la DIT.

Fechas de realización: 9 y 10 de abril del 2025.

Duración: 1 hora el día 9 de abril, 45 minutos el 10 de abril

Número de participantes: 12 participantes

Perfil de los participantes:

- Jefe de Desarrollo
- Jefe de Servicios de cómputo
- Líder de programación C, que es el encargado de proporcionar los diferentes servidores.
- Jefe de Ciberseguridad
- Equipo de ciberseguridad
- Equipo de Base de datos
- Integrantes del equipo de desarrollo
- Director de la DIT.

Temas principales abordados:

1) Dar a conocer el concepto de vigilancia tecnológica, inteligencia competitiva y cómo las mismas ayudan a la DIT a mantenerse a la vanguardia tecnológica.
2) Metodología que se utilizará en la universidad, así como exponer los el caso de Instituto Mexicano del Petróleo.
3) ¿Cómo se implementaría en la universidad?
4) Disposición del equipo para integrar el equipo de VT e ITC.

Hallazgos claves

1) Desconocimiento de Vigilancia e Inteligencia tecnológica competitiva.
    a. La mayoría de los participantes no conocían los términos, por lo que nunca habían trabajado directamente con una unidad o área enfocada en la recolección de información, como la mayoría comento, todos en la DIT realizan de alguna manera desde su trinchera propuestas, revisan nuevas tecnologías o proponen cambios, pero no se tiene una metodología para realizarla de manera estructurada.
    b. Por ende, no se tenía el conocimiento de que existían herramientas que ayudan en realizar la recolección de información útil para el tema que se requiera.
2) Se comprende el porqué de la importancia de la Unidad, dando apertura de cómo se realizaría.
    a. Los integrantes entienden la importancia y el potencial de contar con esta unidad, se comprendió el cómo se puede utilizar, cuestionaron cosas del cómo se pretende llevar a cabo y por qué solo se había cerrado a páginas web, para lo cual se expuso que para fines del tiempo del proyecto de vinculación solo se había seleccionado parte de la DIT, pero que se podría ir implementando en los demás servicios de esta.
    b. Se habló de cómo se podría incorporar el grupo de personas que integren esta unidad o comité de personas, el cómo podría ser un grupo híbrido e ir rolando al personal, todo dependiendo de las necesidades de la universidad y de lo que se requiera tener información relevante para la toma de decisiones.
    c. También se destaca la importancia de considerar los costos aproximados de utilizar nuevas tecnologías vs. las tecnologías o plataformas que se tienen actualmente en este momento, esto debido a que en ocasiones el costo de esta por el momento es más elevado que el mantenerlos en la actual infraestructura, por ejemplo, los costos de la nube pueden ser mucho mayor que el mantener los sitios web en infraestructura en las instalaciones.
3) Importancia de tener información que impacte tanto de manera negativa como positiva al ecosistema digital.
    a. El equipo compartió experiencias que se han vivido en la DIT por no contar con la información oportuna, no solo en cuestión de tecnología, también en lo que le ha costado de recurso humano, por ejemplo, las horas invertidas en dar pronta solución en cambios tecnológicos que afectan a los desarrollos de la universidad, o el uso de herramientas tales como GITHUB, que ante ciberataques que anteriormente se han

tenido, posiblemente el punto de retorno y la pérdida de información en cuestión de desarrollo, se hubiera reducido considerablemente.

b. La DIT, actualmente está en proceso de transformación en la cual no solo se ve como una dirección de facilitar o de proporcionar servicios, tiene como un objetivo ser una dirección propositiva, que le ayude a los usuarios a tener lo que realmente necesiten y que les ayude en sus actividades cotidianas y que a su vez la universidad pueda proporcionar servicios o propuestas a la vanguardia, que le permitan inclusive incorporar otras tecnologías de una manera más orgánica.
c. Se cuestionó sobre si alguna otra universidad cuenta con su unidad, para lo cual se expuso un ejemplo que se encontró dentro de la investigación previamente realizada, en el cual en este momento no solo les ayuda a ellos como universidad, sino que también lo ofrecen como servicio a otras empresas, para que puedan incorporar esta ventaja a sus organizaciones de manera práctica y reducir los riesgos de fallar.

4) Se entiende que dicha unidad no solo se utilizaría para el desarrollo de páginas web, sino para todos los productos y servicios que se ofrecen en la DIT.
    a. Se dio a conocer que esta unidad tiene un gran potencial, qué beneficiaria a todas las jefaturas y servicios que se tienen en la universidad, así como los futuros servicios que se pudieran proporcionar, por ejemplo, el uso de inteligencia artificial que actualmente varios departamentos y la misma DIT tiene entusiasmo en utilizarla para diferentes acciones.
    b. Además, se hicieron recomendaciones para la mejora del modelo y metodología que se propuso, tal como que se presentará un equipo inicial de la unidad, así como que se deben considerar los cambios estratégicos que se están realizando dentro de la DIT y que eso haría que algunos pasos o planteamientos realizados al momento de llevar a cabo este trabajo, se tengan que modificar al momento de implementarlo en la Dirección.
    c. Para algunos la información compartida por otras jefaturas fue de real importancia, esto debido a que como se explicó en un diagrama, en ocasiones lo que haga uno de ellos puede tener efecto tanto positivo como negativo en los sitios web, ya que puede afectar su funcionamiento o su seguridad de los usuarios se puede ver vulnerable.
5) Entusiasmo y compromiso en el equipo en que se forme este grupo para realizar hallazgos oportunos que ayuden a la comunidad universitaria.
6) Conclusiones

La propuesta causó interés entre los involucrados, se sienten entusiasmados en iniciar esta unidad, para ellos es importante que no solo se quede en él para que, sino que se aplique el cómo y de ello motivar e invitar a las demás jefaturas en que se sumen en este proyecto.

6.2 Mejoras en la propuesta inicial

Antes de poder determinar los objetivos y alcances de la vigilancia tecnológica e inteligencia competitiva en la universidad, se llevarán a cabo diversos análisis estratégicos —FODA, PESTEL, CAME y Porter— que permitirán a las jefaturas y a la dirección conocer con mayor claridad la situación actual de la DIT, así como obtener un panorama sobre la forma en que se toman decisiones que impactan en los sitios transaccionales, micrositios y portales principales. Estos análisis serán de gran utilidad para alinear los objetivos de la propuesta con las metas estratégicas en las que actualmente está trabajando la DIT.

Considerar un equipo híbrido, dando la oportunidad a que el equipo pueda agregar el pertenecer a dicho equipo de investigación y filtrado de información al resto de sus actividades, ya que se consideraría que el equipo utilice diferentes herramientas para obtener información relevante para el tema de los desarrollos web y que el comité se reunía una semana completa cada dos meses para el filtrado de información así como realizar las comparaciones entre las tecnologías actuales vs. las nuevas y presentarla a dirección y a las diversas jefaturas, para que todos conozcan la información y permite si así fuera el caso, tomar decisiones en su momento o estar atentos a futuros cambios y que permita tener visibilidad de los cambios tecnológicos.

Hacer la propuesta de los reportes que se les entregaría a los involucrados para que en el menor tiempo posible puedan obtener la información relevante que les ayude a considerar datos que les permitan, si ese fuera el caso, tomar de decisiones eficaces y de manera más ágil.

Con todo lo anteriormente mencionado y considerando la propuesta inicial para la creación de la unidad de vigilancia tecnológica e inteligencia tecnológica competitiva, se propone las mejoras en la ilustración 25 en donde se puede ver claramente la forma de trabajar que se tendría en la unidad de vigilancia tecnológica e inteligencia competitiva.

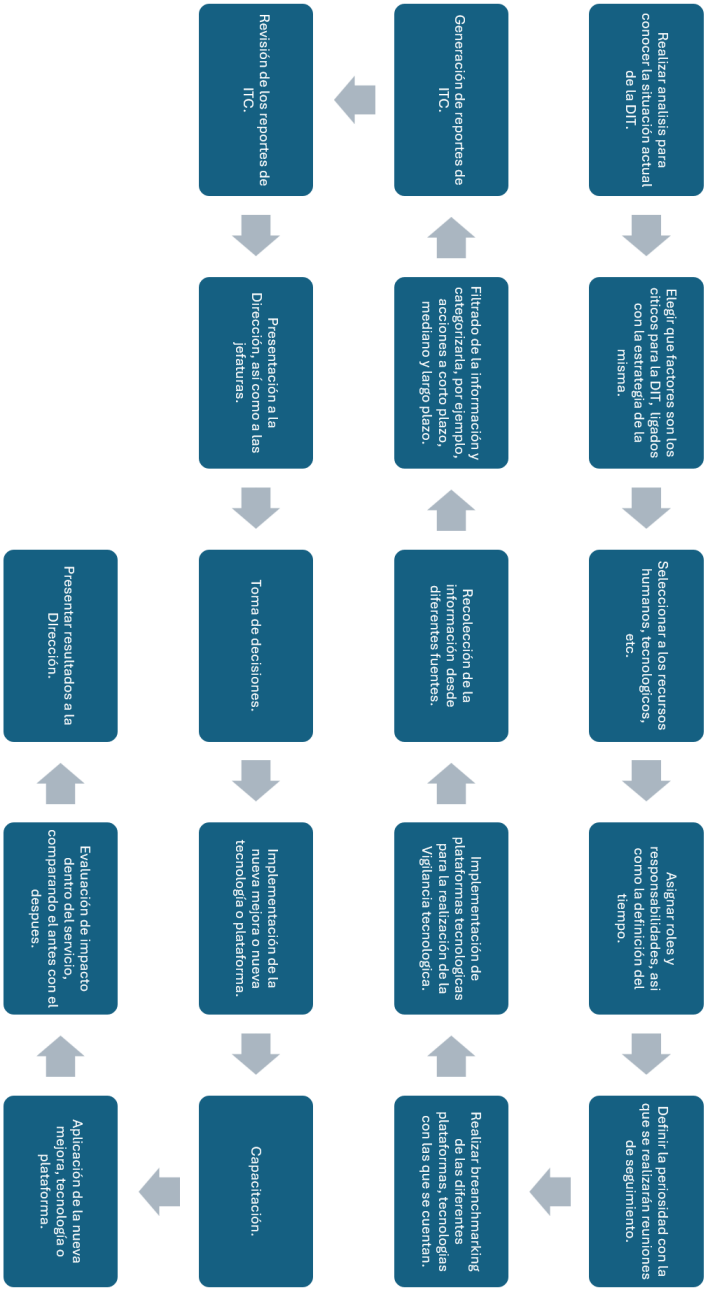


Ilustración 25. Mejora de la propuesta realizada.

Fuente: Elaboración propia basada en (Henderson, 2023)

Con la modificación de los pasos a realizar para la creación de la unidad, se modificaría el orden que se había presentado en la ilustración 18, la cual quedaría finalmente como se muestra en la Ilustración 26:

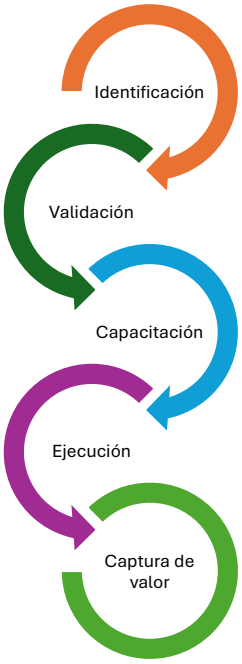


Ilustración 26. Modelo final para la propuesta de la DIT

Fuente: Elaboración propia basada en el modelo de IMP (Petróleo, 2017)

7. Plan de implementación

En este capítulo se desarrolla la implementación a alto nivel, el plan de trabajo, los costos que se tienen que considerar, así como riesgos que se tendrían en la implementación de la unidad dentro de la DIT en su ecosistema digital.

Cabe mencionar que el plan no solo está pensado en los sitios web de la universidad, sino que está pensado para que en un mediano o largo plazo se pueda considerar para implementar en el resto de los servicios ofrecidos por la DIT a la universidad.

7.1 Implementación a alto nivel

El plan de trabajo a alto nivel para la implementación de la unidad de VT e ITC el cual se verá en 7 pasos:

Ilustración 27. línea del tiempo para implementar la UVT e ITC

Fuente: Elaboración propia.

La ilustración 27 muestra los 7 pasos que serán aplicados para este proyecto y a continuación se explicará cada uno de ellos:

- Propuesta y aprobación: En esta etapa se hace la propuesta de manera formal a la dirección de la DIT, en la que se expone el cómo la unidad beneficiará a los sistemas web y finalmente a los usuarios finales. También en esta etapa se requiere la aprobación de la DIT, la cual consiste en los responsables de cada jefatura, así como el del director, los cuales son esenciales para la implementación de la unidad y la colaboración de los integrantes de la dirección.
- Diagnóstico y planificación: En esta etapa se evaluarán las capacidades internas (recursos humanos, tecnológicos), los objetivos de la vigilancia tecnológica, así como identificar y priorizar las áreas de oportunidad en el universo digital de la universidad. Los entregables que se realizarían son: El documento diagnóstico y el plan estratégico de la unidad de vigilancia tecnológica.
- Diseño de la unidad de VT e ITC: Se requiere establecer la estructura organizacional de la unidad, así como los responsables y sus funciones, además de diseñar los procesos relacionados con la búsqueda, análisis, validación y difusión.
  En esta etapa se seleccionan las herramientas tecnológicas que serán utilizadas para la vigilancia tecnológica, además de un manual de operación de la unidad de VT e ITC.
- Capacitación del personal: Se requiere consolidar al equipo que será el encargado de iniciar la unidad, al cual se le dará la capacitación en cuanto la inteligencia tecnológica, vigilancia tecnológica, las fuentes de información, como clasificarlas, el uso del software para la vigilancia tecnológica, etc.
- Piloto: Se selecciona un tema de interés y se aplica todo el ciclo de vigilancia seleccionado previamente, se analiza y se filtra la información, así como la generación de reportes y se efectúan ajustes necesarios.
- Puesta en marcha: Se realizará la ejecución de los procesos previamente establecidos, además se emitirán los primeros reportes y alertas tecnológicas. Se establecerían los indicadores de desempeño que permitan evaluar si la unidad está siendo de utilidad.
  Parte de los entregables que se entregarán en esta etapa, adicionalmente a los reportes, son los análisis realizados, por ejemplo, análisis FODA, PESTE y CAME.
- Seguimiento y mejora continua: Se evalúa el impacto en el ecosistema digital de la información que se entregó, además se efectúan los ajustes a los procesos y herramientas según sea requerido. Esta dará pauta para que se consoliden buenas prácticas dentro de la unidad.
  Los entregables son: Reporte de indicadores y propuestas de mejoras.

7.2 Plan de trabajo

7.2.1 Diagrama WBS

En la ilustración 28 se muestra la estructura de desglose de fases del proyecto con sus respectivas tareas, las cuales están orientadas en la puesta en marcha de la unidad de vigilancia e inteligencia tecnológica competitiva de la universidad, se recomienda consultar el Anexo 1 del presente documento.

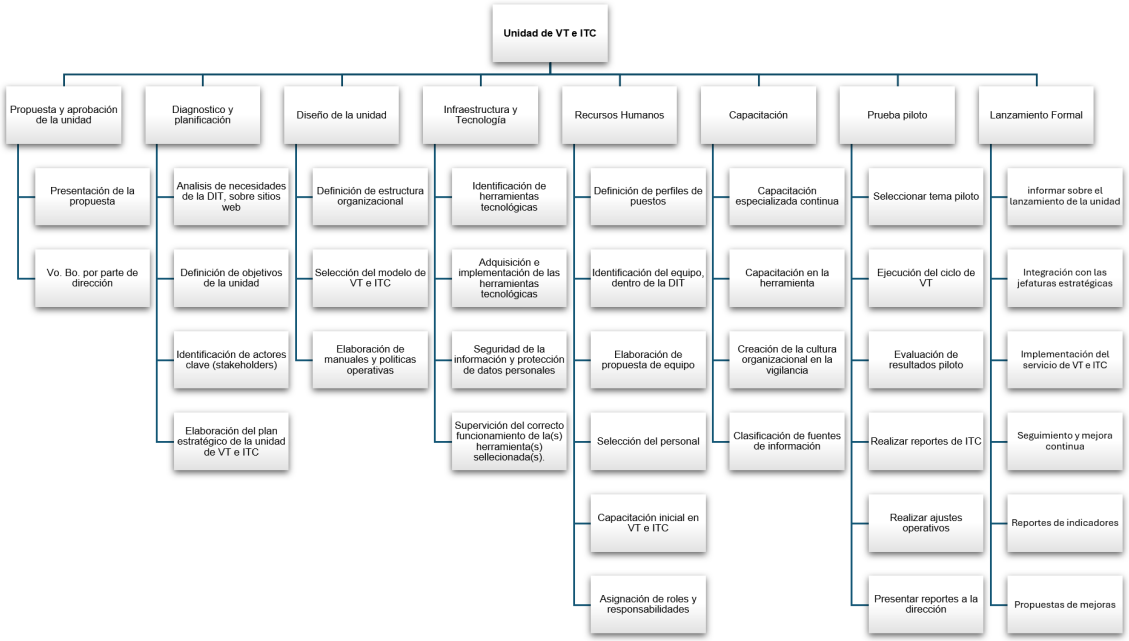


Ilustración 28. Diagrama WSB

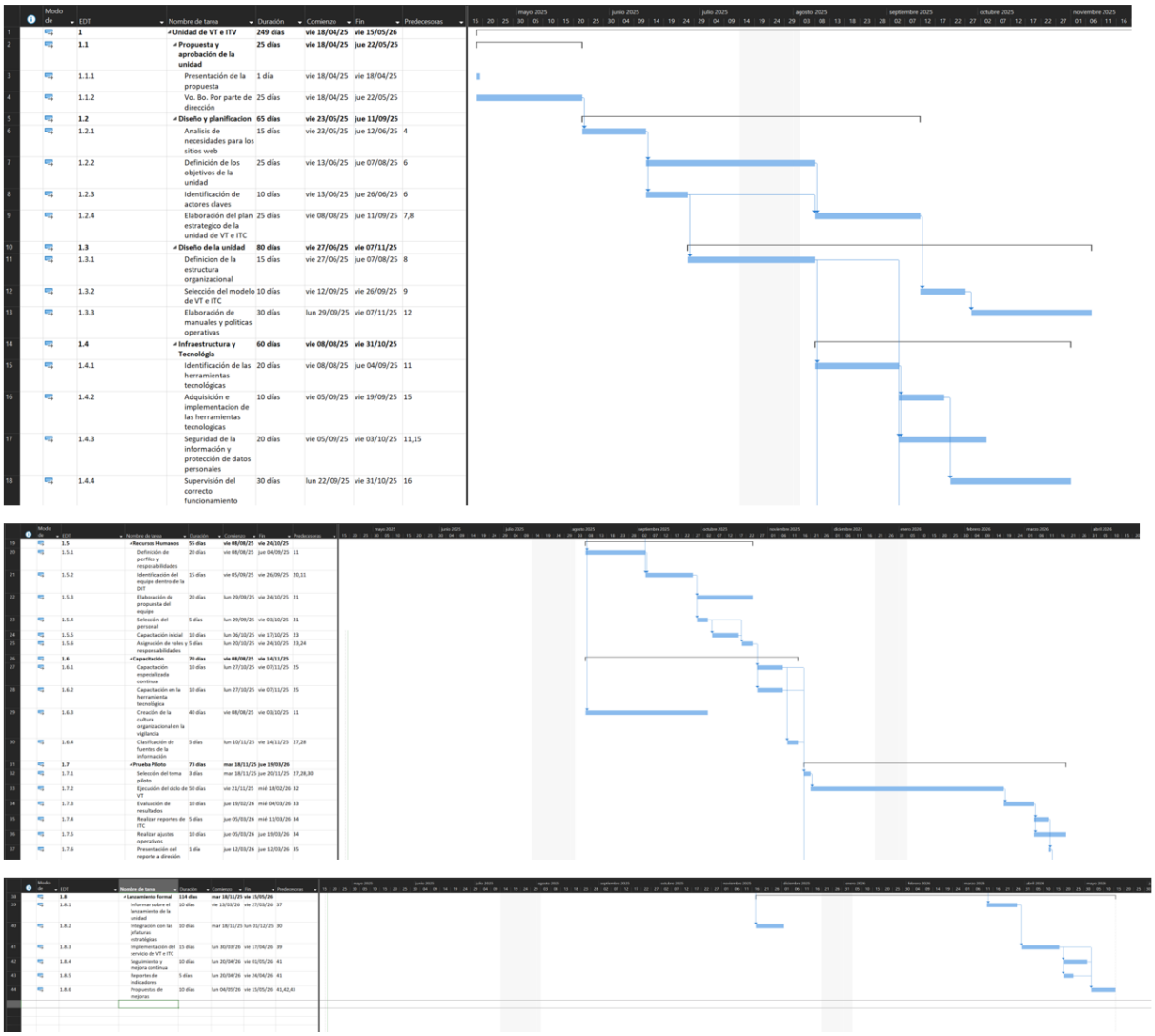
Fuente: Elaboración propia

7.2.2 Diagrama de Gantt

En la Ilustración 29 es un extracto del diagrama de Gantt, el cual de una manera visual y puntual señalas las tareas que se deberán ejecutar por cada una de las fases para habilitar la unidad de VT e ITC y poder cumplir con los objetivos planteados al momento de exponerlo a dirección, cada actividad cuenta con su fecha de inicio y fin, además se consideraron los días de suspensiones laborales.

La puesta en marcha de la unidad se tiene programado un aproximado de ocho meses. Durante este periodo, se podrá analizar, modificar y a evaluar el rendimiento de todos los aspectos involucrados para realizar una nueva versión de este.

Para una mejor apreciación, se recomienda visualizar el Anexo 2.



Modo de	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
	1	**Unidad de VT e ITV**	**249 días**	**vie 18/04/25**	**vie 15/05/26**	
	1.1	**Propuesta y aprobación de la unidad**	**25 días**	**vie 18/04/25**	**jue 22/05/25**	
	1.1.1	Presentación de la propuesta	1 día	vie 18/04/25	vie 18/04/25	
	1.1.2	Vo. Bo. Por parte de dirección	25 días	vie 18/04/25	jue 22/05/25	
	1.2	**Diseño y planificacion**	**65 días**	**vie 23/05/25**	**jue 11/09/25**	
	1.2.1	Analisis de necesidades para los sitios web	15 días	vie 23/05/25	jue 12/06/25	4
	1.2.2	Definición de los objetivos de la unidad	25 días	vie 13/06/25	jue 07/08/25	6
	1.2.3	Identificación de actores claves	10 días	vie 13/06/25	jue 26/06/25	6
	1.2.4	Elaboración del plan estrategico de la unidad de VT e ITC	25 días	vie 08/08/25	jue 11/09/25	7,8
	1.3	**Diseño de la unidad**	**80 días**	**vie 27/06/25**	**vie 07/11/25**	
	1.3.1	Definicion de la estructura organizacional	15 días	vie 27/06/25	jue 07/08/25	8
	1.3.2	Selección del modelo de VT e ITC	10 días	vie 12/09/25	vie 26/09/25	9
	1.3.3	Elaboración de manuales y politicas operativas	30 días	lun 29/09/25	vie 07/11/25	12
	1.4	**Infraestructura y Tecnológia**	**60 días**	**vie 08/08/25**	**vie 31/10/25**	
	1.4.1	Identificación de las herramientas tecnológicas	20 días	vie 08/08/25	jue 04/09/25	11
	1.4.2	Adquisición e implementacion de las herramientas tecnologicas	10 días	vie 05/09/25	vie 19/09/25	15
	1.4.3	Seguridad de la información y protección de datos personales	20 días	vie 05/09/25	vie 03/10/25	11,15
	1.4.4	Supervisión del correcto funcionamiento	30 días	lun 22/09/25	vie 31/10/25	16

Ilustración 29. Diagrama de Grantt

Fuente: Elaboración propia

7.3 Retos que representan a la DIT

El incorporar una unidad de VT e ITC representa para la DIT un reto importante, ya que como se ha mencionado anteriormente la vigilancia se realiza, pero con una metodología y ciclo a cumplir para realizar una buena vigilancia tecnológica, esto implica también en hacer cambios en la forma en la que trabaja.

Otros retos a los que se enfrenta la DIT son:

- Las actividades del día a día de los integrantes de la unidad.
- Falta de recursos humanos capacitados.
- Los objetivos deben ser claros para evitar la ambigüedad sobre lo que se espera de la unidad para el ecosistema digital.
- La resistencia al cambio, esto debido a la incorporación de nuevas prácticas de cómo realizar la vigilancia y el seguimiento estructurado.
- El tiempo que se le dedicará a la recolección y depuración de información, este factor puede ser variable, ya que depende de la cantidad de información obtenida.
- Escasos de recursos financieros.

- Reportes de ITC que no cumplan con las expectativas de la dirección, por lo que deben ser completos y se considera una reunión con dirección para establecer los lineamientos deseados.
- Burocracia entre áreas, esto debido a que puede retrasar la compra de herramientas tecnológicas y afectar los tiempos considerados.

7.4 Gestión de riesgos

Para habilitar la unidad de vigilancia tecnológica e inteligencia tecnológica competitiva, se identificaron los siguientes riesgos asociados:

Tabla 4. Riesgos

Riesgo	Descripción	Plan de mitigación
Alto	Alineación de los objetivos con el plan estratégico de la universidad.	**Comunicación:** Realizar periódicamente una reunión para alinear los objetivos de la unidad, tanto con el plan estratégico de la DIT y la universidad. **Notificaciones:** En caso de que exista algún cambio que se deba considerar de manera inmediata, es importante que exista un canal fluido de comunicaciones y se aplique a la brevedad.
Alto	Resistencia al cambio	**Involucramiento**: Informar y motivar a las jefaturas involucradas con los sitios web. **Comunicación**: Informar de las ventajas y beneficios de contar con la unidad de VT e ITC. **Reuniones**: Se realizarán reuniones para saber cuáles son las preocupaciones de cada uno y desarrollar un plan para que les motive a incorporarse a la iniciativa.
Alto	Sobrecarga de trabajo del equipo	**Distribución del trabajo**: Se les asignarán las diferentes tareas a más elementos de la DIT para que los elementos involucrados en la unidad se desarrollen de manera adecuada. **Nuevos recursos humanos:** En caso de ser necesario, se evaluará la incorporación de nuevos elementos. **Planificación:** Coordinarse con las jefaturas para seleccionar las fechas a las que el equipo le dedicará tiempo a la vigilancia y generación de reportes.
Mediano	Falta de liderazgo y coordinación del equipo	**Capacitación:** Proporcionar las herramientas necesarias y desarrollar las habilidades blandas que se requieran para el liderazgo y coordinación de equipo. Además de las habilidades técnicas requeridas.

		Acompañamiento: Se sugiere tener el acompañamiento de un líder de jefatura que le permita al nuevo líder generar la confianza. **Retroalimentación:** Los colaboradores, jefes y director tienen la apertura para poder hablar de temas que sientan que faltan al líder de la unidad.
Mediano	No tomar decisiones oportunas	**Calendario de alertas**: Una vez que se generen los reportes de la vigilancia, también se generarán calendarios de notificaciones de alertas con criticidad, para que los involucrados tomen las decisiones en el mejor de los tiempos.
Mediano	Saturación de información	**Capacitación:** Proporcionar los conocimientos necesarios para poder filtrar de mejor manera la información. **Ajustes al proceso de búsqueda:** Si el proceso de búsqueda arroja mucha información poco útil, se adecuará para un mejor resultado.
Mediano	Capacidades del equipo	**Capacitación:** Dar las herramientas teórico-prácticas al equipo seleccionado de la DIT, para realizar una buena vigilancia tecnológica. **Prueba piloto:** Realizar una prueba piloto en la que puedan aplicar y reafirmar los conocimientos adquiridos. **Contratación de personal capacitado:** Buscar los perfiles que hagan falta cubrir y que tengan experiencia, para que la curva de adopción se reduzca al menor tiempo posible.
Bajo	Poca colaboración entre áreas	**Comunicación:** Fomentar la participación de todos los involucrados y tener apertura al diálogo.
Bajo	Selección de herramienta de vigilancia tecnológica no apropiada para la universidad	**Investigación:** Llevar a cabo una investigación adecuada de las herramientas que existen para la vigilancia, así como realizar una tabla comparativa de las elegidas y ver cuáles se adecuan más a la necesidad de la universidad. **Pruebas de las herramientas:** Realizar el análisis de las herramientas en una versión de prueba para ver el funcionamiento y cómo proporciona la información.

Fuente: Elaboración propia

7.5 Costos

Los costos considerados para el inicio de la unidad se dividen en recursos tecnológicos, y recursos humanos, en el caso de los recursos tecnológicos se considera un aproximado de $ 5,000 USD anuales, sin I.V.A. y esto solo considerando la herramienta de vigilancia tecnológica, a este supuesto se le tiene que agregar el costo de la infraestructura que, a pesar de ser dentro de las instalaciones de la universidad, estas representan un costo para la DIT.

Adicionalmente, debe considerarse el tiempo de los recursos humanos que se utilizarán de la DIT, que es la forma en la que actualmente se hace un aproximado de cuánto dinero vs. tiempo hombre costará el que estén realizando la actividad de vigilancia. Otro costo que se tiene que considerar es la contratación de proveedores o personal capacitado para el apoyo de realizar las diversas actividades.

8. Limitaciones y recomendaciones

Durante la realización de este trabajo se identificaron diversas limitaciones que influyeron tanto en el desarrollo metodológico como en la implementación y alcance de la propuesta. Estas limitaciones se pueden agrupar en tres grandes dimensiones: metodológicas, institucionales y operativas.

1. Limitaciones metodológicas:

Una de las principales restricciones surgió durante la ejecución de los grupos focales. Debido a la disponibilidad limitada de tiempo por parte de los participantes, fue necesario acortar la duración de las sesiones, lo que generó interrupciones en el flujo de ideas y limitó la profundidad del análisis. Además, algunas intervenciones pudieron estar condicionadas por factores jerárquicos, sesgos de deseabilidad social o falta de conocimiento técnico sobre los temas abordados.

En un inicio, se tenía la intención de realizar un análisis integral de toda la Dirección de Innovación y Tecnología (DIT); sin embargo, dada la complejidad de procesos, la cantidad de áreas involucradas y las restricciones de tiempo, se optó por acotar el alcance del estudio al servicio de desarrollo y mantenimiento de sitios web. No obstante, la unidad propuesta fue diseñada con una visión escalable que permitirá, en el futuro, su aplicación progresiva a otras áreas de la DIT.

2. Limitaciones institucionales:

Si bien el modelo fue presentado al director del área y a las jefaturas involucradas, y aunque se manifestó un alto grado de interés y comprensión sobre la utilidad de la unidad, aún no se ha formalizado el visto bueno institucional por escrito, lo cual es indispensable para iniciar su implementación.

Asimismo, no se ha definido de forma estructurada el alcance detallado de los entregables, como los tipos de reportes y mecanismos de seguimiento, lo que representa un pendiente para su consolidación operativa.

3. Limitaciones operativas y de recursos:

La propuesta se desarrolló en un contexto institucional particular, lo que restringe su generalización a otros entornos sin ajustes específicos. Además, el proyecto se centró en el ecosistema de sitios web informativos y transaccionales, dejando fuera, por alcance, otros elementos tecnológicos como redes, sistemas administrativos o almacenamiento.

Por otro lado, la falta de personal especializado y tiempo disponible para operar sistemáticamente una unidad de vigilancia tecnológica representa una barrera significativa para su ejecución. La alta carga operativa actual dentro de la DIT, sumada a la constante atención de tareas urgentes, limita la capacidad de dedicar recursos estables a iniciativas estratégicas como esta.

Recomendaciones a los lectores

El modelo de Vigilancia Tecnológica e Inteligencia Competitiva (VT/ITC) propuesto y validado en esta investigación ha demostrado su viabilidad dentro del contexto de la Dirección de Innovación y Tecnología (DIT) de una universidad privada. Si bien en este estudio se aplicó específicamente al servicio de sitios web, el modelo ha sido diseñado con un enfoque escalable que permite su ampliación progresiva a otros servicios tecnológicos dentro de la misma organización.

Para quienes deseen replicar o adaptar esta experiencia en otros contextos institucionales, se presentan a continuación una serie de recomendaciones prácticas, derivadas tanto del proceso de investigación como del análisis del entorno organizacional:

Realizar un diagnóstico inicial del entorno institucional

Antes de iniciar la implementación, es fundamental evaluar el estado actual de los servicios tecnológicos, identificar las necesidades prioritarias del área objetivo y establecer el grado de madurez digital de la organización. Este análisis permitirá adaptar el modelo a las capacidades reales y al ritmo de transformación institucional.

Comenzar con un enfoque acotado y escalable

Es recomendable iniciar con un ámbito específico, tal como lo fue en este caso (el servicio de sitios web), para validar procesos, herramientas y flujos de trabajo. Una vez consolidada esta fase, la unidad puede expandirse hacia otros servicios de TI de forma ordenada.

Fomentar la colaboración interdepartamental desde el inicio

La efectividad de la VT/ITC radica en el aprovechamiento del conocimiento colectivo. Por ello, se sugiere involucrar a todas las jefaturas relacionadas desde las primeras etapas del proyecto, establecer canales de comunicación eficientes y promover una cultura de colaboración entre equipos técnicos, operativos y estratégicos.

Definir con claridad los entregables y responsables

Es esencial estructurar, desde el inicio, los productos clave que generará la unidad (reportes, alertas, recomendaciones) y definir quiénes serán los responsables de su elaboración, revisión y seguimiento. Esto favorece la trazabilidad y el uso práctico de la información generada.

Asegurar el respaldo institucional formal

Contar con el visto bueno oficial y por escrito por parte de la dirección es indispensable para dotar de legitimidad, recursos y continuidad al proyecto. Se recomienda presentar una propuesta formal que incluya objetivos, beneficios esperados, requerimientos y un cronograma de implementación.

Conformar un equipo híbrido con roles bien definidos

La unidad debe contar con un equipo multidisciplinario, que combine perfiles técnicos con perfiles estratégicos alineados a los objetivos institucionales. Se sugiere iniciar con un equipo compacto pero capacitado, que pueda asumir esta función como parte de sus responsabilidades actuales.

Seleccionar herramientas tecnológicas adecuadas

Antes de adquirir plataformas o software especializado para VT/ITC, es recomendable realizar una investigación comparativa, evaluar versiones de prueba y analizar su compatibilidad con los sistemas existentes. Esto asegura una implementación más efectiva y sostenible.

Promover la capacitación y sensibilización sobre la VT/ITC

Como se evidenció en esta investigación, muchos actores desconocen los conceptos y beneficios de la VT/ITC. Por ello, es recomendable organizar talleres de sensibilización y capacitación básica para facilitar la adopción progresiva de estos enfoques.

Establecer indicadores de éxito y mecanismos de evaluación

Para monitorear el impacto de la unidad, se deben definir indicadores clave como el número de alertas procesadas, decisiones estratégicas influenciadas, riesgos mitigados o mejoras en tiempos de respuesta. Esto permitirá justificar su permanencia y evolución.

Anticipar desafíos y planificar la gestión del cambio

Es importante prever posibles barreras como la resistencia al cambio, la carga operativa del personal o la falta de recursos. Contar con un plan de gestión del cambio y estrategias de acompañamiento facilitará una integración más fluida y sostenible.

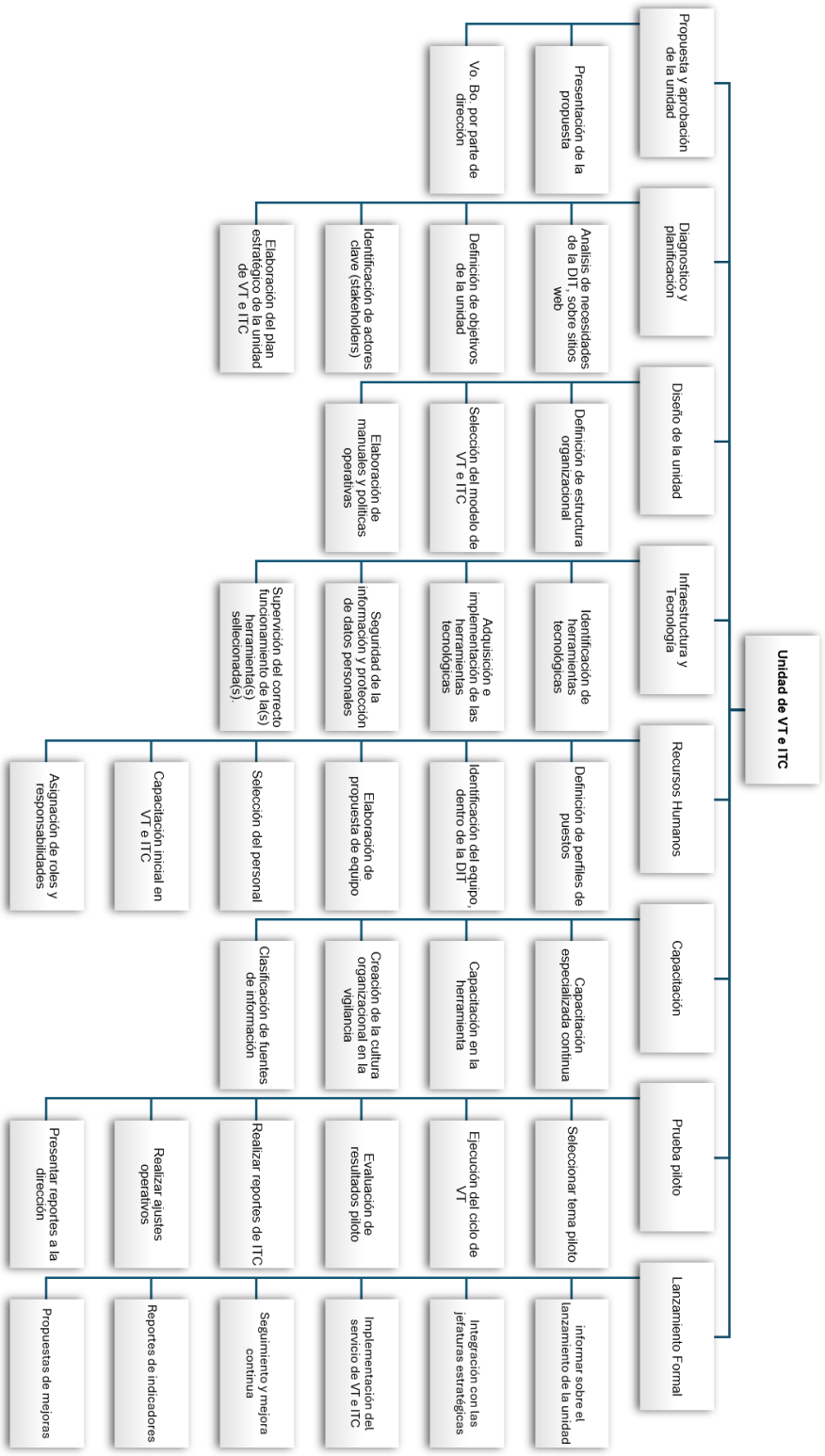
9. Conclusiones

Al realizar el trabajo para la creación de una unidad de vigilancia e Inteligencia tecnológicas competitiva dentro del área de informática en la universidad y tras el análisis exhaustivo de los resultados obtenidos, especialmente los derivados de los *focus group* y del estudio del contexto organizacional, se pueden establecer las siguientes conclusiones clave:

1. Existencia de una necesidad real y urgente de monitoreo tecnológico: El contexto actual muestra una infraestructura tecnológica diversa y, en algunos casos, obsoleta, lo cual incrementa el riesgo de brechas de seguridad, interrupciones de servicio y pérdida de competitividad digital.
2. Alta dependencia entre áreas y procesos descentralizados: Se detectó una fuerte interdependencia entre distintas jefaturas de la DIT, cada una con funciones clave en la operación y seguridad de los sitios web. Sin embargo, la coordinación entre ellas no siempre es fluida ni estructurada.
3. Valor estratégico de la vigilancia e inteligencia tecnológica: Los participantes reconocieron que contar con información anticipada sobre cambios en plataformas, versiones, amenazas o normativas representa una ventaja competitiva.
4. Resistencia al cambio como barrera a la innovación: El estudio identificó una resistencia cultural y operativa al cambio tecnológico, tanto por parte del personal técnico como de los usuarios finales.
5. Potencial de impacto positivo institucional: De concretarse la propuesta, la universidad podría optimizar recursos, reducir riesgos, mejorar la experiencia digital de su comunidad y posicionarse de manera más sólida frente a la competencia.

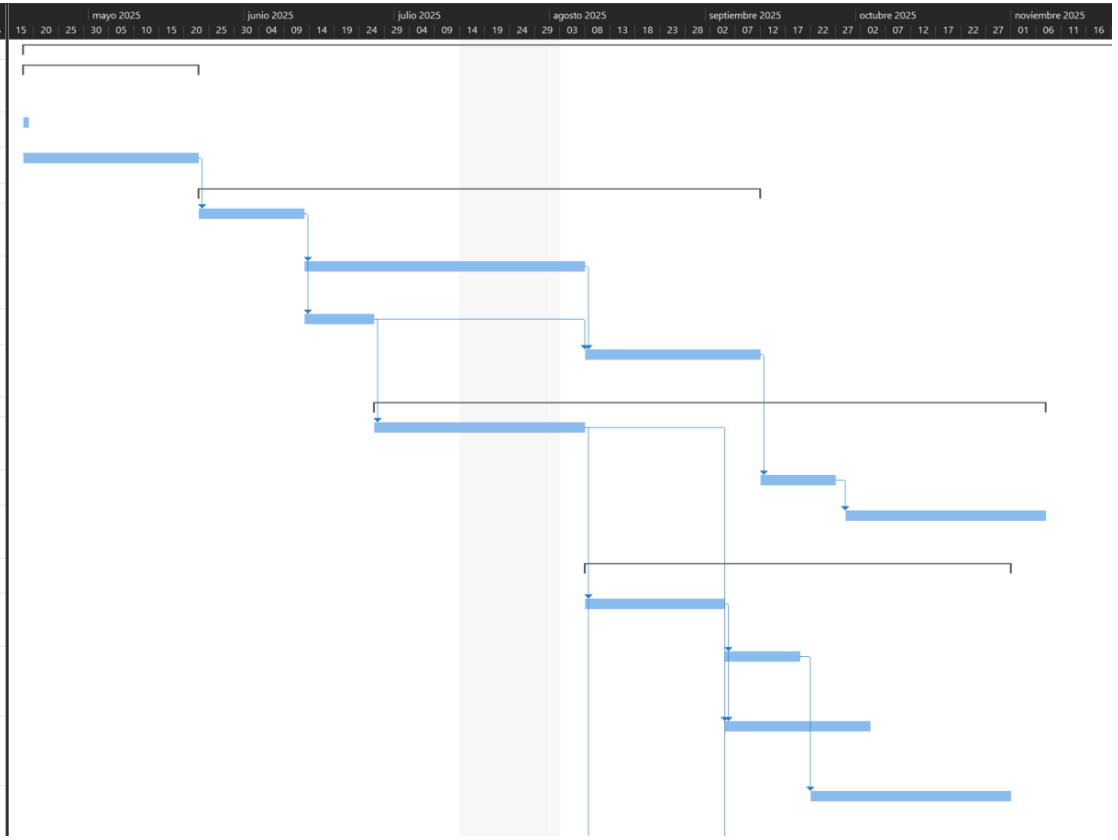
10. Anexos

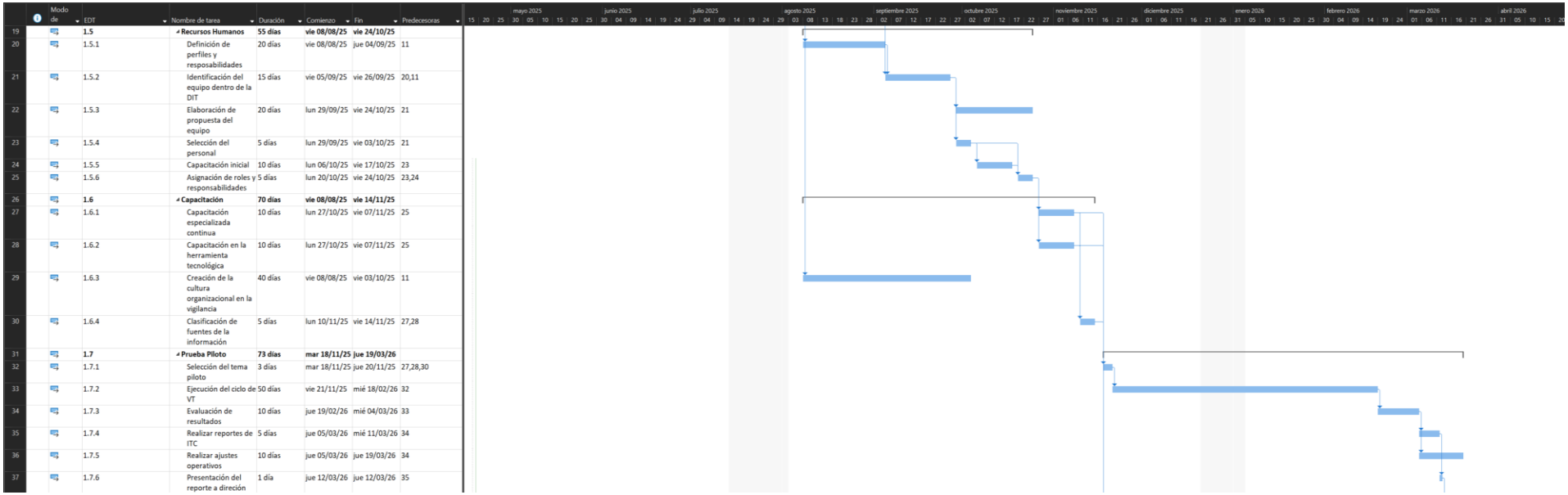
Anexo 1. Diagrama WBS



Anexo 2. Diagrama Gantt

	Modo de	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1		**1**	**Unidad de VT e ITV**	**249 días**	**vie 18/04/25**	**vie 15/05/26**	
2		**1.1**	**Propuesta y aprobación de la unidad**	**25 días**	**vie 18/04/25**	**jue 22/05/25**	
3		1.1.1	Presentación de la propuesta	1 día	vie 18/04/25	vie 18/04/25	
4		1.1.2	Vo. Bo. Por parte de dirección	25 días	vie 18/04/25	jue 22/05/25	
5		**1.2**	**Diseño y planificacion**	**65 días**	**vie 23/05/25**	**jue 11/09/25**	
6		1.2.1	Analisis de necesidades para los sitios web	15 días	vie 23/05/25	jue 12/06/25	4
7		1.2.2	Definición de los objetivos de la unidad	25 días	vie 13/06/25	jue 07/08/25	6
8		1.2.3	Identificación de actores claves	10 días	vie 13/06/25	jue 26/06/25	6
9		1.2.4	Elaboración del plan estrategico de la unidad de VT e ITC	25 días	vie 08/08/25	jue 11/09/25	7,8
10		**1.3**	**Diseño de la unidad**	**80 días**	**vie 27/06/25**	**vie 07/11/25**	
11		1.3.1	Definicion de la estructura organizacional	15 días	vie 27/06/25	jue 07/08/25	8
12		1.3.2	Selección del modelo de VT e ITC	10 días	vie 12/09/25	vie 26/09/25	9
13		1.3.3	Elaboración de manuales y politicas operativas	30 días	lun 29/09/25	vie 07/11/25	12
14		**1.4**	**Infraestructura y Tecnológia**	**60 días**	**vie 08/08/25**	**vie 31/10/25**	
15		1.4.1	Identificación de las herramientas tecnológicas	20 días	vie 08/08/25	jue 04/09/25	11
16		1.4.2	Adquisición e implementacion de las herramientas tecnologicas	10 días	vie 05/09/25	vie 19/09/25	15
17		1.4.3	Seguridad de la información y protección de datos personales	20 días	vie 05/09/25	vie 03/10/25	11,15
18		1.4.4	Supervisión del correcto funcionamiento	30 días	lun 22/09/25	vie 31/10/25	16





	Modo de	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
19		**1.5**	**Recursos Humanos**	**55 días**	**vie 08/08/25**	**vie 24/10/25**	
20		1.5.1	Definición de perfiles y responsabilidades	20 días	vie 08/08/25	jue 04/09/25	11
21		1.5.2	Identificación del equipo dentro de la DIT	15 días	vie 05/09/25	vie 26/09/25	20,11
22		1.5.3	Elaboración de propuesta del equipo	20 días	lun 29/09/25	vie 24/10/25	21
23		1.5.4	Selección del personal	5 días	lun 29/09/25	vie 03/10/25	21
24		1.5.5	Capacitación inicial	10 días	lun 06/10/25	vie 17/10/25	23
25		1.5.6	Asignación de roles y responsabilidades	5 días	lun 20/10/25	vie 24/10/25	23,24
26		**1.6**	**Capacitación**	**70 días**	**vie 08/08/25**	**vie 14/11/25**	
27		1.6.1	Capacitación especializada continua	10 días	lun 27/10/25	vie 07/11/25	25
28		1.6.2	Capacitación en la herramienta tecnológica	10 días	lun 27/10/25	vie 07/11/25	25
29		1.6.3	Creación de la cultura organizacional en la vigilancia	40 días	vie 08/08/25	vie 03/10/25	11
30		1.6.4	Clasificación de fuentes de la información	5 días	lun 10/11/25	vie 14/11/25	27,28
31		**1.7**	**Prueba Piloto**	**73 días**	**mar 18/11/25**	**jue 19/03/26**	
32		1.7.1	Selección del tema piloto	3 días	mar 18/11/25	jue 20/11/25	27,28,30
33		1.7.2	Ejecución del ciclo de VT	50 días	vie 21/11/25	mié 18/02/26	32
34		1.7.3	Evaluación de resultados	10 días	jue 19/02/26	mié 04/03/26	33
35		1.7.4	Realizar reportes de ITC	5 días	jue 05/03/26	mié 11/03/26	34
36		1.7.5	Realizar ajustes operativos	10 días	jue 05/03/26	jue 19/03/26	34
37		1.7.6	Presentación del reporte a dirección	1 día	jue 12/03/26	jue 12/03/26	35

	Modo de	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
38		**1.8**	**Lanzamiento formal**	**114 días**	**mar 18/11/25**	**vie 15/05/26**	
39		1.8.1	Informar sobre el lanzamiento de la unidad	10 días	vie 13/03/26	vie 27/03/26	37
40		1.8.2	Integración con las jefaturas estratégicas	10 días	mar 18/11/25	lun 01/12/25	30
41		1.8.3	Implementación del servicio de VT e ITC	15 días	lun 30/03/26	vie 17/04/26	39
42		1.8.4	Seguimiento y mejora continua	10 días	lun 20/04/26	vie 01/05/26	41
43		1.8.5	Reportes de indicadores	5 días	lun 20/04/26	vie 24/04/26	41
44		1.8.6	Propuestas de mejoras	10 días	lun 04/05/26	vie 15/05/26	41,42,43

Bibliografía

Ardiles Briones, M. y. (15 de abril de 2021). *Modelos de Vigilancia Tecnológica aplicables al ámbito de la Educación Superior en Chile*. Obtenido de Ciencia y Técnica Administrativa - CyTA: https://www.cyta.com.ar/ta/article.php?id=200206

Armijos Ortega, G. A. (2019). *Michel Godet: El prospectivista de la prospectiva y la permanente efectividad de su método en el siglo XXI. Revista TÁMBARA, 14(2), 63–78*. Obtenido de Michel Godet: El prospectivista de la prospectiva y la permanente efectividad de su método en el siglo XXI. Revista TÁMBARA, 14(2), 63–78: https://tambara.org/wp-content/uploads/2019/09/4.prospectiva-M.Godet-Final_Armijos_Ortega_final.pdf

BAI Agencia de Innovación. (2007). *Modelos de Vigilancia tecnológica e inteligencia competitiva.* BAI agencia de innovación.

base22. (s.f.). Obtenido de https://base22.com/es/blog-es/retos-transformacion-digital-en-educacion-superior/

Buzzi, G. (11 de mayo de 2023). *Las 4 herramientas de análisis estratégico que toda empresa debería utilizar.* Obtenido de LinkedIn: https://es.linkedin.com/pulse/las-4-herramientas-de-an%C3%A1lisis-estrat%C3%A9gico-que-toda-empresa-buzzi

Carmona, R. (17 de noviembre de 2023). *Magnet*. Obtenido de Magnet: https://www.magnetmex.com/tecnologia/el-costo-oculto-de-la-tecnologia-obsoleta-en-el-trabajo/

e-intelligent. (15 de Septiembre de 2022). *e-intelligent*. Obtenido de e-intelligent: https://www.e-intelligent.es/es/blog/inteligencia-competitiva/caso-de-exito-analisis-de-vigilancia-tecnologica-e-inteligencia-competitiva-en-el-sector-de-las-criptomonedas/

FPNTI. (2014). Modelo Nacional de Gestión de tecnología e Innovación. 16a. ed. Fundación Premio Nacional de Tecnología e Innovación.

Fundación Premio Nacional de Tecnilogía, A. (2015). Modelo Nacional de Gestión de Tecnología e Innovación, edición 15.

García, M. (22 de Marzo de 2023). *Blog de Blog de maestrias y doctorados de TEC*. Obtenido de Tecnológico de Minterrey : https://blog.maestriasydiplomados.tec.mx/innovacion-tecnologica-que-es-sus-tipos-y-sus-beneficios

Goya Soluciones. (s.f.). *GOYA Soluciones Informáticas*. Obtenido de La tecnología avanza a un ritmo difícil de seguir: https://www.goyasoluciones.com/la-tecnologia-avanza-a-un-ritmo-dificil-de-seguir/

Gtz, S. T. (s.f.). *Modelo de Innovación Temaguide*. Obtenido de salvatapia.com: https://salvatapia.com/innovacion/modelo-de-innovacion-temaguide/#:~:text=El%20Modelo%20Temaguide%20(COTEC%2C%201998).&text=El%20Temaguide%20es%20una%20gu%C3%ADa,%2C%20recursos%2C%20implementaci%C3%B3n%20y%20aprendizaje.

Guía de Vigilancia e Inteligencia Tecnológica. (s.f.). Obtenido de Observatorio tecnológico UA: https://www.ovtt.org/guias/guia-de-inteligencia-tecnologica/

Gutiérrez, A. (4 de Diciembre de 2023). *Cidei*. Obtenido de Cidei.net: https://cidei.net/vigilancia-tecnologica-en-el-sector-financiero/

Gutiérrez, A. (15 de agosto de 2023). *El proceso de la vigilancia tecnológica y cómo implementarla*. Obtenido de Cidei: https://cidei.net/proceso-de-la-vigilancia-tecnologica/

Henderson, J. (2023). Estrategia de Innovación [Diapositivas de PowerPoint]. *Análisis Estratégico de la Tecnología*. Universidad Iberoamericana.

Herrera-Mendoza, A. (. (20223). *Gestión de la Innovación Tecnologica. Del aula a las soluciones.* México: Universidad Iberoamericana.

Impactum. (08 de Septiembre de 2023). *Improvitz*. Obtenido de Impactum: https://impactum.mx/sitios-web-universitarios-optimos-experiencia-digital-destacada/

Instituto Nacional de Salud Pública. (s.f.). *Los riesgos del estrés laboral para la salud*. Obtenido de INSPN: https://www.insp.mx/avisos/3835-riesgos-estres-laboral-salud.html

Kaspersky. (11 de Marzo de 2021). *latam.kaspersky.com*. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/about/press-releases/el-47-de-las-empresas-latinoamericanas-utiliza-tecnologia-obsoleta-dentro-de-su-infraestructura-de-ti-revela-kaspersky

LISA Institute. (s.f.). *¿Qué es la Vigilancia Tecnológica? Tipos y ejemplos [Guía Práctica]*. Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/que-es-la-vigilancia-tecnologica-tipos-ejemplos?srsltid=AfmBOor0oCp_itSz0ZMgTdKwFu2UbYy__iHOkAybCb1W8a7nKe9CCYHz

miro. (s.f.). *Roadmap tecnológico*. Obtenido de miro: https://miro.com/es/planificacion-estrategica/que-es-roadmap-tecnologico/

Obsera, Observatorio Tecnológico UA. (s.f.). *Publicada la nueva Norma UNE 166006:2018 sobre sistemas de vigilancia e inteligencia*. Obtenido de Obsera, Observatorio Tecnológico UA: https://www.ovtt.org/publicada-la-nueva-norma-une-1660062018-sobre-sistemas-de-vigilancia-e-inteligencia/

Observa. (s.f.). *Guía de Vigilancia e Inteligencia Tecnológica*. Obtenido de Observatorio tecnológico UA: https://www.ovtt.org/guias/guia-de-inteligencia-tecnologica/

Observatorio Virtual de Transferencia de Tecnología. (19 de enero de 2025). *¿Qué resultados podemos esperar de la vigilancia tecnológica?* Obtenido de Observatorio Virtual de Transferencia de Tecnología: https://moocvt.ovtt.org/que-resultados-podemos-esperar-de-la-vigilancia-tecnologica/

Petróleo, I. M. (27 de Marzo de 2017). *Organo interno informativo electrónico*. Obtenido de Gobierno de México: https://www.gob.mx/cms/uploads/attachment/file/204301/G102bis.pdf

Prospektiker, M. G. (Enero de 2007). *Prospectiva Estratégica: problemas y métodos.* Obtenido de Prospectiva Estratégica: problemas y métodos: https://archivo.cepal.org/pdfs/GuiaProspectiva/Godet2007.pdf

Redacción Portal ERP México. (11 de 12 de 2024). *Redacción Portal ERP México*. Obtenido de Portal ERP: https://portalerp.com.mx/sectores-mas-atacados-en-mexico-durante-2024-cloudflare

Roadmap: Qué es, tipos y cómo hacerlo. (24 de junio de 2024). Obtenido de Pango Studio: https://pangostudio.com/roadmap-que-es-tipos-y-como-hacerlo/

Roberto Marijuán, L. (30 de noviembre de 2015). *Webinar "Vigilancia Tecnológica: ¿Por dónde empezar?"*. Obtenido de Webinar "Vigilancia Tecnológica: ¿Por dónde empezar?": https://www.youtube.com/watch?v=6xL-XJVryx0

Sánchez, J. L. (2023). *Biblioteca Francisco Xavier Clavigero.* Obtenido de https://www.bib.ibero.mx/tesis/pdf/017562/017562.pdf

Schwartz, E. (s.f.). *The Art of the Long View: Planning for the Future in an Uncertain World.* Obtenido de https://archive.org/details/artoflongview00schw

SYDLE. (11 de 09 de 2023). Obtenido de Blog SYDLE: https://www.sydle.com/es/blog/tipos-de-innovacion-619541bf351e93287c42a7de

SYDLE. (20 de Junio de 2023). *SYDLE*. Obtenido de SYDLE: https://www.sydle.com/es/blog/ley-de-difusion-de-la-innovacion-61829eca3885651fa294b9e6

Velázquez, A. (s.f.). *¿Qué es el método Delphi?* Obtenido de QuestionPro: https://www.questionpro.com/blog/es/metodo-delphi/

Villalpando, J. H. (2023). Vigilancia Tecnológica Inteligencia Tecnológica Competitiva [Diapositivas en PDF]. *Análisis estratégico de la tecnología*. Universisis Iberoamericana.

WebFX. (2025). *WebFX*. Obtenido de Digital Marketing that Drives Revenue: https://www.webfx.com/web-design/statistics/

“Para la redacción y revisión de este documento se utilizó la herramienta de inteligencia artificial ChatGPT, desarrollada por OpenAI, como apoyo para la estructuración de ideas, redacción preliminar de textos y sugerencias de estilo académico.”