UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Training en departamento de IT

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Tadeo Moises Sepúlveda Vargas

ASESOR DE INFORME

Ing. Roberto Federico Mandujano Wild

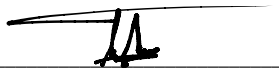
Ciudad Universitaria, Cd. Mx., 2025

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado TRAINING EN DEPARTAMENTO DE IT que presenté para obtener el titulo de INGENIERO EN TELECOMUNICACIONES es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.



TADEO MOISES SEPULVEDA VARGAS
Número de cuenta: 418046021

DEDICATORIA

A mis padres y mi hermano, por haberme apoyado para llegar a ser la persona que soy en la actualidad; gran parte de mis logros incluyendo este, sin su apoyo no los hubiera logrado realizar.

AGRADECIMIENTOS

En primer lugar agradezco a mis padres por el apoyo incondicional brindado para poder llevar a cabo mis objetivos personales y académicos. Siempre me han impulsado a perseguir mis metas y nunca abandonarlas ante posibles adversidades.

A mi hermano, por el apoyo y consejos que me ha proporcionado cuando situaciones difíciles se me han presentado.

Agradezco profundamente a mi tutor el Ing. Roberto Mandujano Wild por su dedicación y paciencia, ya que, sin sus palabras y correcciones precisas, no hubiese podido lograr llegar a esta importante instancia tan deseada.

Son muchos docentes que han sido parte de mi formación profesional, y a todos ellos les quiero agradecer por transmitirme los conocimientos necesarios que me permitieron hoy llegar a donde estoy, principalmente a la maestra Maricela Castañeda Perdomo que me apoyo en momentos difíciles de la carrera para lograr concretarla.

Por último, agradezco a la Universidad Nacional Autónoma de México por el alto nivel de exigencia, pero que al mismo tiempo me enseñó a enfrentar situaciones donde fue necesario aplicar ingenio para lograr sacarlas adelante y con ello, me ha permitido obtener mi título profesional.

ÍNDICE

CAPITULO 1. INTRODUCCIÓN

Objetivos

El objetivo principal de este documento parte de demostrar los conocimientos adquiridos a lo largo de la carrera, a partir de los resultados obtenidos de manera practica en un entorno laboral relacionado al área de IT (del inglés, Tecnologías de la Información).

Los objetivos del programa trainee realizado consisten principalmente en proporcionar soporte a la infraestructura de una empresa, dar soluciones de manera eficiente por medio de un análisis de datos realizado previamente a incidentes relacionados con ciberseguridad y crear soluciones por medio de software donde el usuario final tenga presente una interfaz sencilla como amigable.

Descripción de la empresa y puesto de trabajo

El trabajo realizado como trainee fue dentro de una empresa de tecnología con presencia global enfocada en la industria, las infraestructuras, el transporte y la salud. Desde fábricas más eficientes en recursos, cadenas de suministro resilientes y edificios y redes más inteligentes, hasta un transporte más limpio y cómodo, así como atención médica avanzada, con tecnología con el propósito de agregar valor real para los clientes.

La empresa se encuentra posicionada dentro del top 100 Compañías nivel mundial, a lo largo de la cadena de valor de la electrificación, desde la generación de energía, la transmisión y la distribución hasta las soluciones de redes inteligentes y la aplicación eficiente de la energía eléctrica, así como en las áreas de diagnóstico por imágenes y diagnóstico de laboratorio.

Antecedentes

Las divisiones de la Compañía donde se realizaron las actividades fueron IT, Ciberseguridad y Desarrollo de Software, que a su vez se subdividen en diversas áreas. Para cada división se asignó una estadía de 2 meses para completar las actividades, dando un total de 6 meses para la capacitación.

Se proporcionó por parte de la empresa el equipo y licenciamiento necesario para la realización de las actividades, y posteriormente para cubrir nuevas necesidades que surgieron.

Definición del problema

Cada área dependiendo de la rotación asignada en ese momento como trainee, requería de apoyo en diversas actividades, las cuales principalmente estaban involucradas en el campo de las tecnologías de la información (del inglés, *IT*), entre las cuales además de proporcionar soporte al usuario final (en este caso, los empleados de la misma empresa), era necesario demostrar conocimiento de los conceptos principalmente utilizados en el área de IT, por ello para lograr esto a cabo, me proporcionaron cursos en línea y para complementar el conocimiento adquirido se realizaban actividades prácticas.

En el caso de que el área en turno requiriera la implementación de una herramienta para optimizar determinados procesos, era necesario por parte del trainee proporcionar diferentes soluciones y a partir de una de estas, llegar a la más eficiente para dar una respuesta concreta al problema.

Finalmente, se realizaron 2 casos durante la rotación de ciberseguridad, por medio de los cuales se ejemplificaron aplicaciones para el análisis de infraestructura de red a partir del lenguaje Python, con la finalidad de conocer detalladamente la información del entorno al cual nos encontramos conectados con nuestro dispositivo.

Contexto de la participación profesional

Mi participación en este proyecto se divide en tres partes:

1. Análisis de la situación: Partiendo de una necesidad en particular para cada área donde se realizó la rotación, se determinaron los requisitos para poder resolver cada distinta situación: estás podían ser soft skills y/o hard skills. Teniendo los requisitos establecidos, se procedió a solicitar autorización por parte del jefe directo en cada rotación para establecer un plan de acción, por medio del cual se plantearía una solución.

2. Plan de acción: Teniendo los requisitos establecidos y el procedimiento tanto determinado como autorizado, se procedió a ponerlo en práctica para dar solución al problema. Por cada actividad realizada, siempre se llevó a cabo el lineamiento establecido y tener por escrito cada autorización solicitada que fuera requerida con copia al jefe inmediato, principalmente como prueba de que se siguió línea por línea cada uno de los pasos que involucraba el procedimiento, y en caso de algún posible accidente quedaría documentado. En caso de requerir alguna herramienta adicional al procedimiento establecido, se asistía directamente con el jefe directo para su solicitud, ya que dependiendo del área el costo de la misma era absorbida por un centro de costos distinto.

3. Recopilación de las actividades realizadas: Una vez que todas las actividades asignadas fueran completadas, era necesario realizar una revisión de cada una para verificar que en el caso de que una de ellas hubiera sido omitida o quedara incompleta, era necesario re-agendar la actividad para su posterior realización. Para ciertas actividades se proporcionaba retroalimentación, en caso de que alguna observación fuera necesaria de notificar para mejorar el rendimiento en posteriores asignaciones.

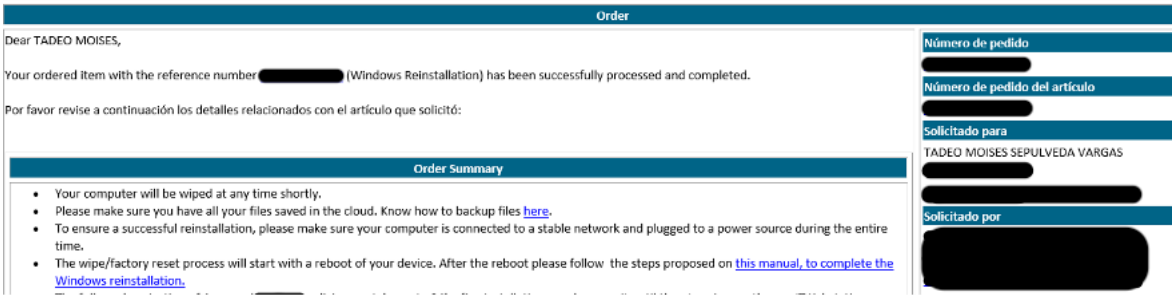
CAPITULO 2. SOPORTE A USUARIOS EN IT

Descripción de las funciones y responsabilidades

El principal objetivo del departamento de IT, consiste en ser responsable de mantener y gestionar la infraestructura tecnológica de la empresa, que generalmente incluye equipos informáticos, redes, servidores, sistemas de almacenamiento y diversos componentes de hardware y software necesarios para el funcionamiento de la misma.

Como parte del programa trainee, se realizaron las siguientes funciones:

1. Soporte técnico: se proporcionó ayuda a los usuarios finales con problemas de hardware y software, resolución de incidencias (tickets) y de acuerdo al tipo de situación, en algunas ocasiones se brindó asistencia por medio de seguimiento con el usuario para garantizar que los sistemas informáticos como sus aplicaciones funcionaran correctamente. Estas resoluciones son como se muestran en la imagen 1.


Order

Dear TADEO MOISES,

Your ordered item with the reference number [redacted] (Windows Reinstallation) has been successfully processed and completed.

Por favor revise a continuación los detalles relacionados con el artículo que solicitó:

Order Summary

- Your computer will be wiped at any time shortly.
- Please make sure you have all your files saved in the cloud. Know how to backup files here.
- To ensure a successful reinstallation, please make sure your computer is connected to a stable network and plugged to a power source during the entire time.
- The wipe/factory reset process will start with a reboot of your device. After the reboot please follow the steps proposed on this manual, to complete the Windows reinstallation.

Número de pedido [redacted]

Número de pedido del artículo [redacted]

Solicitado para

TADEO MOISES SEPULVEDA VARGAS [redacted]

Solicitado por [redacted]

Imagen 1. Ticket de incidencia elaborado por el autor

2. Planificación estratégica: partiendo de las necesidades tecnológicas detectadas y tomando en consideración los objetivos estratégicos de la empresa, se identificaron posibles soluciones que pudieran aportar una mejora en eficiencia y con ello, se elaboró documentación con una ruta tecnológica a largo plazo que permitiera una transición sencilla de las herramientas actuales a las nuevas.

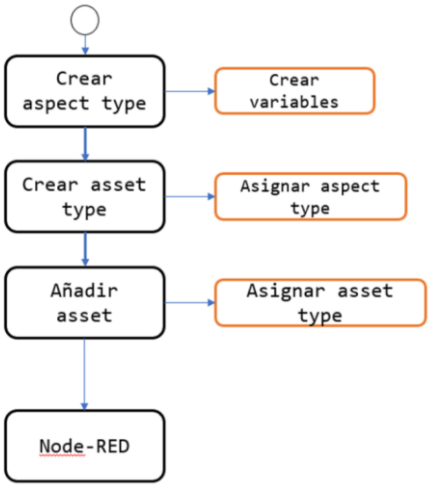


Imagen 2. Diagrama de planificación elaborado por el autor.

3. Gestión de proyectos: al ser un departamento involucrado en su totalidad con la infraestructura tecnológica de la empresa, fue necesario supervisar la implementación de las soluciones a través de proyectos, entre las cuales principalmente se encontraron actualizaciones de software, desarrollo de aplicaciones, migraciones de datos, entre otros. Fue crucial el seguimiento a los proyectos tal como se muestra en la imagen 3, por medio de objetivos en plazos determinados y presupuestos establecidos para lograr los resultados deseados.

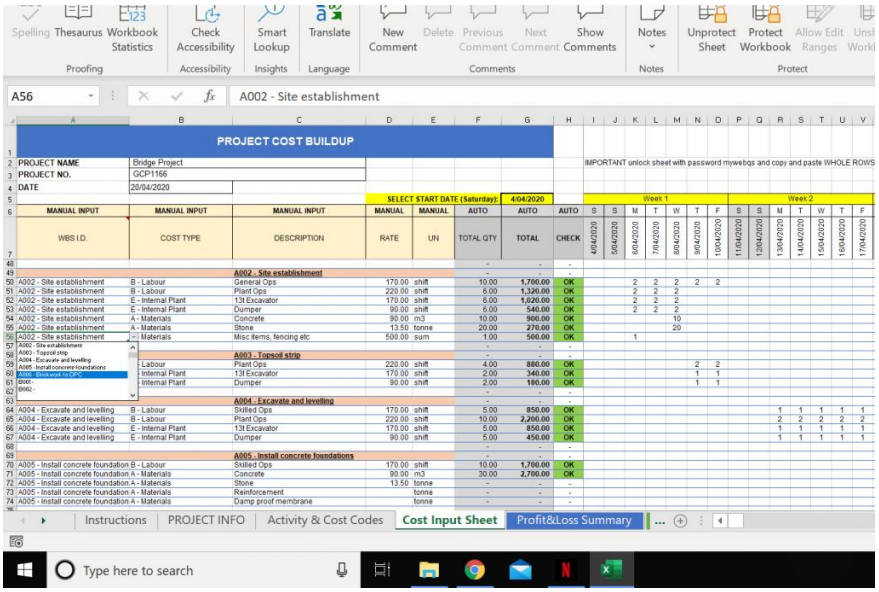


Imagen 3. Tabla de gastos por proyecto propuesto por el autor [1].

Identificación de los principales retos y dificultades en el desempeño del trabajo

Al pertenecer a este departamento uno se encuentra con diversos retos, ya que, al ser centralizado, en otras palabras, cualquier acción que se pueda a llevar a cabo generalmente involucraba interacción con otros departamentos y por ello implicaba realizar un análisis previo a la ejecución de la misma para conocer los posibles riesgos, tanto técnicos como financieros, que podrían presentarse para ambas partes al momento de ponerse en acción.

Entre los principales desafíos que se encontraron al momento de la rotación, destacaron los siguientes:

1. Seguridad de la información: La seguridad es un desafío contante en el departamento de IT dado que frecuentemente se maneja información sensible. Es necesario estar al tanto de las últimas técnicas y herramientas de seguridad existentes en el mercado para proteger los sistemas y datos de la empresa de posibles vulnerabilidades existentes.

2. Complejidad de la infraestructura existente y presión por plazos: Dado el tamaño global de la empresa, generalmente los sistemas y su infraestructura estaban compuestos por una variedad extensa de componentes interdependientes. El mantenimiento y gestión de esta complejidad en gran parte de las ocasiones representa un desafío ya que no es posible que su funcionalidad se vea interrumpida, principalmente en el caso de implementaciones de arquitecturas basadas en la nube. Siempre existe el riesgo de que surja una incidencia o problema técnico en cualquier momento al incorporar un nuevo componente, por ello es necesario contar con una respuesta rápida para minimizar el tiempo inactivo y permitir un funcionamiento constante de los sistemas.

3. Gestión del cambio y avances tecnológicos: El campo de la tecnológica avanza rápidamente, y a consecuencia de ello también las amenazas se vuelven más peligrosas. Es necesario mantenerse actualizado con las últimas tendencias y tecnologías emergentes, representando un importante desafío ya que implica en gran parte aprender nuevas habilidades y una adaptabilidad rápida ante los posibles cambios. Al incorporar nuevas tecnologías o sistemas, se puede encontrar resistencia al cambio por parte de los empleados y a consecuencia de ello, los profesionales del departamento de IT deben saber comunicar adecuadamente los

beneficios que estos cambios podrían representar, siempre dando prioridad a la capacitación de los empleados para garantizar una transición exitosa y transparente.

4. Recursos limitados: Debido a la existencia de un presupuesto anual en cada departamento de la empresa, esto implica también que para el departamento de IT cada decisión incorporará un costo y representara una posible dificultad para la adquisición de herramientas, talento y tecnologías necesarias para llevar a cabo tareas y proyectos de manera eficaz.

Los desafíos previamente mencionados son solo algunos de los que actualmente existen y se enfrentan diariamente en el departamento de IT, por ello es importante contar con una planificación adecuada para mitigar cualquier posible afectación. Cabe mencionar que esto no exenta de adquirir habilidades relevantes y un enfoque adecuado para la resolución de problemas, ya que sin ambos importantes factores no es posible superar un reto de la manera más efectiva y sencilla.

Análisis de las habilidades y competencias necesarias

Para tener éxito en el campo de la IT, es necesario tener una variedad de habilidades y competencias. Los profesionales de IT necesitan un conjunto de habilidades diversas para sobresalir en la industria en constante cambio. Algunas de las habilidades y competencias clave necesarias para el éxito en IT son las siguientes:

1. Propiedad técnica: En IT una base sólida en habilidades técnicas es esencial. Esto puede incluir conocimientos de lenguajes de programación, sistemas operativos, bases de datos, protocolos de red, computación en la nube, ciberseguridad y otras tecnologías relevantes.
2. Habilidades de solución de problemas: Los profesionales de IT se enfrentan con frecuencia a problemas y desafíos complejos. El éxito depende de la capacidad de analizar los problemas, identificar las causas fundamentales y crear soluciones efectivas.
3. Los profesionales de IT deben comprometerse con el aprendizaje continuo debido a la naturaleza cambiante de la tecnología. Para realizar el trabajo, uno debe mantenerse al día con las últimas tendencias y desarrollos en la industria.

4. Los entornos de IT pueden ser impredecibles. Los profesionales deben ser adaptables y flexibles para manejar las tecnologías cambiantes, los requisitos del proyecto y los eventos imprevistos.
5. Atención al detalle: Los errores en IT pueden tener efectos significativos. La atención al detalle es fundamental para garantizar la precisión y evitar errores importantes.
6. Habilidades de comunicación: Para que los profesionales de IT puedan colaborar con los miembros del equipo, las partes interesadas y los clientes, es esencial que se comuniquen bien. Es especialmente importante poder explicar conceptos técnicos a personas no técnicas.
7. Gestión de proyectos: Los proyectos de IT con frecuencia involucran diversas actividades, plazos y miembros de equipo. La competencia en la gestión de proyectos garantiza que los proyectos se lleven a cabo a tiempo, dentro del presupuesto y cumplan los objetivos.
8. Habilidades de solución de problemas: una competencia clave es identificar y resolver problemas técnicos de manera eficiente. Las habilidades de solución de problemas permiten a los profesionales de IT detectar problemas y restaurar los servicios rápidamente.
9. Creatividad e Innovación: Los profesionales de IT deben ser creativos para resolver problemas, encontrar soluciones innovadoras a los problemas e investigar nuevas tecnologías y enfoques.
10. Concientización de la ciberseguridad: Comprender las amenazas y las mejores prácticas de ciberseguridad es esencial para proteger los sistemas, los datos y la información sensible de posibles violaciones.
11. Trabajo en equipo y colaboración: Los proyectos de IT a menudo involucran equipos interdisciplinarios. El éxito depende de la capacidad de trabajar adecuadamente con otros, compartir información y colaborar eficazmente.
12. Conducta ética: Los profesionales de IT frecuentemente manejan datos sensibles y tienen acceso a sistemas críticos. Demostrar comportamiento ético, honesto y responsable en el manejo de la información es crucial.
13. Administración del tiempo: Para garantizar la eficiencia y la productividad, es necesario tener excelentes habilidades de gestión del tiempo para organizar varias tareas y prioridades.
14. Atención al Cliente: Para ofrecer soluciones que satisfagan sus necesidades, los profesionales de IT deben ser orientados al cliente y comprender las necesidades de los usuarios finales y los clientes.
15. Business Acumen: Comprender el contexto empresarial más amplio y alinear las iniciativas de IT con los objetivos de la organización ayuda al éxito de los profesionales de IT y al éxito general de la empresa.

Las personas pueden tener éxito en el campo dinámico y gratificante de la tecnología de la información al desarrollar y perfeccionar estas habilidades y competencias, empleando los diferentes medios que forman parte del dia a dia en esta área tal como se conceptualiza en la imagen 4.

Imagen 4. Conceptualización de habilidades y competencia necesarias [2].

CAPITULO 3. PROYECTOS DE AUTOMATIZACIÓN

Contexto de la situación actual

La automatización se ha convertido en un factor clave para la eficiencia y la productividad en los proyectos de IT en el entorno tecnológico en rápida evolución de hoy. La automatización promete optimizar la asignación de recursos, reducir los errores humanos y racionalizar los procesos. Las organizaciones deben considerar cuidadosamente la automatización de tareas en los proyectos de IT a pesar de sus innegables ventajas. Para tomar decisiones informadas y garantizar que las iniciativas de automatización produzcan los resultados deseados al tiempo que protejan contra posibles trampas, es fundamental comprender estos riesgos. Algunos de los peligros asociados con la automatización de tareas en proyectos de IT son:

1. Personal: El desplazamiento de personal es uno de los principales riesgos de la automatización de tareas en los proyectos de IT. A medida que se automatizan las tareas cotidianas y repetitivas, ciertas tareas pueden convertirse en redundantes, lo que puede resultar en pérdidas de empleo o incluso desempleo.
2. Aumento de errores: La automatización acelera los errores. Los errores en los procesos automatizados pueden propagarse rápidamente y causar interrupciones del sistema, pérdidas financieras y problemas generalizados.
3. Excesiva dependencia de la tecnología: Depender demasiado de la automatización puede hacer que las organizaciones sean vulnerables a fallas del sistema, fallas técnicas o ataques cibernéticos. La falta de intervención humana podría impedir la resolución oportuna y poner en peligro la continuidad del negocio.
4. Vulnerabilidad de seguridad: Si los procesos automatizados no están adecuadamente protegidos, pueden ser susceptibles a vulnerabilidades de seguridad. Los sistemas de automatización que no están configurados correctamente pueden exponer infraestructuras de IT críticas y datos sensibles, lo que puede comprometer la privacidad de los datos y la integridad de la organización.
5. Falta de adaptabilidad: Algunos procesos automatizados no son adaptables, lo que dificulta adaptarse a las necesidades cambiantes de la empresa o a los cambios imprevistos. Las empresas pueden encontrar dificultades para adaptar sus flujos de trabajo automatizados a las necesidades cambiantes.

6. Disminución de la interacción humana: Una automatización excesiva puede resultar en menos interacción humana con los clientes o usuarios finales, lo que reduce el toque personal y puede afectar la satisfacción y la lealtad de los usuarios.
7. Dilemas éticos: La automatización en los proyectos de IT plantea preguntas éticas sobre la privacidad de los datos, el uso responsable de la IA y los efectos sociales potenciales en el empleo y el bienestar humano.
8. Implementación compleja: Introducir la automatización en los proyectos de IT puede ser un esfuerzo complicado que requiere planificación, inversión y experiencia significativas. Las implementaciones mal ejecutadas pueden retrasar el proyecto, sobrecargar los costos y obtener resultados insatisfactorios.
9. Resistencia al cambio: Los empleados pueden evitar la automatización porque temen desplazarse o no saben cómo adaptarse a las nuevas tecnologías. La resistencia puede impedir que los procesos automatizados se integren y adopten con éxito.
10. Integración del sistema legado: Integrar la automatización con los sistemas legados existentes puede resultar difícil, requerir recursos adicionales y posiblemente causar problemas de compatibilidad que impiden el progreso general del proyecto.
11. Cumplimiento de las leyes: Los procesos automatizados deben cumplir con las leyes del sector y las leyes de protección de datos. El incumplimiento tiene consecuencias legales y puede dañar la reputación de una empresa.
12. Riesgos: Un solo punto de fracaso es la dependencia excesiva de la automatización. Los errores técnicos o fallas en el sistema pueden tener efectos en cascada en varios procesos interconectados.

En conclusión, aunque la automatización tiene muchos beneficios para los proyectos de IT, es importante comprender y reducir los riesgos asociados para que funcione adecuadamente. Para aprovechar todo el potencial de la automatización y protegerse contra posibles trampas e incertidumbres, es fundamental encontrar el equilibrio adecuado entre la automatización y la intervención humana.

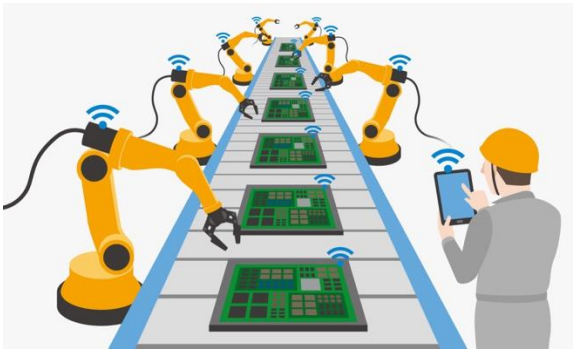


Imagen 5. Conceptualización de la automatización laboral [3]

Conceptos básicos de bases de datos y su importancia en la gestión de información empresarial

Las bases de datos se desarrollan en respuesta a las necesidades de las organizaciones para gestionar datos y mejorar la eficiencia de los sistemas informáticos. Los datos y la información son conceptos distintos, siendo los datos la materia prima para la creación de información. Para maximizar la utilidad de la información, las organizaciones deben gestionarla adecuadamente, considerando los costos asociados a su producción, distribución, seguridad, almacenamiento y recuperación.

Los sistemas de información operan de manera similar, incluyendo la introducción, procesamiento, obtención y almacenamiento de datos. Estos sistemas se utilizan en diversas áreas funcionales de una organización, como contabilidad, finanzas, recursos humanos y producción. Cada área utiliza sistemas de información específicos para sus necesidades, como sistemas de contabilidad para registrar transacciones financieras y sistemas de recursos humanos para mantener registros de empleados y evaluar su desempeño.

En la producción, los sistemas de información se utilizan para controlar inventarios, procesar pedidos de clientes y optimizar la asignación de recursos como es posible apreciar en la imagen 6. Además, en un entorno competitivo, mantener costos bajos es esencial, y los sistemas de información desempeñan un papel vital en la planificación de recursos y la reducción de contratiempos en la producción.

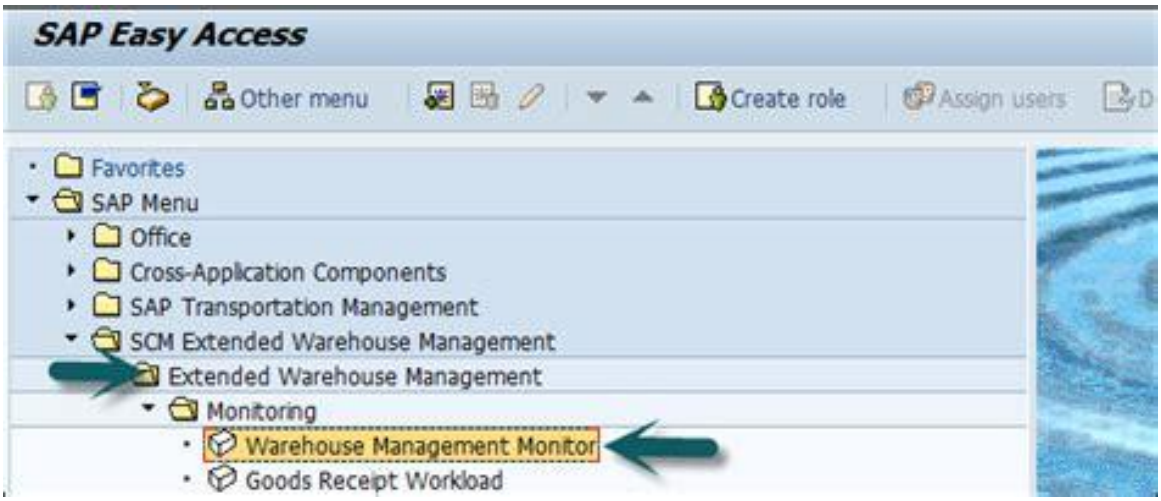


Imagen 6. Control de inventarios en SAP elaborado por el autor.

Las bases de datos son sistemas computarizados que almacenan y hacen disponible la información cuando se solicita. Se definen como una serie de datos organizados y relacionados entre sí, esenciales para los sistemas de apoyo a la toma de decisiones y la ventaja competitiva. Sus componentes principales incluyen los datos en sí, el hardware de almacenamiento, el software del sistema manejador de base de datos (DBMS) y los usuarios pueden ser programadores, usuarios finales o administradores de bases de datos.

El uso de bases de datos ofrece ventajas significativas, como la globalización de la información, eliminación de redundancia e inconsistencia de datos, compartición de información, mayor velocidad en la manipulación de datos, reducción de la labor de mantenimiento de archivos físicos, disponibilidad actualizada de información, globalización de la información que la hace un recurso corporativo compartido, eliminación de datos redundantes e inconsistentes, posibilidad de compartir información entre sistemas y usuarios, mantenimiento de la integridad de los datos y la independencia de datos que permite cambios en la información sin afectar las aplicaciones existentes, como se muestra en la imagen 7.

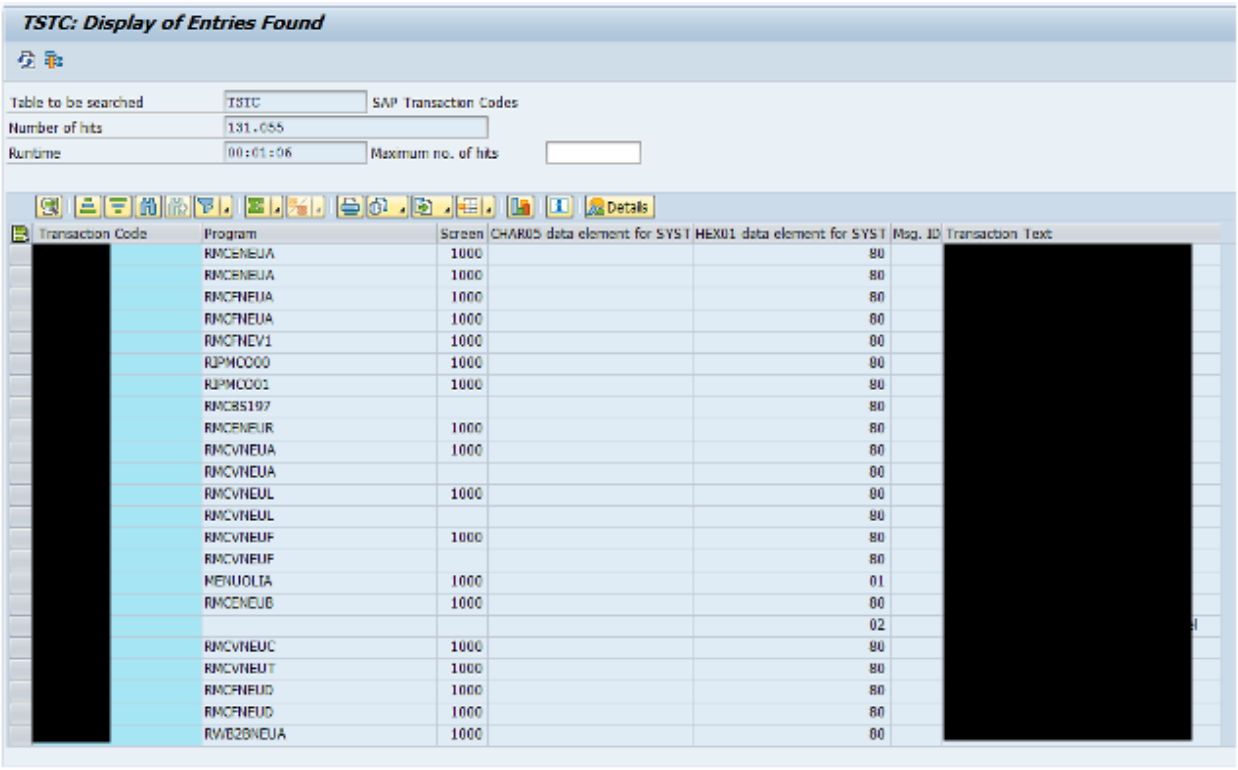


Imagen 7. Control de transacciones en SAP elaborado por el autor.

Ejemplo de un proyecto de automatización con una base de datos y descripción de sus ventajas y limitaciones

Para este proyecto se utilizó la plataforma Knime, la cual es una plataforma de ciencia de datos y preparación de datos de bajo código que hace que comprender los datos y diseñar flujos de trabajo analíticos sea accesible para todos, tal como se muestra en la imagen 8. Se trabajó con un archivo de datos llamado "adult.csv" el cual fue exportado de una base de datos. Este archivo contiene información hipotética sobre diferentes personas, incluyendo datos demográficos y sus ingresos. El objetivo principal es analizar y visualizar la relación entre los ingresos y los puestos de trabajo de los empleados, como se puede apreciar en la imagen 8.

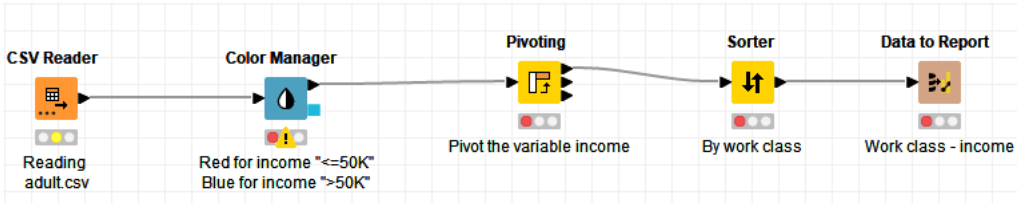


Imagen 8. Diagrama de flujo en KNIME elaborado por el autor.

Paso 1: Conocer e identificar los Datos

Para comenzar, se cargó el archivo "adult.csv" en Knime. Cada línea de este archivo representa a un empleado y contiene información demográfica su grupo de ingreso económico, sin embargo, nos enfocaremos en este último atributo que indica si el empleado gana menos de 50,000 dólares al año (línea roja) o más de 50,000 dólares al año (línea azul).

Paso 2: Análisis y Visualización de Datos

Después de cargar el archivo, se realizó un filtrado de los datos, separando los empleados en dos grupos: aquellos con ingresos menores a 50,000 dólares (línea roja) y aquellos con ingresos mayores a 50,000 dólares (línea azul). Este paso ayudo a crear dos conjuntos de datos distintos.

A continuación, se procedió a generar una gráfica que relaciono el ingreso con la clase trabajadora. Para ello, se agruparon las personas por su ocupación o puesto y se calculó la distribución de ingresos en cada grupo, obteniendo finalmente una distribución de los ingresos en diferentes categorías laborales.

Paso 3: Generación de Reporte

Finalmente, se generó un reporte en Knime que resuma los resultados obtenidos. El reporte incluyo información sobre la distribución de ingresos por puesto de trabajo, resaltando las diferencias en los ingresos entre las distintas categorías laborales. Esto nos permitió tener una visión clara de cómo la categoría laboral influye en los ingresos de las personas.

Ventajas de KNIME:

1. Interfaz amigable: KNIME ofrece una interfaz de usuario fácil de usar.
2. Manipulación intuitiva de datos: Visualmente facilita el manejo de los datos al asignarle diferentes iconos.
3. Documentación de flujos: Permite documentar paso a paso cada etapa del flujo de trabajo.
4. Manejo de grandes volúmenes de datos: Optimiza el procesamiento de grandes conjuntos de datos.
5. Acceso a repositorio público: Proporciona acceso a ejemplos y conjuntos de datos de manera que los usuarios puedan consultar procesos similares que sirvan de guía para solución de su nueva necesidad.
6. Herramientas de manipulación y análisis de datos: Ofrece potentes herramientas para manipular y analizar datos.
7. Open source: Es de código abierto y permite la creación de nuevos nodos personalizados e integración con otras herramientas como R o Python.

Limitaciones de KNIME:

1. Curva de aprendizaje: A pesar de su interfaz amigable, puede requerir tiempo para aprender a utilizar todas sus funciones y nodos.
2. Recursos de hardware: El rendimiento de KNIME puede verse afectado por la capacidad de hardware de la máquina en la que se ejecuta, especialmente con conjuntos de datos grandes.
3. No es adecuado para programación avanzada: KNIME está diseñado principalmente para usuarios sin experiencia en programación, lo que puede limitar su utilidad para tareas altamente especializadas que requieren programación personalizada.
4. Integración de lenguajes de programación: Aunque se integra con R y Python, la integración puede no ser tan fluida como en herramientas especializadas en esos lenguajes.
5. Escalabilidad limitada: Si bien puede manejar grandes volúmenes de datos, puede encontrar limitaciones en términos de escalabilidad para aplicaciones empresariales extremadamente grandes y complejas.

Factores por considerar de los proyectos automatizados

```python
dataCADO=pd.read_excel(LocCADO, sheet_name="Sheet1")
dataKOB1=pd.read_excel(LocKOB1, sheet_name="Sheet1")

#Usar columnas de Sheet1: comparar valores de columna E, O
#Filtrar por columna Cost Element cuyos valores unicamente S6186701
#Restar a valores de KOB los de CADO y agregar en una columna la diferencia
#dataCADO=pd.read_excel('..\26072023_CADO P10 2023.xlsx', sheet_name="Sheet1")
#data.drop(columns=data.columns[0], axis=1, inplace=True)
#data=data.drop(data.index[5415:])

RemoverColumnas=['WBS element','Short Text','Receiver order','Description','Processing status','Operation Short Text','Exception']
#RemoverColumnas=['WBS element','Short Text','Receiver order','Short Text','Reason for Variance','Exception']

dataCADO=dataCADO.drop(RemoverColumnas,axis=1)

print(dataCADO)
dataCADO=dataCADO[dataCADO['Name'].str.contains("Approved", na=False)]

HorasCADO=dataCADO.groupby(["Personnel Number"],as_index=False).agg({'Name of employee or applicant': 'first','Hours': 'sum'})
#HorasCADO=HorasCADO.round({'Hours':0})
print(HorasCADO)

dataKOB1=dataKOB1[dataKOB1['Cost Element'].str.contains("S6186701")]
dataKOB1=dataKOB1.groupby(["Personnel Number"],as_index=False).agg({'Total quantity': 'sum'})
dataKOB1.rename(columns = {'Total quantity':'Total quantity KOB1'}, inplace = True)
#dataKOB1=dataKOB1.round({'Total quantity':0})
print(dataKOB1)

dataCADOvsKOB1=pd.DataFrame.merge(HorasCADO,dataKOB1,on='Personnel Number')
dataCADOvsKOB1['Dif']=dataCADOvsKOB1['Total quantity KOB1']-dataCADOvsKOB1['Hours']
print(dataCADOvsKOB1)

FechaHOY = str(datetime.datetime.now().strftime("%Y-%m-%d-%H%M"))
```

Imagen 9. Automatización de análisis financiero en Python elaborado por el autor.

La automatización de proyectos ha emergido como una práctica esencial en el entorno laboral, principalmente empleando códigos similares al que se aprecia en la imagen 9, que puede afectar la eficiencia y efectividad de las organizaciones. Aunque esta tecnología puede ofrecer muchos beneficios, también presenta desafíos. Las ventajas y desventajas por considerar en una automatización de proyectos laborales se describen a continuación:

Los beneficios de la automatización en un proyecto laboral incluyen:

1. Eficacia y productividad: La automatización permite a las organizaciones realizar tareas repetitivas de manera más rápida y precisa, lo que aumenta la productividad y reduce el tiempo dedicado a tareas manuales.
2. Reducción de errores humanos: La automatización mejora significativamente la calidad y precisión de las tareas porque reduce los errores humanos.
3. Ahorro de costos: A largo plazo, la automatización de tareas rutinarias puede reducir los costos laborales porque se necesitará menos personal para hacerlas.
4. Escalabilidad: La automatización permite a las organizaciones manejar un mayor volumen de trabajo sin necesidad de contratar un número significativamente mayor de trabajadores.
5. Mejora de la calidad: La automatización garantiza una ejecución consistente de las tareas, lo que resulta en una entrega de productos o servicios de mayor calidad.

6. Mayor disponibilidad: Las tareas automatizadas pueden ejecutarse las 24 horas del día, los 7 días de la semana, lo que aumenta la disponibilidad y la capacidad de respuesta de la organización.
7. Análisis de datos: La automatización facilita la recopilación y el análisis de datos en tiempo real, lo que puede conducir a una toma de decisiones más estratégica.

Los inconvenientes de la automatización en proyectos de trabajo:

1. Costos iniciales: La implementación de sistemas de automatización, incluido el software, el hardware y la capacitación, puede resultar costosa.
2. Pérdida de empleo: La automatización puede eliminar algunos puestos de trabajo, lo que genera preocupaciones entre los empleados acerca de su seguridad laboral.
3. Dependencia tecnológica: La automatización pone a las organizaciones más dependientes de la tecnología, lo que las pone en peligro en caso de fallas técnicas o ciberataques.
4. Falta de flexibilidad: Algunas tareas automatizadas pueden no tener la flexibilidad necesaria para adaptarse a situaciones imprevistas, lo que puede requerir la intervención humana.
5. Necesidad de actualizaciones continuas: Para mantener su eficacia, los sistemas automatizados necesitan actualizaciones regulares, lo que puede ser costoso y llevar tiempo.
6. Riesgo de obsolescencia: Con el tiempo, la tecnología utilizada en la automatización puede volverse obsoleta, lo que requiere inversiones adicionales para mantenerse al día.
7. Pérdida de habilidades humanas: La automatización puede causar la pérdida de habilidades humanas porque las personas pueden volverse menos competentes en tareas que antes realizaban manualmente.

En resumen, la automatización en el lugar de trabajo puede tener muchos beneficios, como aumentar la eficiencia, la productividad y la reducción de errores, pero también tiene sus desventajas, como los costos iniciales, la posibilidad de perder el trabajo y la dependencia de la tecnología. Los objetivos, necesidades y consideraciones éticas y sociales de la organización deben ser considerados antes de decidir automatizar un proyecto.

CAPITULO 4. ANALISIS FINANCIERO EN EL DEPARTAMENTO DE IT: CONCEPTOS BÁSICOS Y SUS APLICACIONES A PROYECTOS

Conociendo la función de las finanzas en un departamento de IT

El departamento de Tecnologías de la Información (IT) ha evolucionado para convertirse en un componente esencial de las operaciones de una organización en el entorno empresarial actual. Aunque no es su objetivo principal generar utilidades directas, juega un papel importante en la eficiencia operativa y en la capacidad de una empresa para mantenerse competitiva. A pesar de esto, el departamento de finanzas sigue siendo crucial en el departamento de IT porque juega un papel importante en la gestión de los recursos financieros, la toma de decisiones estratégicas y asegurarse de que los fondos se usen de manera transparente. La importancia de este departamento se explica a continuación.

Administración de recursos:

El departamento de finanzas es responsable de asignar y administrar los recursos financieros del departamento de tecnología de la información. Aunque la tecnología de la información no busca directamente generar utilidades, es esencial administrar estos recursos de manera efectiva. Los presupuestos se asignan, los costos se controlan y se garantiza que los recursos estén disponibles cuando se necesiten para mantener el funcionamiento adecuado de los sistemas y proyectos de IT.

Invertir de manera estratégica:

En la era digital, la estrategia de una empresa debe invertir en tecnología de la información. El departamento de finanzas y el departamento de tecnología trabajan juntos para tomar decisiones inteligentes sobre dónde y cómo invertir en tecnología para lograr los objetivos comerciales. Esto implica evaluar las inversiones en hardware, software, capacitación y desarrollo de sistemas. Los departamentos trabajan juntos para alinear las inversiones en IT con los objetivos comerciales.

Administración de Costos y Eficiencia:

En el ámbito de la tecnología de la información, el control de costos es fundamental para mantener un equilibrio entre la eficiencia operativa y el uso prudente de los recursos financieros. El departamento de finanzas es esencial para supervisar y controlar los costos de proyectos, infraestructura, personal y adquisiciones tecnológicas. Esto garantiza que los recursos se utilicen de manera efectiva y que no se derrochen o gasten demasiado.

Administración de Riesgos:

La gestión de los riesgos financieros asociados con proyectos y operaciones de IT es un tema importante. El departamento de finanzas ayuda a identificar y evaluar los riesgos financieros asociados con proyectos de IT, como costos iniciales y costos en curso. Además, colabora en el desarrollo de estrategias para reducir los riesgos financieros, lo que puede ser especialmente importante en proyectos a largo plazo.

Transparencia y Informe:

Los informes financieros y la transparencia en el uso de los fondos son cruciales para cualquier organización. La responsabilidad de proporcionar informes claros y precisos sobre gastos, inversiones y resultados financieros relacionados con la tecnología recae en el departamento de finanzas de IT. Esto ayuda a los líderes de la organización a tomar decisiones bien fundamentadas y ayuda a los accionistas o partes interesadas a comprender el impacto financiero de las operaciones de IT.

En resumen, aunque el departamento de IT no tiene como objetivo principal generar utilidades directas, la gestión financiera y la colaboración con el departamento financiero son esenciales para garantizar la eficiencia operativa, la alineación con los objetivos comerciales, la reducción de riesgos y la transparencia en el uso de los recursos. La cooperación entre los departamentos de IT y finanzas ayuda en la toma de decisiones y el éxito general de la empresa.

Algunos de los conceptos utilizados en el área de finanzas

Durante la rotación del programa trainee en el área financiera del departamento de IT, se capacitó y posteriormente utilizó, una variedad de conceptos financieros que se aplicaron para realizar un análisis financiero de las actividades involucradas a IT. A continuación, se detallan algunos de los conceptos más importantes que se emplearon:

Balance de activos fijos:

Un balance de activos fijos en finanzas, particularmente en un departamento de IT, es un informe contable que lista y valora los activos tangibles a largo plazo que son propiedad de la empresa y se utilizan para la operación de la infraestructura tecnológica. Estos activos pueden incluir servidores, equipos de red, estaciones de trabajo, sistemas de almacenamiento, centros de datos y otras partes importantes de tecnología de la información. En un departamento de IT, el balance de activos fijos es crucial porque permite monitorear las inversiones en infraestructura tecnológica y comprender cómo estos activos afectan la salud financiera de la empresa.

En el contexto de los activos fijos, la depreciación es un concepto fundamental. La imagen 10 representa cómo el valor de estos activos disminuye con el tiempo debido al uso, la obsolescencia tecnológica y el desgaste. La depreciación afecta directamente la contabilidad de la empresa y se muestra en los estados financieros. La depreciación en un balance de activos fijos de un departamento de IT se muestra de la siguiente manera:

1. Valor inicial de los activos: el valor inicial de los activos de IT se muestra en el balance inicial. Este costo incluye no solo el costo de la compra, sino también los costos de instalación y configuración, así como los costos de posibles mejoras posteriores.
2. La depreciación acumulada de los activos se registra en el informe. La depreciación se calcula utilizando métodos contables particulares, como el método de línea recta, y se aplica a lo largo del período de vida útil estimado del activo. La depreciación acumulada muestra cómo el valor de los activos ha disminuido con el tiempo.
3. Valor en libros: El valor de los activos en libros se puede calcular restando la depreciación del valor inicial. Este valor en los registros es el valor actual de los activos en los registros contables de la empresa.

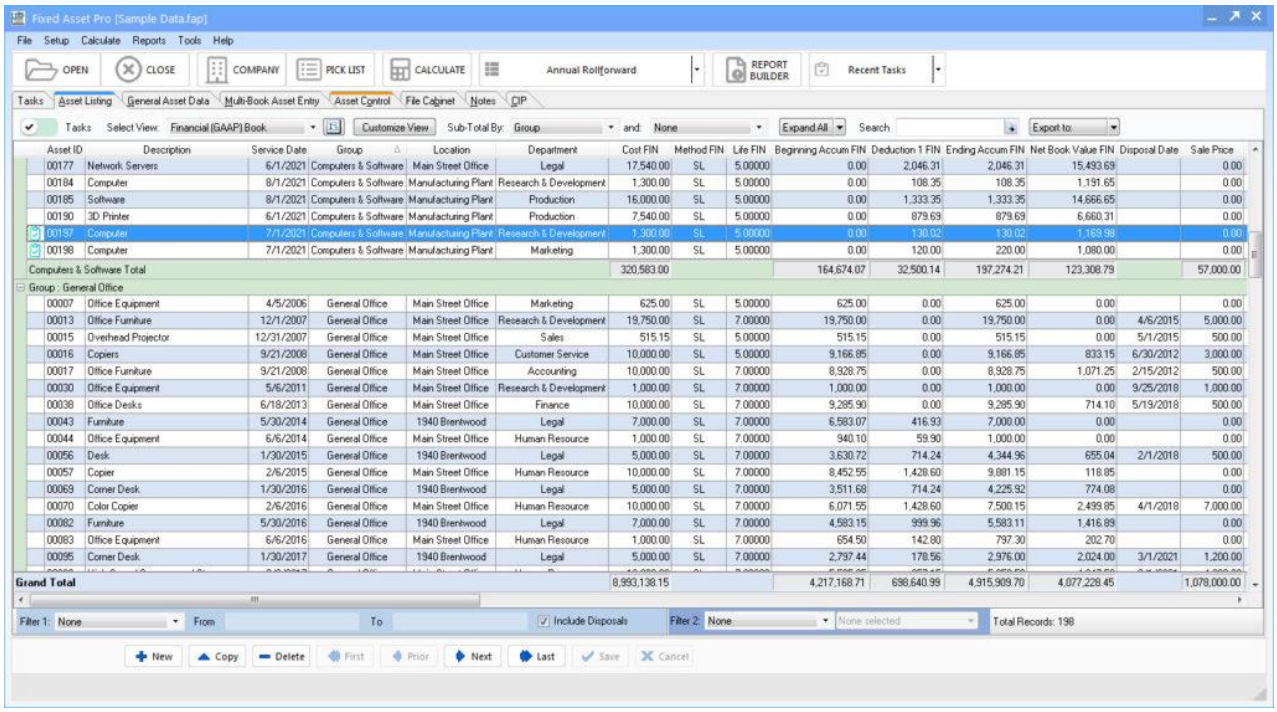


Imagen 10. Depreciación de activos fijos [4]

La depreciación tiene un impacto significativo en el departamento de IT porque afecta tanto la gestión financiera estratégica como la presentación de informes financieros. La depreciación reduce el valor de los activos en los estados financieros, lo que puede afectar la percepción de la salud financiera en la empresa. Además, tal como se muestra en la imagen 11, la depreciación afecta la planificación de inversiones en IT porque la organización debe considerar cuándo reemplazar activos obsoletos o mantenerlos en funcionamiento.

COMPAÑÍA LA ASTURIANA S.A DE C.V. ESTADO DE SITUACIÓN FINANCIERA 31 DE DICIEMBRE DE 2002			
CUENTA	PRESUPUESTADO	REAL	VARIACIONES
CIRCULANTE			
Caja y Bancos	120,000.00	210,000.00	-90,000.00
Clientes	478,400.00	446,200.00	32,200.00
Almacen de art.terminados	186,000.00	160,000.00	26,000.00
Almacen de mat. Prima	50,600.00	44,620.00	5,980.00
Suma	835,000.00	860,820.00	-25,820.00
FIJO			
Terrenos	207,000.00	0.00	207,000.00
Edificios	368,000.00	501,400.00	-133,400.00
Deprec. Acumulada	-138,000.00	-144,900.00	6,900.00
Maquinaria y equipo	487,600.00	487,600.00	0.00
Deprec. Acumulada	-193,200.00	-193,200.00	0.00
Suma	731,400.00	650,900.00	80,500.00
DIFERIDO			
Gastos de organización	92,000.00	117,300.00	-25,300.00
Suma total del activo	1,658,400.00	1,629,020.00	29,380.00
PASIVO			
CIRCULANTE			
Proveedores	21,000.00	50,000.00	-29,000.00
Iva por pagar	71,760.00	66,930.00	4,830.00
ISR por pagar	169,850.40	170,883.10	-1,032.70
PTU por pagar	49,956.00	50,259.60	-303.60
Suma	312,566.40	338,072.70	-25,506.30
CAPITAL			
Capital social	1,183,000.00	1,183,000.00	0.00
Utilidad del ejercicio	162,833.00	107,947.30	54,885.70
Suma	1,345,833.00	1,290,947.30	54,885.70
Suma Pasivo + Capital	1,658,399.40	1,629,020.00	29,379.40

Imagen 11. Estado financiero ficticio propuesto por el autor.

En resumen, para monitorear las inversiones en infraestructura tecnológica, un balance de activos fijos es esencial en el departamento de IT. Debido a que afecta la presentación de informes financieros y la toma de decisiones estratégicas relacionadas con la inversión y el mantenimiento de activos tecnológicos, la depreciación de estos activos es un componente crucial en la contabilidad y la gestión financiera.

Reporte de gastos relacionados a proyectos:

En el departamento de IT, un reporte de gastos relacionados con proyectos es un documento contable que detalla los costos y gastos relacionados con iniciativas específicas de IT. Estos informes son fundamentales para el seguimiento y generalmente es necesario aplicar alguna metodología para poder tener un plan de trabajo tal como se muestra en la imagen 12. La gestión y la presentación de costos relacionados con

proyectos de IT, proporcionan información detallada sobre cómo se están utilizando los recursos financieros en el ámbito tecnológico. Estos informes ayudan a la organización a tomar decisiones informadas, garantizar la transparencia financiera y controlar los presupuestos destinados a los proyectos de IT.

Un informe de gastos relacionado con proyectos de IT incluye los siguientes datos:

1. Descripción del proyecto: Se proporciona una descripción detallada del proyecto de IT con sus objetivos, alcance y cronograma.
2. Detalle de gastos: Se enumeran todos los gastos relacionados con el proyecto, que pueden incluir hardware, software, servicios profesionales, salarios de personal, capacitación y otros gastos relacionados.
3. Planeación: Los cronogramas de gastos indican cuándo se realizaron los gastos a lo largo del ciclo de vida del proyecto. Esto facilita la evaluación de la distribución de costos a lo largo del tiempo.
4. Actuales: La comparación con el presupuesto es cuando se compara el gasto real del proyecto con el presupuesto inicial que se le asignó. Esto ayuda a identificar desviaciones del presupuesto y a evaluar si el proyecto cumple con las restricciones financieras.
5. La justificación de los gastos: Se proporciona una explicación detallada de los gastos, lo que permite a los responsables del proyecto y a los líderes de IT comprender por qué se han incurrido ciertos costos.
6. Resultados del proyecto: En algunos casos, el informe puede incluir información sobre los resultados del proyecto, como la finalización de tareas o la consecución de metas importantes.

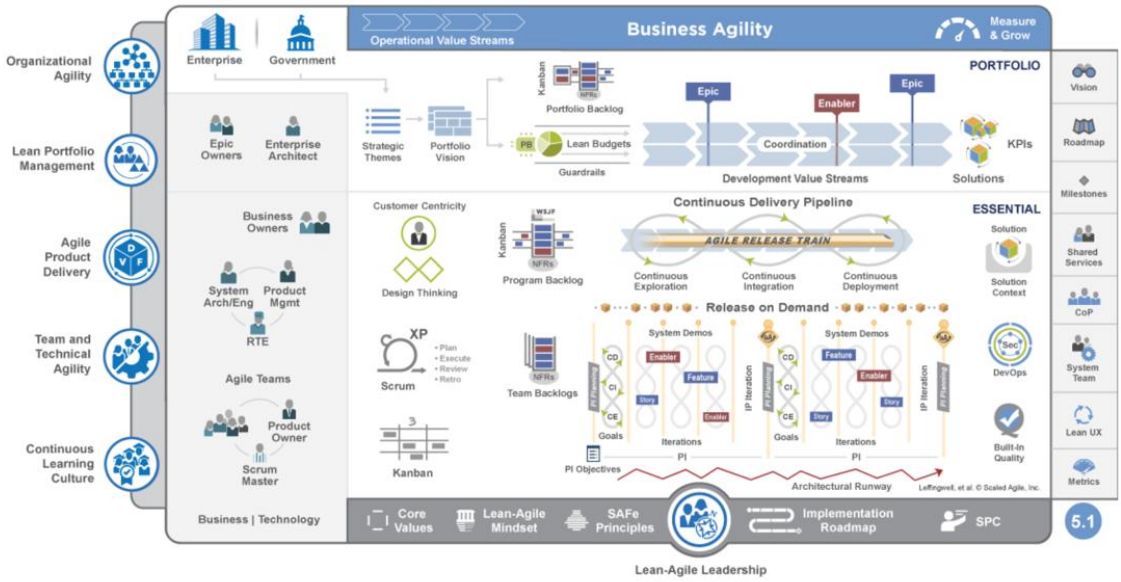


Imagen 12. Metodología AGILE [5].

Los reportes de gastos de proyecto son cruciales para el departamento de IT porque permiten un control financiero efectivo, aseguran que los proyectos se ejecuten de manera eficiente y garantizan que los recursos se utilicen de manera responsable. Estos informes ayudan a tomar decisiones porque permiten a los gerentes y líderes de IT evaluar si un proyecto está cumpliendo con el presupuesto y tomar medidas correctivas si es necesario. Además, brindan una visión clara de cómo se utilizan los recursos financieros en los proyectos de IT, lo que facilita la comunicación con partes interesadas internas y externas.

Reporte de efectos cambiarios:

En el contexto de un departamento de finanzas, un informe de efectos cambiarios es un informe que detalla los efectos financieros que resultan de las fluctuaciones en las tasas de cambio de divisas extranjeras. Estos informes son útiles para la empresa, ya que opera en mercados internacionales y realiza transacciones en monedas diferentes a la de su país de origen. Un ejemplo de este tipo de reportes es posible apreciar en la siguiente imagen:

Exchange	Name	Current	Low	High	Last trade time - UTC
USD/CAD	US Dollar/Canadian Dollar FX Spot Rate	$ 1.3583	$ 1.3527	$ 1.3666	12 Jun 20 13:06
CAD/USD	Canadian Dollar/US Dollar FX Cross Rate	$ 0.7363	$ 0.7317	$ 0.7393	12 Jun 20 13:07
USD/AUD	US Dollar/Australian Dollar FX Cross Rate	$ 1.4548	$ 1.4470	$ 1.4706	12 Jun 20 13:06
AUD/GBP	Australian Dollar/UK Pound Sterling FX Cross Rate	£ 0.55	£ 0.54	£ 0.55	12 Jun 20 13:07
USD/EUR	US Dollar/Euro FX Cross Rate	€ 0.88	€ 0.88	€ 0.89	12 Jun 20 13:05
AUD/EUR	Australian Dollar/Euro FX Cross Rate	€ 0.61	€ 0.60	€ 0.61	12 Jun 20 13:06
NZD/AUD	New Zealand Dollar/Australian Dollar FX Cross Rate	$ 0.9372	$ 0.9359	$ 0.9406	12 Jun 20 13:04
AED/ZAR	UAE Dirham/South African Rand FX Cross Rate	R 4.63	R 4.62	R 4.71	12 Jun 20 13:05
UZS/RUB	Uzbekistan Sum/Russian Rouble FX Cross Rate	0.00681 ₽	0.00685 ₽	0.00694 ₽	12 Jun 20 13:06
INR/CNY	Indian Rupee/Chinese Renminbi FX Cross Rate	¥ 0.0932	¥ 0.0927	¥ 0.0934	12 Jun 20 13:06
ARS/CLP	Argentine Peso/Chilean Peso FX Cross Rate	$ 11.31	$ 11.30	$ 11.43	12 Jun 20 13:04
CHF/JPY	Swiss Franc/Japanese Yen FX Cross Rate	¥ 113.42	¥ 112.88	¥ 113.66	12 Jun 20 13:08
EUR/CHF	Euro/Swiss Franc FX Cross Rate	1.0691 CHF	1.0657 CHF	1.0726 CHF	12 Jun 20 13:08

Imagen 13. Reporte de efectos cambiarios propuesto por el autor.

El reporte de efectos cambiarios generalmente incluye los siguientes datos:

1. Las transacciones que involucran otras monedas en asuntos comerciales o financieros se denominan transacciones en moneda extranjera. Esto puede incluir cualquier actividad que implique la conversión de moneda, como ventas, compras, préstamos, inversiones, etc.
2. Las tasas de cambio utilizadas en cada transacción o período de tiempo específico se muestran en el informe. La tasa de cambio inicial, la tasa de cambio al cierre del período y cualquier tasa intermedia relevante pueden incluirse en el mismo.
3. El valor de una transacción en su moneda local original y el valor de la transacción en su moneda extranjera resultante se conocen como diferencias de cambio. Estas variaciones pueden ser ganancias (si el dólar se fortalece) o pérdidas (si el dólar se debilita).
4. El informe detalla cómo estos cambios afectan los estados financieros de la empresa. Pueden afectar los ingresos, los gastos, el patrimonio neto y otras variables financieras, por ejemplo.
5. Notas explicativas: El informe con frecuencia incluye notas explicativas que detallan las políticas contables utilizadas para registrar y contabilizar las fluctuaciones de divisas, así como cualquier información relevante sobre los riesgos relacionados con las fluctuaciones de las tasas de cambio.

Los reportes de efectos cambiarios son esenciales para evaluar el impacto financiero de la exposición a riesgos cambiarios y para la toma de decisiones sobre las estrategias de cobertura o gestión de riesgos. Además, están obligados por normas contables y reglamentos para garantizar la transparencia y precisión en la presentación de los estados financieros de la empresa. Además, es fundamental comprender cómo las fluctuaciones de divisas pueden afectar la rentabilidad y la posición financiera de una empresa en un mundo globalizado.

Por qué es importante planificar antes de desarrollar? Posibles consecuencias de una mala gestión en IT

Por varias razones clave, la planificación antes del desarrollo es crucial en un departamento de IT. Estas razones y sus posibles consecuencias se detallan a continuación:

Optimización de los recursos económicos:

La planificación financiera previa permite al departamento de IT estimar de manera precisa los recursos financieros necesarios para llevar a cabo un proyecto. El presupuesto se asigna de manera eficiente con esta anticipación, lo que evita gastos innecesarios o derroches. La consecuencia positiva es que se utilizan los recursos financieros de manera más eficiente.

Administración de Costos:

A lo largo del ciclo de vida de un proyecto de IT, la planificación permite establecer presupuestos realistas y monitorear de cerca los costos. Esto evita sorpresas financieras desagradables y desviaciones presupuestarias significativas que podrían dañar la salud financiera de la empresa. La consecuencia desfavorable de no planificar adecuadamente podría ser el agotamiento de los recursos financieros o incluso la suspensión del proyecto debido a costos imprevistos.

Evaluación del ROI de la inversión:

Las organizaciones pueden estimar el retorno de la inversión anticipada en un proyecto de IT utilizando la planificación financiera. Como se ejemplifica en la imagen 14, esto significa que pueden evaluar si el proyecto es financieramente viable y cuándo se obtendrán los beneficios que superarán los costos. La falta de planificación puede llevar a la inversión en proyectos que no produzcan el ROI esperado, lo que puede afectar negativamente la rentabilidad.

Imagen 14. Evaluación del ROI propuesto por el autor.

Priorizar los proyectos:

La mayoría de las organizaciones tienen varios proyectos de IT en su cartera. La planificación financiera les brinda una base para evaluar y priorizar estos proyectos en función de su impacto financiero previsto y de cómo se alinean con los objetivos estratégicos. La falta de prioridad puede llevar a la inversión de la organización en proyectos que no generan el valor esperado.

Gestión de riesgos económicos:

La planificación anticipada también ayuda a identificar y administrar los riesgos financieros de un proyecto de IT. Identificar los riesgos financieros con anticipación permite crear planes de mitigación y estar preparado para cualquier problema que surja. De no hacerlo, el progreso del proyecto podría verse obstaculizado por problemas financieros imprevistos.

En resumen, la planificación financiera previa al desarrollo de proyectos de IT es crucial para la gestión eficiente de recursos, el control de costos, la toma de decisiones informadas y la reducción de riesgos financieros. La falta de planificación puede conducir a problemas financieros, gastos innecesarios y proyectos que no cumplen con las expectativas de retorno de la inversión, lo que puede afectar negativamente la salud financiera de la organización.

CAPITULO 5. LA CIBERSEGURIDAD EN LA EMPRESA

Introducción a los conceptos de ciberseguridad y su importancia en la protección de la información empresarial

En esencia, la ciberseguridad es la protección que protege una amplia gama de dispositivos tecnológicos, desde computadoras y servidores hasta dispositivos móviles, sistemas electrónicos, redes y datos, de los ataques cibernéticos. La tecnología es omnipresente y se puede encontrar en casi todas las áreas de una empresa. Esta disciplina puede dividirse en varias categorías principales, cada una con una función específica en el amplio campo de la ciberseguridad.

En primer lugar, abordamos la seguridad de red, un componente crucial que se enfoca en proteger la red informática corporativa de las amenazas que acechan, ya sean intrusos con motivaciones específicas o el malware oportunista que se infiltra en una red cibernética extensa. Se trata de un “continuo juego de gato y ratón” en el que nuestro departamento de ciberseguridad debe mantenerse un paso por delante de los atacantes para proteger datos sensibles de la empresa y garantizar la continuidad de las operaciones.

La seguridad de las aplicaciones es otra parte importante de la seguridad cibernética. La preservación de la integridad de los programas y dispositivos es su objetivo principal, para evitar la infiltración de amenazas potenciales. Es importante destacar que la seguridad efectiva debe estar presente desde el mismo proceso de diseño, anticipando y previniendo vulnerabilidades, no solo durante la etapa de implementación. Un ejemplo de seguridad efectiva en el proceso de diseño es como el de la siguiente imagen:

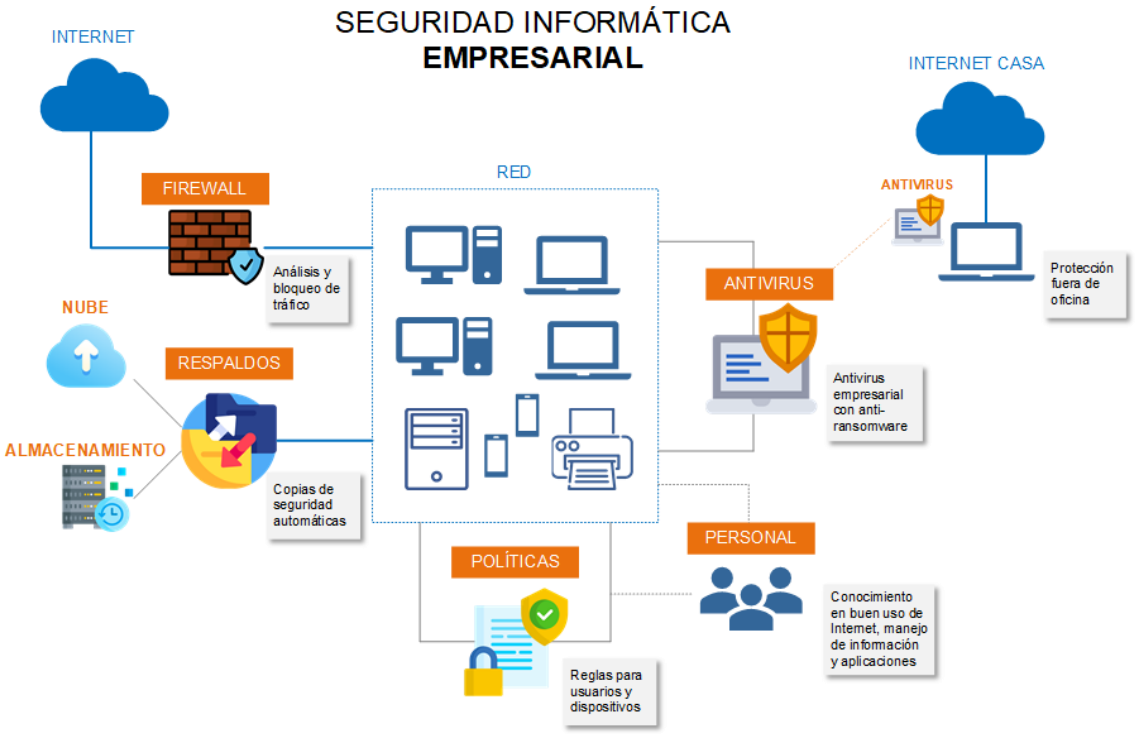


Imagen 15. Seguridad de la red corporativa [6].

La protección de la información es fundamental para la ciberseguridad. Es necesario asegurarse de que los datos sean privados e íntegros tanto durante el almacenamiento como durante el tránsito a través de las redes, por ello, es necesario que siempre vengan encriptados de tal manera que la información únicamente pueda ser visualizada por el usuario al que va dirigido, disminuyendo así el riesgo de una posible filtración. La privacidad y la confidencialidad de la información son cruciales, especialmente en un mundo en el que la información es un activo valioso.

La seguridad operativa es un componente que incluye procesos y decisiones, como administrar y proteger los recursos de datos. Esto incluye la gestión de permisos de usuario para acceder a la red y las reglas sobre cómo y dónde se comparten o almacenan los datos. Es la base para un funcionamiento seguro y fluido de los sistemas y redes.

Cuando la organización enfrenta incidentes de ciberseguridad o situaciones que paralizan sus operaciones o causan la pérdida de datos, debe seguir la hoja de ruta de recuperación ante desastres y continuidad comercial. La continuidad comercial se refiere a la estrategia para mantener la operación incluso cuando algunos recursos críticos se ven

comprometidos, mientras que las políticas de recuperación ante desastres establecen cómo se restauran las operaciones y la información para volver a la normalidad.

Finalmente, pero no menos crucial, la capacitación del usuario final. Se dice con frecuencia que los humanos son el eslabón más débil de la cadena de la ciberseguridad. Los usuarios imprudentes pueden introducir virus y amenazas en sistemas que en teoría deberían ser seguros. Por lo tanto, la capacitación de los usuarios para identificar y evitar peligros, como no abrir archivos adjuntos de correos sospechosos o conectar unidades USB desconocidas, es esencial para mantener a salvo cualquier organización.

En resumen, la ciberseguridad es un campo multifacético que abarca la protección de sistemas y datos desde una variedad de perspectivas, desde las redes y aplicaciones hasta la seguridad operativa y la información. Es un esfuerzo continuo que implica tanto la implementación de tecnología avanzada como la capacitación y concientización de las personas, y su importancia radica en la defensa de la infraestructura tecnológica que sustenta nuestra vida moderna.

Explicación de los tipos de ataques cibernéticos más comunes y las medidas para evitarlos

Los ciberataques son una realidad en el mundo digital actual, lo que amenaza la seguridad de las empresas y organizaciones. Se dice que existen dos tipos de organizaciones: las que han sido atacadas y las que aún no lo saben. En un mundo cada vez más interconectado, la ciberseguridad es esencial para proteger la integridad de la información y los sistemas. En este contexto, es fundamental comprender no solo la frecuencia de estos ataques, sino también sus motivaciones, técnicas y métodos para prevenirlos.

La frecuencia de ciberataques

Los ciberataques ocurren todos los días y están en constante cambio. Esta amenaza constante se manifiesta en una variedad de formas y niveles de sofisticación. La proliferación de dispositivos conectados a internet ha aumentado la superficie de ataque, lo que aumenta la exposición a las amenazas cibernéticas. La ciberseguridad es una prioridad ineludible para la empresa en todo el mundo debido a la frecuencia y diversidad de los ciberataques.

Razones detrás de los ciberataques

Las razones detrás de los ciberataques pueden variar. El lucro es uno de los más comunes. Los ciberdelincuentes buscan ganar dinero a través de actividades como el secuestro de datos, también conocido como ransomware, o el robo de información financiera y personal. Estos ataques pueden causar muchas pérdidas.

Hay motivaciones más amplias además del lucro. El "hacktivismo", una forma de activismo cibernético donde los objetivos van más allá del beneficio económico motiva a algunos atacantes. Estos actores buscan cambiar las cosas en la sociedad o en la política, o simplemente causar caos en línea para avanzar en sus agendas. El hacktivismo puede incluir difundir datos confidenciales o arruinar sitios web.

[1]Los tipos de ciberataques más comunes

1. El término "malware" se refiere a software malicioso como virus, gusanos, spyware y ransomware. El malware se propaga con frecuencia a través de engaños, como la descarga de archivos adjuntos o la visita a sitios web comprometidos. El malware suele explotar vulnerabilidades en sistemas. El malware puede bloquear el acceso, robar datos, instalar más software dañino o incluso hacer que el sistema sea inoperable una vez dentro de un sistema.

2. La suplantación de identidad, también conocida como phishing, consiste en enviar comunicaciones falsas que parecen provenir de fuentes confiables con el fin de engañar a las víctimas para que revelen información confidencial o descarguen malware. El phishing es una amenaza cada vez más común y una táctica de ataque en constante evolución.

3. Ataque de intermediario (MitM): Cuando un atacante se infiltra en las comunicaciones entre dos partes, tiene la capacidad de interceptar, filtrar o robar datos confidenciales. Estos ataques pueden ocurrir en redes públicas no seguras o porque el malware se instala en dispositivos comprometidos.

4. Ataque de denegación de servicio (DDoS): Los ataques DDoS abruman sistemas, servidores o redes con tráfico falso o redundante, agotando los recursos y el ancho de banda y causando interrupciones en los servicios. Los atacantes pueden llevar a cabo un ataque DDoS con múltiples dispositivos comprometidos.

5. Inyección de SQL: Este tipo de ataque utiliza código malicioso en servidores que utilizan lenguaje de consulta estructurado (SQL) para obligar a revelar información confidencial. Los atacantes pueden lograr esto al usar formularios de búsqueda en sitios web vulnerables.

6. Ataques de día cero: ocurren antes de la creación y distribución de un parche o solución, pero después de que se ha descubierto una vulnerabilidad en la red. Los atacantes buscan esta vulnerabilidad recién descubierta, por lo que es necesaria vigilancia constante para detectarla y reducirla.

[1] https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

7. La tunelización de DNS utiliza el protocolo DNS para enviar tráfico que no pertenece a las solicitudes DNS por el puerto 53. Este método se puede utilizar para ocultar datos y extraer datos de sistemas comprometidos.

¿Cómo se pueden prevenir los ciberataques más comunes?

La prevención es fundamental para proteger la integridad de la información y los sistemas en un mundo donde los ciberataques son una amenaza constante y en constante evolución. Aquí están algunas sugerencias importantes para evitar ciberataques. Dado que todos son responsables de la ciberseguridad en la era digital actual, estas tácticas se pueden implementar tanto a nivel organizativo como individual.

Algunas de las recomendaciones para prevenir los ataques cibernéticos son:

Educación y Sensibilización

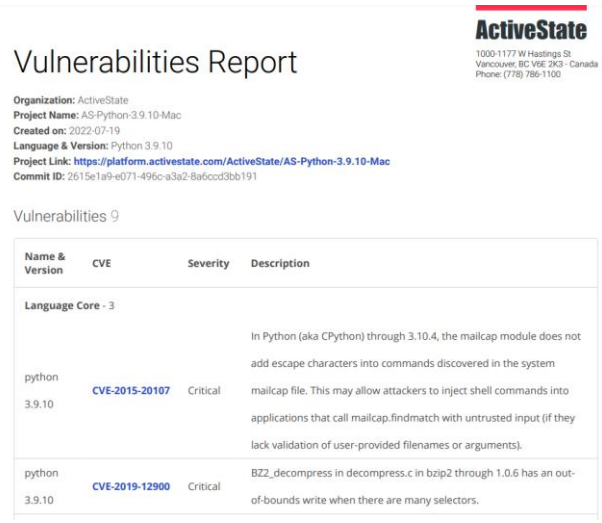
La educación y la concienciación son fundamentales para prevenir ciberataques. Es fundamental que las personas estén bien informadas sobre las mejores prácticas de seguridad y las amenazas cibernéticas, tanto a nivel organizacional como individual. Esto incluye:

1. Mostrar a los empleados y usuarios cómo identificar correos electrónicos de phishing, enlaces sospechosos y adjuntos peligrosos.
2. Fomentar una cultura de ciberseguridad en la que todos sepan cómo proteger sus activos digitales.
3. Mantenerse al día con las amenazas y estrategias más recientes utilizadas por los ciberdelincuentes.

Cambios y parches

Es fundamental mantener el software, los sistemas operativos y las aplicaciones actualizados. Los ciberdelincuentes frecuentemente utilizan fallas conocidas en software que no está actualizado para realizar ataques. Para protegerse de los ciberataques:

1. Configurar actualizaciones automáticas en sistemas y aplicaciones para asegurarse de que se apliquen parches críticos tan pronto como estén disponibles.
2. Realizar evaluaciones de vulnerabilidad regulares para detectar y corregir posibles brechas de seguridad en la infraestructura.



ActiveState

1000-1177 W Hastings St
Vancouver, BC V6E 2K3 - Canada
Phone: (778) 786-1100

Vulnerabilities Report

Organization: ActiveState
Project Name: AS-Python-3.9.10-Mac
Created on: 2022-07-19
Language & Version: Python 3.9.10
Project Link: https://platform.activestate.com/ActiveState/AS-Python-3.9.10-Mac
Commit ID: 2615e1a9-e071-496c-a3a2-8a6ccd3bb191

Vulnerabilities 9

Name & Version	CVE	Severity	Description
Language Core - 3			
python 3.9.10	CVE-2015-20107	Critical	In Python (aka CPython) through 3.10.4, the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input (if they lack validation of user-provided filenames or arguments).
python 3.9.10	CVE-2019-12900	Critical	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.

Imagen 17. Notificación de vulnerabilidad a usuario corporativo [7].

Contraseñas Confiables

Una defensa fundamental contra el acceso no autorizado es una contraseña fuerte. Aquí hay algunas sugerencias:

1. Usar contraseñas largas y complejas con letras mayúsculas, minúsculas, números y caracteres especiales.
2. Evitar usar contraseñas típicas o predecibles, como "123456" o "contraseña".
3. Para almacenar y administrar contraseñas de manera segura, emplear gestores de contraseñas.

La autenticación de dos factores conocido como 2FA

La autenticación de dos factores es una capa de seguridad adicional que requiere la verificación de la identidad utilizando dos métodos diferentes. Esto dificulta que los atacantes accedan a cuentas, incluso si saben la contraseña. Siempre que sea posible, habilitar 2FA.

Los firewalls y la seguridad de la red

Para proteger la infraestructura y filtrar el tráfico no deseado, se deben usar firewalls y soluciones de seguridad de red. Además, establecer políticas robustas de seguridad de red que impidan el acceso no autorizado.

Resistencia de datos

Realizar copias de seguridad regulares de los datos importantes y almacenarlos tanto en línea como fuera de línea. Contar con copias de seguridad puede ser esencial para la recuperación de datos en caso de un ataque de ransomware u otro incidente.

Controles de acceso

Implementar políticas de control de acceso que limiten los privilegios de los usuarios de acuerdo con las necesidades. Los usuarios deben tener acceso únicamente a los recursos necesarios para completar sus tareas laborales.

Observación y Detección de Riesgos:

Para identificar comportamientos inusuales o actividades sospechosas en la red, se deben utilizar soluciones de monitoreo de seguridad y detección de amenazas. Esto hace posible una respuesta temprana ante amenazas potenciales.

Diseño de un plan de respuesta ante incidentes:

Construir y mantener un plan de respuesta ante incidentes que describa cómo responder a los ataques cibernéticos en caso de que ocurran. Un plan sólido puede reducir el impacto y el tiempo que dura un incidente.

Evaluación realizada por terceros:

Es fundamental evaluar las prácticas de seguridad dado que la organización trabaja con proveedores externos que tienen acceso a los sistemas o datos. Antes de

otorgarles acceso, se debe asegurar de que cumplan con estándares de ciberseguridad.

En el mundo digital actual, todos tienen la responsabilidad de evitar ciberataques. La protección contra las amenazas cibernéticas en constante evolución depende de la educación, la concienciación y la adopción de buenas prácticas. Se puede reducir significativamente el riesgo de ser víctima de un ciberataque al seguir estas recomendaciones y mantenerse vigilante tanto a nivel personal como organizacional.

Herramientas utilizadas en la detección y respuesta a incidentes de ciberseguridad

Los patrones de reacción deben adaptarse a la evolución de las amenazas en la web. Para lograrlo, se requiere un sistema EDR para proteger los puntos finales de una empresa, como computadoras o teléfonos inteligentes que se utilizan diariamente.

El sistema EDR, también conocido como Detección y Reacción de Puntos Finales, es una nueva versión de los antivirus actuales que se están volviendo obsoletos e ineficaces para garantizar la ciberseguridad de las empresas. Se pueden detectar rápidamente las amenazas gracias a su poderosa inteligencia artificial. De igual manera, con una configuración automatizada como la que se ejemplifica en la imagen 8, el sistema responderá de inmediato ante un ataque cibernético. Los archivos serán neutralizados y recuperados fácilmente con opciones automáticas, lo cual es sin duda muy ventajoso.

Imagen 16. Funciones de un EDR [8].

Un sistema EDR es más efectivo que cualquier antivirus porque es una herramienta de prevención avanzada con las siguientes características:

1. Erradica la pérdida de tiempo por parte del equipo en la revisión de falsos positivos.
2. Optimiza el trabajo de IT.
3. Observa y responde al malware y otras amenazas.
4. Utiliza un sistema de bloqueo sofisticado.
5. Ataca los riesgos durante la producción.
6. Las empresa no perderá tiempo y seguirá trabajando rápidamente gracias a su respuesta inmediata.
7. Finalmente, tiene la capacidad de restablecer y restaurar el endpoint.

¿Cómo funciona el sistema EDR para detectar riesgos?

[2]El Sistema EDR clasifica los archivos como certeros, perjudiciales o incógnitos cuando detecta actividad inusual. Luego, haga lo siguiente:

1. Emite alertas una vez que detecta una amenaza y la neutraliza al mismo tiempo.
2. Si se elige una consola de monitorización que incluya un sistema EDR, es fácil ver la información de peligro con un simple vistazo como el sistema de monitorización RMM (de las siglas en inglés, *Remote Monitoring and Management*).
3. Brinda la oportunidad de conocer datos e información importantes sobre los ataques, la cantidad de peligros activos y los que se han presentado.
4. Con identificación de nombres y fechas, puede valorar la información sobre amenazas presentadas.
5. También puede explorar la web para obtener más información sobre los riesgos a los que estuviste expuesto.

La acción de detección y estudio del Sistema EDR permite que las amenazas futuras con características similares sean bloqueadas de inmediato.

[2] https://admcloudservices.com/blog/sistema-seguridad-edr-que-es.html

Conociendo las ventajas del sistema EDR.

[3]La principal ventaja del Sistema EDR es aumentar la protección contra los ataques novedosos que se presentan en la web. Además, brinda las siguientes ventajas de esta solución de seguridad cibernética:

1. Los peligros pueden ser detectados de manera anticipada.
2. Esta herramienta facilita el trabajo pre-infección y post-infección para examinar patrones de conducta.
3. Ante una inminente exposición al peligro, el Sistema EDR actúa de inmediato.
4. A través de un estudio del origen del peligro, el ataque, la afección y la respuesta, es posible conocer la ruta del ataque y el cliente podrá entender la amenaza.

¿Cuándo es recomendable utilizar el sistema EDR?

Se recomienda su uso en organizaciones donde se cuenta con una amplia cantidad de usuarios, dado el alto costo que representa a comparación de una solución antivirus. Al ser un sistema que permite a los equipos de seguridad investigar los incidentes, contener las amenazas y mitigar el impacto en la infraestructura de IT sin que el usuario final tenga interacción directa con los mismos sin afectar su productividad en otras tareas, representa una parte fundamental de estrategia de seguridad cibernetica para las organizaciones.

El empleo de Python para la ciberseguridad

Python es una herramienta poderosa en el análisis de ciberseguridad debido a su versatilidad y la amplia disponibilidad de bibliotecas específicas, como scapy, requests y Beautiful Soup. Permite a los profesionales automatizar tareas de análisis de vulnerabilidades, realizar escaneos de redes y desarrollar herramientas de detección de intrusiones. Además, su facilidad de uso facilita el desarrollo de scripts personalizados para analizar datos y detectar patrones en el tráfico de red, lo que mejora la capacidad de respuesta ante incidentes. Esta capacidad para integrar diversas funciones en un solo lenguaje hace que Python sea esencial en la ciberseguridad, potenciando tanto la eficiencia como la eficacia en la protección de sistemas y datos.

[3] https://geekflare.com/es/edr-tools/

Caso 1: Análisis de red por medio de Python

Introducción

Un escáner de red es una herramienta esencial para el análisis y la administración de redes. Permite a los administradores identificar dispositivos activos en una red, así como obtener información sobre sus características. Este resumen, de acuerdo a lo aprendido en la materia de “Tecnologias de interconexión de redes”, se basa en la creación de un escáner de red utilizando Python, explicando su funcionamiento, el código utilizado, sus conclusiones y los posibles casos de uso.

Explicación del Código

El código empleado similar al de la imagen 18 presenta un enfoque práctico para desarrollar un escáner de red utilizando la biblioteca scapy, que permite la creación y análisis de paquetes. A continuación, se detallan las partes clave del código:

```python
import scapy.all as scapy

def scan(ip_range):
    print(f"Scanning IP range: {ip_range}")

    arp_request = scapy.ARP(pdst=ip_range)
    broadcast = scapy.Ether(dst="ff:ff:ff:ff:ff:ff")
    arp_request_broadcast = broadcast / arp_request

    print("Sending ARP requests...")
    answered_list = scapy.srp(arp_request_broadcast, timeout=5, verbose=True)[0]

    if not answered_list:
        print("No responses received.")
    else:
        print("Responses received.")

    devices = []
    for element in answered_list:
        device = {'ip': element[1].psrc, 'mac': element[1].hwsrc}
        devices.append(device)
        print(f"Device found: IP = {device['ip']}, MAC = {device['mac']}")

    return devices

def display_devices(devices):
    if devices:
        print("\nIP\t\t\tMAC Address")
        print("-----------------------------------------")
        for device in devices:
            print(f"{device['ip']}\t\t{device['mac']}")
    else:
        print("No devices found.")

def scan_network(ip_range):
    devices = scan(ip_range)
    display_devices(devices)

if __name__ == "__main__":
    ip_range = '192.168.1.0/24'
    scan_network(ip_range)
```

Imagen 18. Código fuente de análisis de red elaborado por el autor.

1. **Importación de Bibliotecas**:

   from scapy.all import ARP, Ether, srp

   Se importan las funciones necesarias de scapy, específicamente las que permiten crear paquetes ARP y Ethernet.

2. **Definición de la Función Principal**: Se define una función que configura el escáner y envía paquetes ARP a la red.

   def scan(ip_range):

      arp_request = ARP(pdst=ip_range)

      ether_frame = Ether(dst="ff:ff:ff:ff:ff:ff")

      packet = ether_frame / arp_request

      result = srp(packet, timeout=2, verbose=False)[0]

   Aquí, se construye un paquete ARP que se envía a la dirección IP especificada.

3. **Recepción de Respuestas**: La función procesa las respuestas de los dispositivos en la red. Se extrae la dirección IP y la dirección MAC de cada dispositivo que responde.

      devices = []

      for sent, received in result:

         devices.append({'ip': received.psrc, 'mac': received.hwsrc})

4. **Salida de Resultados**: Finalmente, se imprime la lista de dispositivos detectados con sus respectivas direcciones IP y MAC.

   return devices

5. **Ejecución del Escáner**: Al ejecutar el script similar al proceso empleado en la imagen 19, el usuario puede especificar previamente un rango de IP’s que desea escanear, y posteriormente se invoca la función scan().

```
PS C:\Users\tadsv> & C:/Users/tadsv/AppData/Local/Programs/Python/Python313/python.exe c:/Users/tadsv/Downloads/network_scan.py
Scanning IP range: 192.168.1.0/24
Sending ARP requests...
Begin emission

Finished sending 256 packets

Received 816 packets, got 1 answers, remaining 255 packets
Responses received.
Device found: IP = 192.168.1.2, MAC = 3c:7c:3f:e3:0d:18

IP                   MAC Address
-----------------------------------------
192.168.1.2          3c:7c:3f:e3:0d:18
PS C:\Users\tadsv>
```

Imagen 19. Ejecución de código fuente elaborado por el autor.

Análisis de caso

La creación de un escáner de red en Python es un proyecto valioso tanto para profesionales de redes como para estudiantes que deseen aprender sobre la administración de redes. La simplicidad y la potencia de scapy permiten implementar un escáner efectivo en poco tiempo. Sin embargo, es esencial utilizar estas herramientas de manera responsable y ética, ya que escanear redes sin autorización puede tener consecuencias legales.

Casos de Uso

1. **Administración de Redes**: Los administradores pueden utilizar escáneres de red para identificar dispositivos conectados, lo que facilita la gestión y el mantenimiento de la infraestructura de red.
2. **Seguridad Informática**: Los profesionales de la ciberseguridad pueden emplear escáneres para detectar dispositivos vulnerables o no autorizados en la red, ayudando a fortalecer la seguridad.
3. **Auditorías de Red**: Durante auditorías, los escáneres permiten a los auditores identificar dispositivos activos y sus configuraciones, asegurando que se cumplan las políticas de seguridad.
4. **Educación y Capacitación**: Estudiantes de redes y seguridad pueden aprender sobre el funcionamiento de las redes y la tecnología ARP mediante la práctica con escáneres de red.

Caso 2: Análisis de paquetes de red por medio de Python

Introducción

El packet sniffer es una herramienta que permite interceptar y analizar paquetes de datos que circulan por una red. En este contexto (basado en lo aprendido durante la materia de “Tecnologias de interconexión de redes”), Python se presenta como un lenguaje versátil y accesible para desarrollar este tipo de aplicaciones. Este resumen se centra en la creación de un packet sniffer utilizando Python, describiendo su funcionamiento, el código utilizado, casos de uso y conclusiones sobre su implementación.

Explicación del Código

Este caso tal como se muestra en la imagen 20, cubre un enfoque para crear un packet sniffer utilizando la biblioteca scapy, que facilita la manipulación de paquetes en redes. A continuación, se desglosa el código principal:

```python
from scapy.all import sniff
from scapy.layers.inet import IP, TCP, UDP, ICMP

def packet_callback(packet):
    if IP in packet:
        ip_layer = packet[IP]
        protocol = ip_layer.proto
        src_ip = ip_layer.src
        dst_ip = ip_layer.dst

        # Determine the protocol
        protocol_name = ""
        if protocol == 1:
            protocol_name = "ICMP"
        elif protocol == 6:
            protocol_name = "TCP"
        elif protocol == 17:
            protocol_name = "UDP"
        else:
            protocol_name = "Unknown Protocol"

        # Print packet details
        print(f"Protocol: {protocol_name}")
        print(f"Source IP: {src_ip}")
        print(f"Destination IP: {dst_ip}")
        print("-" * 50)

def main():
    # Capture packets on the default network interface
    sniff(prn=packet_callback, filter="ip", store=0)

if __name__ == "__main__":
    main()
```

Imagen 20. Código fuente de análisis de paquetes de red elaborado por el autor.

- **Importación de Bibliotecas**:

  from scapy.all import *

  Se importa scapy para poder utilizar sus funciones para capturar y analizar paquetes.

- **Definición de Funciones (packet_callback)**: Se define una función para manejar los paquetes capturados. Esta función puede extraer información relevante de cada paquete, como el protocolo, dirección IP de origen y destino, y puertos.

- **Captura de Paquetes**: Se utiliza la función sniff() de scapy para iniciar la captura de paquetes en la red.

  El parámetro prn indica la función que se llamará para cada paquete capturado, y count especifica el número de paquetes a capturar.

- **Ejecución**: Finalmente, el código se ejecuta tal como se ejemplifica en la imagen 21, lo que permite realizar la captura de paquetes en tiempo real.

```
--------------------------------------------------
Protocol: TCP
Source IP: 66.110.49.114
Destination IP: 192.168.50.220
--------------------------------------------------
Protocol: TCP
Source IP: 66.110.49.114
Destination IP: 192.168.50.220
--------------------------------------------------
Protocol: TCP
Source IP: 192.168.50.220
Destination IP: 66.110.49.114
--------------------------------------------------
Protocol: TCP
Source IP: 192.168.50.220
Destination IP: 66.110.49.114
--------------------------------------------------
```

Imagen 21. Ejecución de código fuente elaborado por el autor.

Análisis del caso:

El desarrollo de un packet sniffer en Python con scapy es una tarea accesible y educativa que permite a los desarrolladores entender mejor el funcionamiento de las redes. Esta herramienta no solo es útil para la educación en ciberseguridad, sino también para el diagnóstico de redes y la identificación de problemas de seguridad. Sin embargo, es fundamental utilizar estas herramientas de manera ética y legal, ya que la captura de tráfico sin autorización puede ser un delito.

Casos de Uso

1. **Análisis de Tráfico de Red**: Los administradores de red pueden utilizar un packet sniffer para monitorear el tráfico y detectar cuellos de botella o problemas de rendimiento.
2. **Seguridad en Redes**: Los profesionales de ciberseguridad pueden emplear estas herramientas para identificar accesos no autorizados o actividades sospechosas en la red.
3. **Educación y Aprendizaje**: Estudiantes y entusiastas de la programación pueden aprender sobre protocolos de red y análisis de datos mediante la práctica con packet sniffers.
4. **Desarrollo de Software de Red**: Los desarrolladores pueden usar packet sniffers para probar y depurar aplicaciones que interactúan con la red, asegurando que se manejen correctamente los paquetes de datos.

CONCLUSIONES

En base a las observaciones de conocimientos técnicos que me dieron mis superiores durante el programa trainee, aprendí a realizar resolución de problemas relacionados a la infraestructura empleada en IT, gestión de proyectos, análisis de datos aplicado a las finanzas y empleo de diversas herramientas de ciberseguridad con el objetivo de prevenir posibles situaciones de riesgo para la empresa.

Para el caso de ciberseguridad, al implementar y experimentar con estas herramientas, se adquiere un entendimiento profundo de los protocolos de red y la seguridad informática, habilidades cruciales en el mundo laboral actual. Estas competencias no solo mejoran la capacidad de diagnóstico y resolución de problemas en infraestructuras de red, sino que también abren oportunidades en campos como la administración de sistemas, la ciberseguridad y el desarrollo de software. Además, el dominio de Python y bibliotecas como scapy se traduce en una ventaja competitiva, permitiendo a los profesionales adaptarse y prosperar en un entorno tecnológico en constante evolución.

La retroalimentación recibida al presentar los datos de los diferentes proyectos realizados para cada rotación, me ayudaron a reforzar mi falta de experiencia en este tipo de reportes, siendo principalmente el área de finanzas donde pude aprender la importancia de explicar los tecnicismos empleados de una manera clara y sencilla para personal que no es directamente del área.

Los proyectos de los que formé parte durante el programa trainee me retroalimentaron en conocimientos técnicos adquiridos durante mis estudios en la Facultad de Ingeniería de la UNAM como Ingeniero en Telecomunicaciones, además de ayudarme en aprender y reforzar algunos aspectos del manejo de diversas situaciones en el día a día en la empresa con un factor que considero variable: el de las relaciones humanas.

Considero que haber tenido la posibilidad de rotar en cada área de las previamente mencionadas, me aportó bastante en mi crecimiento profesional y me dio la posibilidad de conocer las diversas herramientas que se utilizan día a día en la empresa para sus diferentes áreas de aplicación.

BIBLIOGRAFÍA

- Universidad de Pamplona. (2014, octubre). Administración de Base de Datos. https://www.unipamplona.edu.co/unipamplona/portalIG/home_109/recursos/octubre2014/administraciondeempresas/semestre5/11092015/adminbasedatos.pdf
- Simple reporting example – Knime. (s. f.). KNIME Community Hub. https://hub.knime.com/knime/spaces/Examples/latest/05_Reporting/01_BIRT/01_Simple_Example_for_Reporting~tFnUT054gmCSU-x3
- Emery, J. (2023). What is KNIME and tips for getting started. phData. https://www.phdata.io/blog/getting-started-with-knime/
- Colina Vargas, A. M. (s. f.). RETOS Y PERSPECTIVAS DE LAS TECNOLOGÍAS DE INFORMACIÓN. Universidad Ecotec. https://libros.ecotec.edu.ec/index.php/editorial/catalog/download/2/2/28-1?inline=1
- ¿Qué es la ciberseguridad? (2023, 17 agosto). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
- Antón, Á. (2023, 31 julio). ¿Qué es un EDR? - ADM Cloud & Services. ADM Cloud & Services. https://admcloudservices.com/blog/sistema-seguridad-edr-que-es.html
- Sharma, L. (2023). 13 Herramientas EDR para detectar y responder rápidamente a los ciberataques. Geekflare. https://geekflare.com/es/edr-tools/
- Du Mortier, G. (2021, 26 agosto). 8 Herramientas EDR para detectar ataques cibernéticos. Cosas de Nerds. https://cosasdenerds.com/herramientas-edr-para-detectar-ciberataques/

- Create a Packet Sniffer and Analyzer with Python. (s.f.). PySeek. https://pyseek.com/2024/07/creating-a-packet-sniffer-in-python/
- Create a Python Network Scanner: Find IPs & MACs. (s.f.-a). PySeek. https://pyseek.com/2024/07/create-a-network-scanner-using-python/

REFERENCIAS

[1] Chrisslater. (2024, 10 mayo). Construction Budget Excel Template / Cost Control Template - WebQS. webQS. https://mywebqs.com/downloads/construction-budget-template-excel/

[2] Mallorca, P. (2025, 14 enero). Psicólogos en Mallorca. Habilidades Sociales en el entorno laboral. https://www.psicomallorca.com/index.php/2021/02/05/habilidades-sociales/

[3] Concepción, D. (2019, 24 septiembre). Cómo enfrentar la llegada de la automatización en el trabajo. Diario Concepción. https://www.diarioconcepcion.cl/economia-y-negocios/2019/09/24/como-enfrentar-la-llegada-de-la-automatizacion-en-el-trabajo.html

[4] Fixed Asset Pro | MoneySoft® | Calculate Asset Depreciation, Fast. (2025, 20 enero). MoneySoft® - Resources For Sound Business DecisionsTM. https://moneysoft.com/fixed-asset-depreciation-software/

[5] Pcartier. (2021, 9 marzo). How to improve business agility with SAFe. News, tips & guidance for agile, development, Atlassian-Software (JIRA, Confluence, Bitbucket, . . .) and Google Cloud. https://seibert.group/blog/en/business-agility-with-safe/

[6] Trisigma. (2022, 19 mayo). Seguridad de Información - Seguridad y administracion informática. Seguridad y Administracion Informática. https://www.trisigma.mx/seguridadinformatica/

[7] Vulnerabilities Report. (2022). https://docs.activestate.com/platform/projects/vulnerabilities_remediation/

[8] Du Mortier, G. (2021, 26 agosto). 8 Herramientas EDR para detectar ataques cibernéticos. Cosas de Nerds. https://cosasdenerds.com/herramientas-edr-para-detectar-ciberataques/