ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Desarrollo de un Sistema Web y un Módulo de Seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información

MILTON ANDRÉS ESCOBAR QUINTANA
RAÚL OSWALDO ALARCÓN PÉREZ

Trabajo de Titulación modalidad Proyecto de investigación y Desarrollo presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA.

RIOBAMBA- ECUADOR
NOVIEMBRE DE 2023

DECLARACIÓN DE AUTENTICIDAD Y CESIÓN DE DERECHOS DE AUTOR

Nosotros, MILTON ANDRÉS ESCOBAR QUINTANA y RAÚL OSWALDO ALARCÓN PÉREZ, declaramos que el presente Proyecto de Investigación, es de nuestra autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autores, asumimos la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Milton Andrés Escobar Quintana	Raúl Oswaldo Alarcón Pérez
0202027447	0201871415

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **Desarrollo de un Sistema Web y un Módulo de Seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información,** de responsabilidad de los señores Milton Andrés Escobar Quintana y Raúl Oswaldo Alarcón Pérez, ha sido minuciosamente revisado por los miembros del Tribunal del Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos legales, en tal virtud el tribunal autoriza su presentación.

Ing. Ivan Mesias Hidalgo Cajo Mgtr.
PRESIDENTE _____

Ing. Verónica Vanessa Bermeo Jiménez Mgtr.
DIRECTORA _____

Ing. Carlos Roberto Villa Padilla Mgtr.
MIEMBRO _____

Ing. Braulio Adrián Caisaguano Villa Mgtr.
MIEMBRO _____

Noviembre de 2023

DEDICATORIA

La presente investigación está dedicada a Dios por ser nuestra luz, guía, fortaleza y su mano de fidelidad y amor quien ha estado con nosotros hasta el día de hoy, a nuestros padres quienes más influyeron en nuestras vidas, dándonos los mejores consejos, guiándonos y haciendo de nosotros personas de bien.

Finalmente dedicamos esta investigación a nuestra directora de tesis y miembros del tribunal y a todos nuestros amigos, por guiarnos y apoyarme cuando más los necesitábamos, por extender su mano en momentos difíciles y por el amor brindado cada día, de verdad mil gracias, siempre los llevaremos en nuestros corazones.

Raúl Oswaldo Alarcón Pérez
Milton Andrés Escobar Quintana

AGRADECIMIENTO

A todos quienes participaron para la realización y ejecución de este proyecto, a nuestras familias por su apoyo incondicional y un especial reconocimiento y agradecimiento a nuestra directora del trabajo de titulación Ing. Verónica Vanessa Bermeo Jiménez Mag. a nuestros miembros de tribunal Ing. Carlos Roberto Villa Padilla Mag. e Ing. Braulio Adrián Caisaguano Villa Mag. quienes fueron nuestra guía para que el proyecto se llevara a cabo.

Raúl Oswaldo Alarcón Pérez
Milton Andrés Escobar Quintana

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

RESUMEN

En la presente investigación se desarrolló un sistema web y un módulo de seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información. Dentro de la etapa de ingeniería de software del sistema, se aplicó la metodología espiral la misma que refleja la relación de tareas con prototipos rápidos, mayor paralelismo y concurrencia en las actividades de diseño y construcción. El diseño del módulo de seguridad se basó en la norma ISO 27001, misma que proporciona un marco para proteger la información y ayudar a las organizaciones a identificar y gestionar de una manera efectiva los riesgos que amenazan a la seguridad de la información, de esta manera se estableció los requisitos para la implementación, mantenimiento y mejora continua del sistema de seguridad de la información ayudando a proteger la confidencialidad, integridad y disponibilidad de la información. Con la implementación del sistema web y módulo de seguridad en una empresa que no disponía de estas herramientas se obtuvo como resultados una reducción de costos del 40%, mayor productividad en un 44%, aumento en la disponibilidad de la información del 50%, mayor confiabilidad en un 70%, mejor rendimiento de un 90% y mejora en la seguridad de la información en un 90%, de donde se concluye que la utilización de un sistema informático con técnicas de seguridad apropiadas implementadas en cualquier empresa ayudara a controlar y mitigar los riesgos que afecten a la integridad de la seguridad de la información.

Palabras Clave: DESARROLLO DE UN SISTEMA WEB. MÓDULO DE SEGURIDAD, NORMA ISO 27000, MITIGAR, CONTROLAR, INTEGRIDAD DE LA INFORMACIÓN

SUMMARY

In this research, a web system and a security module based on ISO 27000 standards were developed to mitigate and control information integrity. During the software engineering phase of the system, the spiral methodology was applied, reflecting a relationship between tasks with rapid prototypes, greater parallelism, and concurrency in design and construction activities. The security module design was based on ISO 27001 standards, which provide a framework for information protection and assist organizations in effectively identifying and managing information security risks. This established the requirements for implementing, maintaining, and continuously improving the information security system, thereby safeguarding the confidentiality, integrity, and availability of information. With the implementation of the web system and security module in a company that previously lacked these tools, the following results were obtained: a 40% reduction in costs, a 44% increase in productivity, a 50% improvement in information availability, a 70% increase in reliability, a 90% performance improvement, and a 90% enhancement in information security. From this, it is concluded that the use of a computer system with appropriate security techniques implemented in any company will help control and mitigate risks that affect information security integrity.

Keywords: WEB SYSTEM DEVELOPMENT, SECURITY MODULE, ISO 27000 STANDARD, MITIGATE, CONTROL, INFORMATION INTEGRITY.

CAPÍTULO I

1. INTRODUCCIÓN

Con el desarrollo acelerado de la tecnología también se ha visto un aumento considerable en los riesgos que afectan a la seguridad de la información de todas las empresas y organizaciones. Teniendo como consecuencias el no poder ofrecer en un 100% los servicios más esenciales que las entidades deberían ofrecer a sus clientes como es la Confidencialidad Integridad y Disponibilidad de la información.

En la búsqueda de soluciones a esta problemática surgen las normas ISO (Organización Internacional de Estandarización). Dentro de las cuales destaca la ISO 27001 que es la norma que define buenas prácticas que se encuentran asociadas a la seguridad de la información. El principal objetivo de esta norma es la defensa, la protección y la gestión de la información, siendo uno de los activos más importantes de la organización. La norma ISO 27001 define todos los requisitos genéricos y que se pueden aplicar a cualquier tipo de empresa, sin importar su tamaño o tipo.

Dentro de esta investigación se propone elaborar un sistema informático que automatice los procesos y transacciones financieras como son la recepción de cobros de los diferentes rubros que se manejen en la entidad a intervenir, para lo cual se aplicara varias normas importantes que se estipulan en las normas ISO 27001 dentro del desarrollo de la plataforma informática las mismas que ayuden a controlar los riesgos que puedan afectar a la confidencialidad, disponibilidad pero poniendo un mayor énfasis a la integridad de la información que se maneja en esta empresa (DIALNET, 2023).

Es importante mencionar también que no se aplicara todas las normas que recomienda la ISO 27001, si no que más bien se pretende elaborar un modelo con varias seguridades de la información que se requieren de manera específica para esta investigación.

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la siguiente figura:

Fuente: (Normas ISO, 2020)

1.1. PLANTEAMIENTO DE PROBLEMA

1.1.1. Situación problemática

Las entidades públicas y privadas dedicadas a ofrecer servicios en los que involucran cobros de rubros por diferentes conceptos, disponen necesariamente de personal dedicado al área financiera y a lo económico, quienes son los encargados de registrar, archivar, disponer, reportar, respaldar la información del capital económico que fluye mediante las transacciones realizadas. Este proceso puede convertirse en una tarea mucho más agradable y fácil de conllevar con la ayuda de los sistemas informáticos, pero así mismo este proceso puede convertirse en un dolor de cabeza y más que eso ocasionar pérdidas económicas que pueden llevar a la quiebra hasta las empresas más grandes y poderosas a nivel mundial si no se maneja la información de forma íntegra y correcta.

En el Instituto de Posgrado y Educación Continua de la ESPOCH es una empresa dedicada a prestar sus servicios en formación de profesionales de cuarto nivel otorgando títulos de magister a sus estudiantes, sin embargo no cuenta con un sistema informático en el área financiera para registrar los pagos de los estudiantes por rubros como es preinscripción, inscripción, matricula, colegiatura, certificados, derechos, traducciones,

por lo que todas estas transacciones se las realiza de acuerdo a la modalidad que la persona de turno crea conveniente convirtiéndose en un gravísimo problema para el instituto de posgrado y la ESPOCH, ya que al momento de que la persona encargada de los cobros es trasladada a otra unidad o simplemente es despedida toda la información económica queda registrada en documentos físicos, archivos de Excel guardados en carpetas en un computador pero que no son entendibles para la próxima persona que se hace cargo de esa función, sin poder dar un seguimiento correcto, oportuno y continuo en lo que tiene que ver en cobros, deudas y reportes de información financiera, además hasta que la persona pueda empaparse de toda la información que ha recibido por el empleado anterior le conlleva una gran cantidad de tiempo, ocasionando una descoordinación en los procesos con las demás áreas del instituto presentado así una mala imagen a los usuarios finales y público en general. Otro problema no menor que presenta el Instituto de Posgrado, es que no se tiene estandarizado el formato de los comprobantes o certificados entregados a los estudiantes por concepto de pagos, el Instituto puede garantizar la integridad de la información en los documentos físicos entregados, pero al no contar con mecanismos de seguridad en los certificados físicos otorgados, no puede garantizar que esa información no sufra modificaciones o falsificaciones posteriormente es decir las personas que reciben estos documentos podrían modificar los documentos para beneficio personal, convirtiéndose en un delito que puede afectar no solo al Instituto de Posgrado sino también a las empresas que reciban estos documentos que además es un problema grave dentro de la sociedad que se castiga con prisión.

De este tipo de fraude por desgracia, no está exenta ninguna empresa ya sea pequeña o grande la falsificación de documentos ha estado presente en los sectores financieros, de construcción, industria manufacturera, comercio al mayoreo y menudeo, tecnologías, telecomunicaciones, etc., lógicamente los daños ocasionados han sido mayores en organizaciones medianas y grandes, pero todas, sin excepción, han resentido las consecuencias nocivas de los fraudes.

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede mejorar la integridad de la información en el área financiera del Instituto de Posgrado y Educación Continua con la implementación de un sistema y módulo de seguridad?

1.3. PREGUNTAS DIRECTRICES O ESPECÍFICAS DE LA INVESTIGACIÓN

- ¿Cómo mejorar la seguridad de la información sin influir negativamente el rendimiento de los procesos en el área financiera?
- ¿Cómo determinar vulnerabilidades referentes a la integridad y falsificación de documentos emitidos por el sistema financiero de posgrado?
- ¿Cómo mejorar la seguridad de la información con la implementación de un código QR en los reportes físicos impresos?

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

En la actualidad a nivel mundial la telemática es un medio obligatorio para realizar varias de nuestras actividades, se utiliza sistemas para educación, comunicación, financieras, compras, redes sociales y más, por lo que las empresas que aún no utilizan medios digitales, sistemas informáticos dentro de sus actividades su rendimiento de producción se verá afectado ya que los procesos que realiza una persona en el ámbito laboral no se puede comparar con la velocidad a los que trabaja un sistema informático. El Instituto de posgrado no cuenta con un programa informático, razones por las que el desarrollo e implementación de un sistema que automatice los procesos en el área financiera, es una de las principales razones que justifica realizar este proyecto de investigación, que además incorpora un módulo de seguridad normado por la ISO 27000 en lo que se refiere a la integridad de la información, es decir el proceso de transferencia de información laboral almacenada por un empleado público en cierto periodo de tiempo, este disponible de forma segura, clara, completa para la o las personas que tome la posta, se combatirá también la falsificación de documentos mediante la inserción de códigos QR en los archivos impresos, que garantice que los certificados físicos financieros presentados por los estudiantes en procesos como inscripciones, matriculas, pre defensas, defensas, graduación de un programa de maestría o finalización de cursos, son una fiel copia de la información que reposa en el sistema financiero sin que haya sufrido modificaciones o peor aún que ni siquiera haya sido emitido por el sistema del IPEC sino más bien podría haber sido elaborado por personas inescrupulosas dedicadas a la falsificación de documentos ocasionando varios problemas económicos y de legibilidad de títulos obtenidos en la institución, en la actualidad estos certificados no cuenta con seguridades extras anti falsificación, justificando plenamente la incorporación del mecanismo de seguridad de información planteado (QR), se manejara también la seguridad de la

información que viaja a través de la red para que no sea alterada y llegue integra al punto de origen (I+D, 2020).

Resumiendo se puede manifestar que el desarrollo de este proyecto se justifica por varias razones: automatización y velocidad en los procesos financieros, seguridad en la información emitida, continuidad en el registro y almacenamiento de la información.

1.5. OBJETIVOS DE LA INVESTIGACIÓN

1.5.1. Objetivo general

Desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información.

1.5.2. Objetivos específicos

- Desarrollo de un sistema web para el registro de cobros del Instituto de Posgrado y Educación Continua de la ESPOCH.
- Desarrollo de un módulo de seguridad que reduzca las vulnerabilidades a la integridad de la información basado en la norma ISO 27000
- Implementación del módulo de seguridad en el sistema web de cobros del Instituto de Posgrado y Educación Continua de la ESPOCH.
- Validar los resultados para determinar la reducción de vulnerabilidades referente a la integridad de la información en el área financiera del Instituto de Posgrado

1.6. HIPÓTESIS

1.6.1. Hipótesis general

H0: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, NO permitirá mitigar y controlar la integridad de la información del área financiera del instituto de posgrado y educación continua de la Escuela Superior Politécnica de Chimborazo.

H1: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, SI permitirá mitigar y controlar la integridad de la información del área financiera del Instituto de Posgrado y Educación Continua de la Escuela Superior Politécnica de Chimborazo.

1.6.2. Hipótesis específicas

- La elaboración del sustento teórico y conceptual fundamenta la investigación.
- La implementación de un sistema web permite mejorar la integridad de la información de los procesos financieros del Instituto de Posgrado.
- La implementación de un módulo de seguridad basado en la norma ISO 27000 en el sistema web financiero si reducirá las vulnerabilidades a la integridad de la información.

1.7. IDENTIFICACIÓN DE LAS VARIABLES

Variable Independiente: Implementación de un módulo de seguridad en el desarrollo de un sistema web.

Variable Dependiente: Mitigar y controlar la integridad de la información.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. ANTECEDENTES DEL PROBLEMA

La automatización de los procesos financieros en las empresas a nivel mundial no es nuevo, las cooperativas, los bancos y varias instituciones que realizan transacciones financieras en sus actividades cotidianas se vieron en la necesidad de utilizar sistemas informáticos en sus procesos ya que con ello ayudaban agilitar sus tareas, mayor precisión en cálculos, disminución de errores y varias ventajas sobre el ser humano, sin embargo la seguridad de la información se podría decir que recién en esta última década se le ha dado la importancia que realmente merece, los ataques informáticos que se producen a nivel mundial y que van en aumento día a día ocasionando pérdidas económicas, estafas, falsificaciones y muchas maneras más de ciberdelincuencia ayudado a que se le dé la importancia necesaria, a continuación se presentara algunos temas relacionados y similares al proyecto presentado.

La investigación realizada por (Amaya, Juez, 2016) con el tema: "Análisis, diseño, desarrollo e implementación de un sistema de control para registros y cobro de matrícula y pensiones para la unidad educativa particular mixta Mercedes de Jesús Molina mediante un aplicativo web.", en la que se concluye lo siguiente:

Se facilitó el registro y procesamiento de la información de los cobros de matrículas y pensiones a través de la aplicación. Además, se logró un impacto positivo en los administradores de la institución como son la directiva, directora, secretaria y la superiora de la comunidad ya que con la aplicación obtienen de manera precisa los deudores.

Se recomienda:

Al manipular el sistema de información, se debe llevar a cabo con cautela, disciplina y responsabilidad para así lograr una mejor administración y control de los procesos y cuidado de los recursos informáticos, los usuarios antes de hacer uso del sistema por primera vez deberían revisar detenidamente el manual de usuario para un correcto uso del mismo

Así mismo se muestra el estudio de (Can, 2015), con el tema: "Análisis y estudio del código QR y su aplicación en centros de información", en la que se concluye lo siguiente:

Debido a que los códigos QR no son intuitivos de naturaleza y se necesitan aplicaciones de identificación para la decodificación de sus contenidos, una de las propuestas podría ser añadir informaciones como textos o imágenes sobre su uso en el propio código QR basándose en su tolerancia a errores. Asimismo, como los códigos QR originales son en blanco y negro, para que sean más atractivos, podríamos crear códigos QR con color, e incluso integrarlos con elementos creativos.

En segundo lugar, aunque los códigos QR tienen una gran capacidad de guardar informaciones, no funcionan perfectamente en todas las situaciones. Por ejemplo, en un monitor que cambia de publicidades con mucha frecuencia no es un sitio conveniente para la aplicación de códigos QR, ya que los usuarios tendrán que correr de prisa para el escaneo. Además, hay que tener en cuenta la velocidad de la transmisión de información del internet móvil cuando queremos ofrecer recursos electrónicos a los usuarios a través de códigos QR. Si un código QR contiene demasiada información, tampoco sería una buena experiencia cuando los usuarios sufren la lenta velocidad de carga de una página web. En cambio, un código QR que se dirige a informaciones precisas es lo que pretenden los usuarios (CEPAL, 2022).

Igualmente, pese a que los códigos QR requieren el escaneo para decodificar su contenido, mucha gente tiene curiosidad en descubrir lo que contienen para la utilización de servicios asociados a ellos. Y por ello hay que establecer sistemas de seguridad para evitar posibles riegos de virus informático y para que la gente disfrute de los servicios sin preocupaciones.

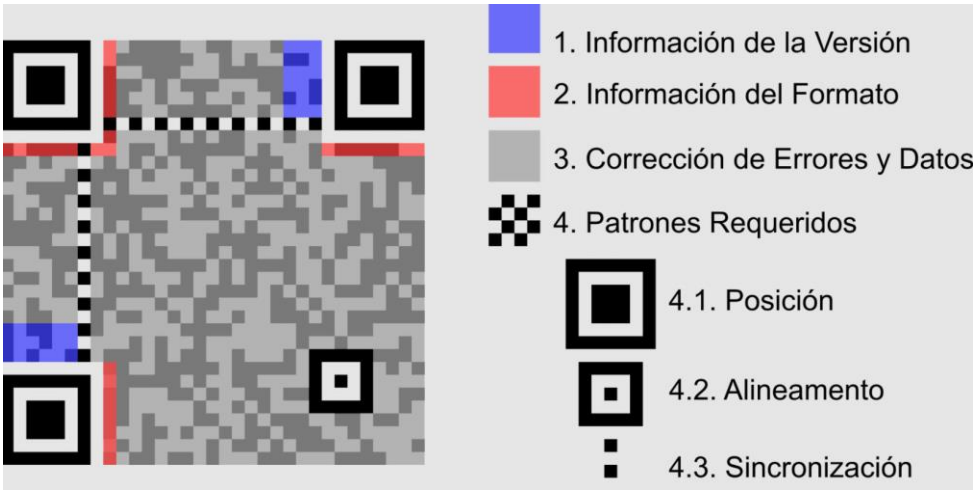


Figura 1-2: Código QR
Fuente: (Juan Ranchal, 2021)

La Escuela Superior Politécnica de Chimborazo presenta en sus diferentes sistemas informáticos, mecanismos de seguridad tratados en este proyecto como es la implementación de certificados SSL en el sistema de cobros a nivel general https://ordenespago.espoch.edu.ec/, el respaldo de la información mediante la creación automática de backups 2 veces por día en el sistema académico de posgrado sisepec.espoch.edu.ec, métodos de autenticidad mediante correos institucionales a todos sus sistemas web, etc. antecedentes que servirán de un gran apoyo al momento de elaborar el módulo de seguridad propuesto.

2.2. BASES TEÓRICAS

2.2.1. Sistemas web

Los sistemas Web o aplicaciones Web son un tipo de software codificados en un lenguaje de programación que presenta mucho dinamismo y funcionalidades muy potentes a casos particulares están creados e instalados no sobre una plataforma o sistemas operativos (Windows, Linux), sino que se alojan en un servidor en Internet o sobre una intranet (red local). Los sistemas Web funcionan sobre cualquier plataforma y sobre cualquier navegador Web Chrome, Firefox, Internet Explorer, etc. y no es necesario instalar en cada computadora personal que además no se puede porque no es un instalador sino más bien los usuarios se conectan a un servidor donde se aloja el sistema (Raquel, 2022).

La Ingeniería de Software es la que regula la forma de creación de un sistema web mediante un conjunto de procesos, herramientas y métodos de una forma organizada, conocido como metodología de desarrollo cumpliendo un papel importantísimo durante todo el proceso. Existen dos tipos de metodologías para el desarrollo del software; las metodologías tradicionales las cuales han demostrado ser funcionales y efectivas en proyectos pequeños y de gran tamaño en relación al tiempo y recursos utilizados técnicas como el control riguroso en todos los procesos, modelado de datos y documentación detallada y las metodologías ágiles mismas que tratan de mejorar varios aspectos en el software desarrollado tales como; tiempos, mantenimiento de la calidad del software, flexibilidad.

Figura 2-1: Metodologías Tradicionales vs Metodologías Ágiles
Fuente: (IEBS Digital School, 2023)

Tabla 1-2: Comparativa entre las metodologías tradicionales y agiles

METODOLOGÍAS TRADICIONALES	METODOLOGÍAS AGILES
Sigue las normas y estándares y políticas establecidas en el ambiente de desarrollo.	Puede respetar los estándares y normas establecidas si es necesario, pero más bien fundamenta el desarrollo en la experiencia obtenida en varios proyectos realizados es más libre.
Acepta muy pocos o ningún cambio en el desarrollo del proyecto.	Si es necesario y fundamental aceptan cambios durante todo el proceso de desarrollo del proyecto.
Al inicio del desarrollo se establece un contrato y plazos.	El contrato se firma al final del proyecto, ya que depende de todo lo realizado incluyendo los cambios solicitados, es mucho más flexible.
El cliente interactúa con el equipo de desarrollo de una manera formal con reuniones documentadas.	El cliente es parte del equipo de desarrollo interactúa directamente en todo momento cuando se lo requiera.
Respeta mucho las normas a la hora del desarrollo ocasionando pérdida de tiempo.	Si es necesario todos colaboran en cualquier etapa del desarrollo.
Mayor relevancia en la utilización de modelos en la arquitectura del software.	Menor relevancia en la arquitectura y mayor énfasis en la funcionalidad del software

Realizado por: Escobar, M. Alarcón, R, 2023.

Desde la aparición de los sistemas web su cambio ha sido muy agresivo cada año adoptando diferentes tendencias y otorgando cada vez mejoras en sus servicios a sus usuarios a continuación se presenta una tabla con las principales características y evolución de los elementos que forman parte de los sistemas web.

Tabla 2-1: Principales características de los sistemas web

CARACTERISTICAS:
• Elementos 3D interactivos • Neomorfismo: diseño web tridimensional • Gráficos de gran calidad con SVG (archivos pequeños) • Microinteracciones: efectos de animación. • Usabilidad
TENDENCIAS
▪ Utilización de la tecnología 5G: es decir altísima velocidad en la transferencia de datos, disminución de hasta diez veces en la latencia, mientras mejora el rendimiento general de la red y la capacidad de tráfico, es decir, hablamos de una tecnología que será hasta 100 veces más rápida y potente en comparación con la 4G (100 mgbs de subida y 20 mgbs de bajada y 1 gigabit por segundo para conexiones de baja movilidad) en el 2021. ▪ Aplicaciones basadas en la nube: capacidad de transferir y almacenar datos sin utilizar la memoria o espacio de disco de los dispositivos. ▪ Inteligencia artificial y aprendizaje automático: se intenta permitir que las aplicaciones trabajen de manera automática con la capacidad de atender, observar y analizar patrones de comportamiento ya sea de los procesos repetitivos o usuarios. ▪ AMP-Páginas web aceleradas por Google: se refiere a que el propio buscador las promocione
PRINCIPALES TIENDAS DE APLICACIONES
▪ Google Play ▪ Apple Store ▪ Windows ▪ Amazon o Blackberry

Realizado por: Escobar, M. Alarcón, R, 2023.

Servidor es un ordenador de gran potencia que se encarga de "prestar el servicio" de transmitir la información pedida por sus clientes. Los **Servidores** web son un componente de los servidores que tienen como principal función almacenar, en web hosting, todos los archivos propios de una página web (imágenes, textos, videos, etc.) y transmitirlos a los usuarios a través de los navegadores mediante el protocolo HTTP (Hipertext Transfer Protocol) (Souza, 2023)

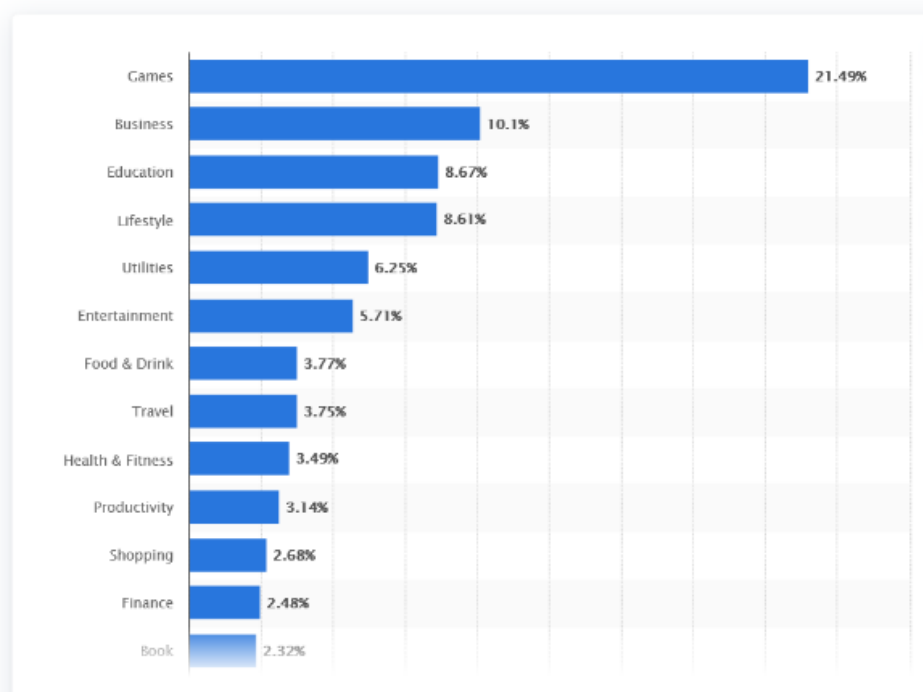


Figura 3-2: Ranking de las principales aplicaciones a nivel mundial.
Fuente: (Centro de estadísticas de aplicaciones, 2021)

2.2.2. Seguridad de la información

La Seguridad de la Información (S-I) es un conjunto de controles, políticas, técnicas, antivirus, cortafuegos, cifrado de datos y buenas practicas realizadas por personas especializadas encaminadas a minimizar o eliminar definitivamente los ataques, vulnerabilidades, desastres naturales o disturbios sociales que pongan en peligro o destruyan la información de una institución es de suma importancia siempre mantener los 3 principales pilares de la seguridad, la confidencialidad, la integridad y la disponibilidad de la información de la empresa.

- **Confidencialidad:** es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
- **Integridad:** es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
- **Disponibilidad:** es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

La información además se puede clasificar como Crítica, Valiosa, Sw¿ensible.

2.2.3. Elementos de la seguridad informática

Control: solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

Autenticidad: definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

No Repudio: evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

Auditoria: determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

Operatividad vs Seguridad: con una buena operatividad se puede minimizar los riesgos de vulnerabilidades.

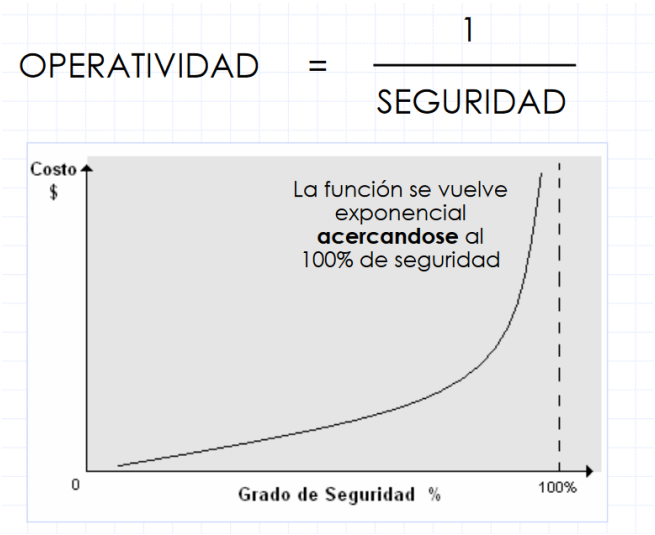


Figura 4-2: Operatividad vs Seguridad
Fuente: (Cristian Borghello, 2023)

2.2.4. Seguridad física

Se refiere a la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información tales como:

Amenazas: se refiere a los sucesos a los que está expuesto los equipos informáticos que contiene la información de una entidad tales como:

- ✓ Incendios
- ✓ Inundaciones
- ✓ Terremotos
- ✓ Trabajos no ergo métricos
- ✓ Instalaciones eléctricas
  - • Cableados defectuosos
  - • Suministro ininterrumpido de corriente
  - • Estática
- ✓ Seguridad del equipamiento

Controles: acciones o mecanismos que se puede implementar para contrarrestar las amenazas físicas hacia la información de datos:

- Sistemas de alarma
- Control de personas
- Control de vehículos
- Barreras infrarrojas-ultrasónicas
- Control de hardware
- Controles biométricos
- Huellas digitales
- Control de voz
- Patrones oculares
- Verificación de firmas

2.2.5. Seguridad lógica

Se refiere a la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a las personas autorizadas para hacerlo.

Identificación: El usuario se da a conocer al sistema.
Autentificación: Verificación del sistema ante la Identificación.

Formas de Autentificación-Verificación:

- ✓ Algo que la persona conoce - Password
- ✓ Algo que la persona es - Huella digital
- ✓ Algo que la persona hace - Firmar

- ✓ Algo que la persona posee - Token Card

2.2.6. Delito informático

Definido como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. Se realizan por medios informáticos y tienen como objeto a la información en sí misma por ejemplo:

- ✓ Fraudes cometidos mediante manipulación de computadoras
- ✓ Daños a programas o datos almacenados
- ✓ Manipulación de datos de E/S
- ✓ Distribución de virus
- ✓ Espionaje
- ✓ Acceso no autorizado
- ✓ Reproducción y distribución de programas protegido por la ley

2.2.7. Amenazas humanas: Hacker, Cracker, Phreaker, Pirata Informático, Insider.

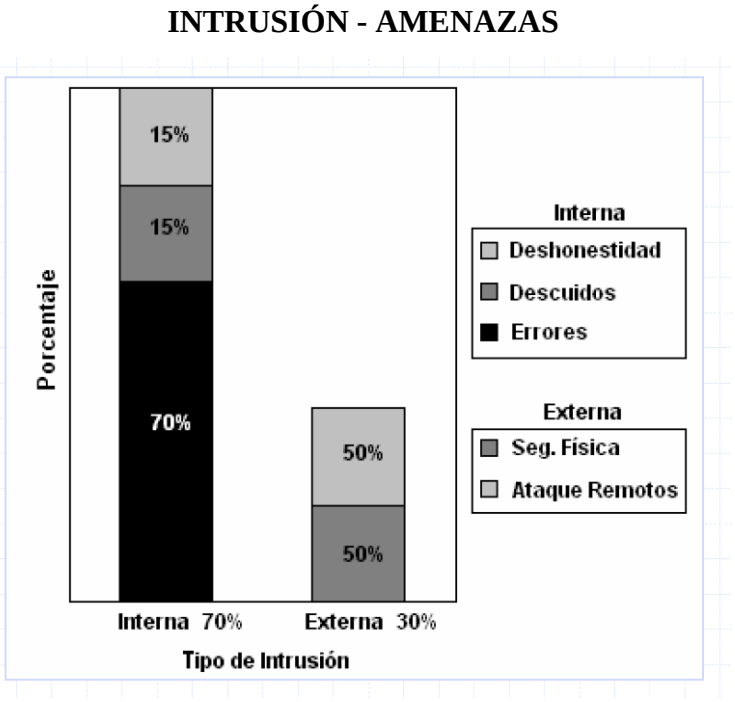


Figura 5-2: Intrusión vs Amenazas
Fuente: (Cristian Borghello, 2023)

2.2.8. Comunicaciones

Protocolo: conjunto de normas que rige el intercambio de información entre dos computadoras.

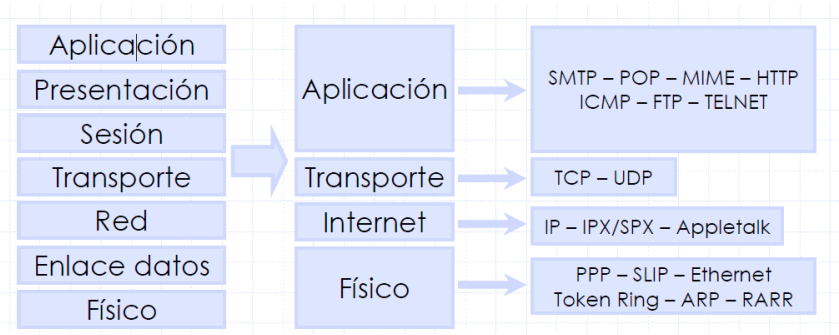


Figura 6-2: Modelo OSI vs Modelo TCP/IP
Fuente: (Cristian Borghello, 2023)

2.2.9. Amenazas

Una amenaza informática es cualquier acto que aprovecha una vulnerabilidad para atacar o piratear un sistema informático. Las amenazas de TI empresarial provienen en gran medida de ataques externos, aunque también existen amenazas internas (Tarazona, 2006)

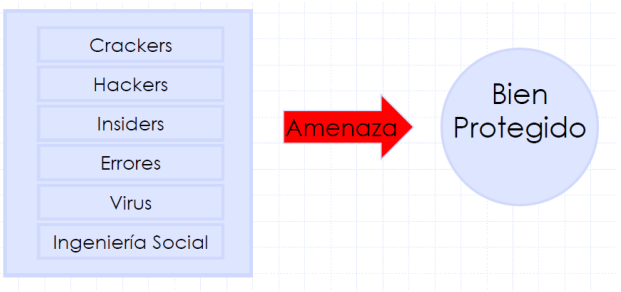


Figura 7-2: Amenazas Informáticas
Fuente: (Cristian Borghello, 2023)

Tipos de Ataques

- ✓ Ingeniería Social – Social Inversa
- ✓ Trashing
- ✓ Vulnerabilidades propias de los sistemas

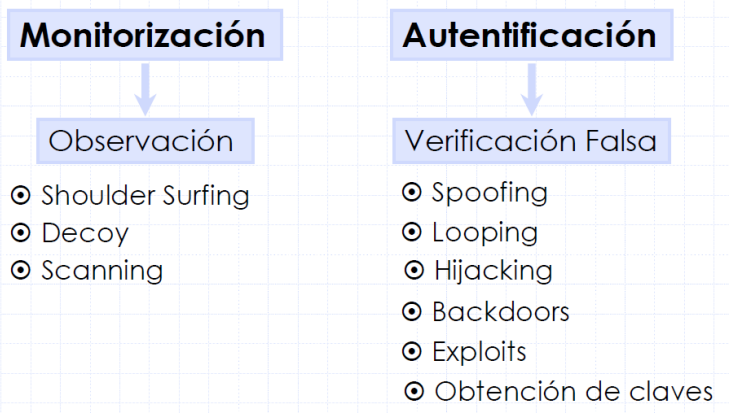


Figura 8-2: Ataques Informáticos
Fuente: (Cristian Borghello, 2023)

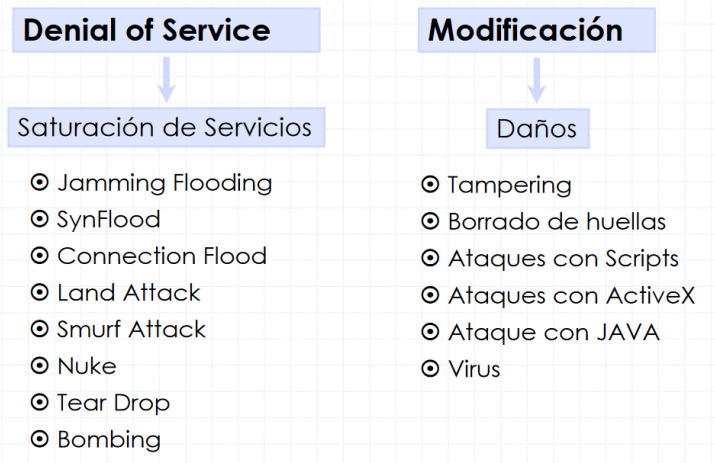


Figura 9-2: Ataques Informáticos
Fuente: (Cristian Borghello, 2023)

Implementación	Defensa
➢ Recopilación de información	➢ Mantener hardware actualizado
➢ Exploración del sistema	➢ No permitir tráfico broadcast
➢ Enumeración e identificación	➢ Filtrar tráfico de red
➢ Intrusión	➢ Auditorías
	➢ Actualización de los sistemas
	➢ Capacitación permanente

2.2.10. Virus

Programa de actuar subrepticio para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o daño de los programas, información y/o hardware afectados.

Figura 10-2: Modelo de mutación de virus
Fuente: (Cristian Borghello, 2023)

Tipos de Virus

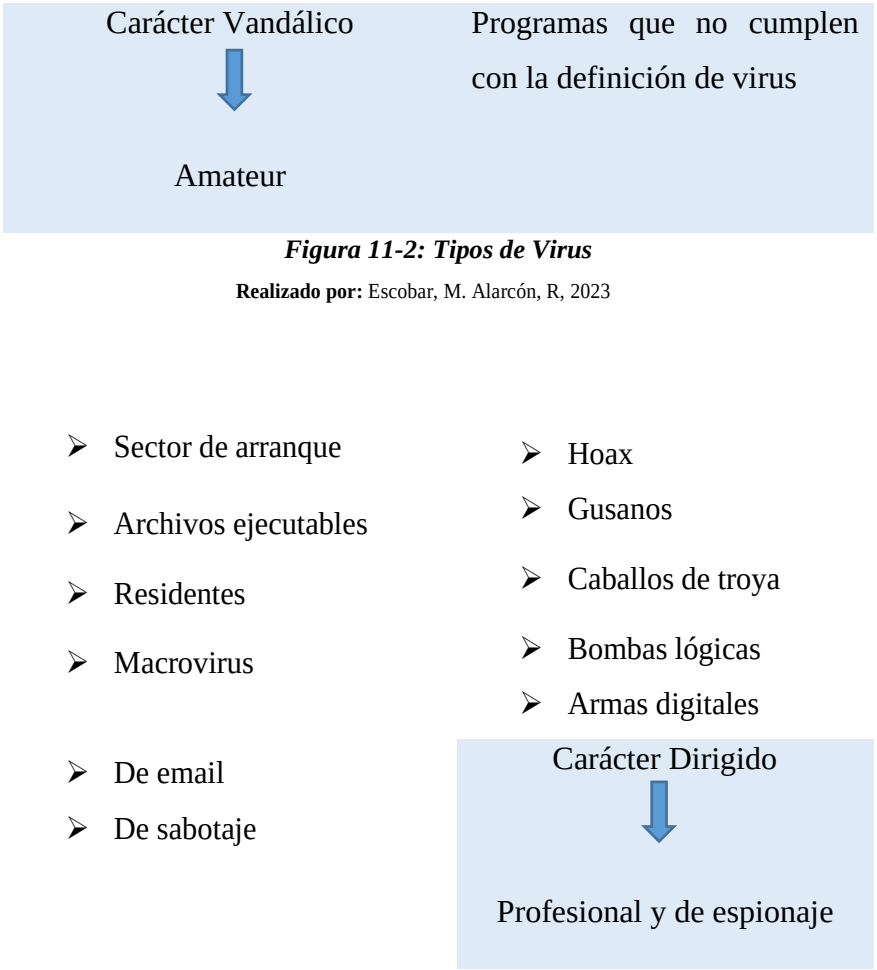
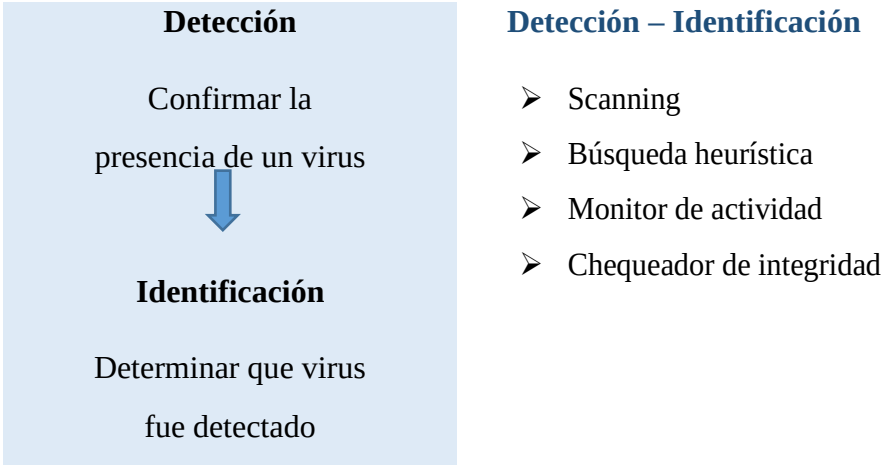


Figura 11-2: Tipos de Virus

Realizado por: Escobar, M. Alarcón, R, 2023

.

Antivirus: definido como una gran base de datos con la "huella digital" de todos los virus conocidos para identificarlos y también con las pautas más comunes de los virus.



Passwords

Normas de elección de passwords

- No usar contraseñas con algún significado.
- No utilizar contraseñas que sean palabras.
- Mezclar caracteres alfanuméricos.
- Longitud mínima de 7 caracteres.
- Contraseñas diferentes en sistemas diferentes.
- Ser fáciles de recordar >> Uso de nmotécnicos.

Normas de gestión de passwords

- NO permitir cuentas sin contraseña.
- NO mantener las contraseñas por defecto.
- NO compartirlas.
- NO escribir, enviar o decir la contraseña.
- Cambiarlas periódicamente.

2.3. POR QUÉ ES IMPORTANTE LA SEGURIDAD DE LA INFORMACIÓN

Se ha mencionado un poco acerca de la necesidad de garantizar la seguridad de la información y después de tener un mapa más amplio sobre ella, ya podemos vislumbrar algunas amenazas y riesgos que nos llevan una vez más, a reconocer su importancia.

Sin embargo, es importante ahondar en el tema, ya que hay riesgos y amenazas que todavía no alcanzamos a identificar y que es importante hacerlo, ya que nos permitirán conocer las acciones y medidas que necesitamos implementar para evadirlas.

2.3.1. Robo de información

Probablemente esta sea la más obvia de todas las razones para considerar la seguridad de la información como parte de la organización de la empresa. Sin embargo, hay implicaciones a estos robos.

Por ejemplo, cada empresa construye su *know how* que no es otra cosa que el perfeccionamiento de sus procesos con respecto al interior, el saber cómo llegar al

resultado o producto esperado. Ese es un bien o activo intelectual de la empresa, con mayor valor en algunos casos que los bienes inmuebles.

El momento en que sucede ese robo de información, esa información queda vulnerable, ofreciendo lo que significan años de trabajo a otros, eso sin mencionar la vulnerabilidad al interior de la empresa pues prácticamente quedan al desnudo.

2.3.2. Pérdidas económicas

La pérdida de activos en sí ya representa una pérdida económica, pero al vulnerar nuestra información, también se corre el riesgo de perder capital y liquidez.

El dinero es común que se maneje de forma digital hoy en día. Los billetes y monedas poco a poco han disminuido su influencia para darle paso a nuevas formas de comercio e intercambio, como las tarjetas de crédito y débito, las bancas digitales, transferencias interbancarias, entre otros.

Estas nuevas medidas nos llevan a correr riesgos. Un ejemplo es el robo de datos bancarios, de los cuáles hemos visto o cuando menos escuchado, que han existido miles de fraudes y robos que han puesto en riesgo las finanzas personales de muchos.

Esto no significa que esté mal el uso de los nuevos medios, simplemente implica una adaptación como personas a su protección: si antes protegías tu cartera, ahora vas a tener que proteger tu banca en línea.

Estos mecanismos no se crearon con la intención de correr mayores riesgos, al contrario, para proporcionarnos más comodidad, pero todo lleva una responsabilidad.

2.3.3. Confianza con los clientes

Como empresas, debemos de ser conscientes de que la mayor virtud como ofertantes de un bien o servicio, lo más importante es garantizar que la confianza que los clientes tienen con la empresa, no se vea en riesgo por ningún motivo.

Precisamente esa confianza puede estar en riesgo si no se protegen adecuadamente los datos y la información que los clientes proporcionan a la empresa como parte de la relación económica.

Por ejemplo: información confidencial, datos bancarios, registro de las operaciones, en fin, estos son solo unos ejemplos de los datos que como cliente no quisieras dar a conocer públicamente.

2.3.4. Vulnerabilidad ante la competencia

En la guerra y en el amor, todo se vale. Eso dice una vieja frase que parecen tomar en serio en el mundo de los negocios, ya que como hemos podido observar en los últimos años, los ciberataques han estado a la orden del día, no solo a las empresas, incluso a instituciones públicas.

La mayor parte de estos ataques se realizan con la intención de sabotear el trabajo, ya sea para lograr una ventaja comparativa sobre la competencia o, por el contrario, quitarles una ventaja.

El hecho es que, como un activo valioso, la información debe ser resguardada para evitar poner en riesgo la viabilidad de la empresa.

Sin embargo, esto no solo tiene que ver con ciberataques, también existen filtraciones de información e incluso falta de medidas de prevención que pueden poner en riesgo de manera muy sencilla la información.

Debemos ser muy conscientes de que la información es un bien que podemos utilizar a nuestro favor, pero también que puede ser usado en nuestra contra siempre, así la valoraremos más.

2.3.5. Seguridad personal

La información es poder, dicen por ahí, y eso es cierto, al ofrecer información estamos dándole cierto poder a la otra persona. Si lo pensamos así, probablemente seremos mucho más cuidadosos con el uso de la información.

Como parte de las vulnerabilidades, encontramos nuestra seguridad expuesta si no cuidamos nuestra información. Un ejemplo ya lo vimos con el robo de datos bancarios, sin embargo, existen un sin fin de malos usos que se puede dar a otro tipo de información.

Un ejemplo es la cantidad de escándalos que hemos visto en diarios o páginas de Internet debido a filtraciones de información o robos de datos a políticos, empresarios e incluso artistas.

Otro ejemplo la cautela con la que tenemos que cuidar información como bienes o la ubicación de nuestro hogar, ya que puede ser información utilizada por la delincuencia para atentar contra nosotros.

2.3.6. Competencia empresarial

Ya vimos que puede suceder cuando gente utiliza el pretexto de la competencia para realizar acciones poco éticas y sacar ventaja del resto.

Pero, por otro lado, ¿qué nos dirías si te decimos que la seguridad de la información también representa una oportunidad de mercado? Algo que puede convertirse en una ventaja comparativa con el resto o cuando menos no jugarnos en contra.

Al ser un tema que poco a poco ha tomado relevancia en el mundo, es una demanda cada vez más solicitada en el mercado y que muy pronto seguramente más que una demanda, se convertirá en una exigencia mínima a garantizar.

Conocer e implementar medidas de seguridad de la información permitirá ofrecer tranquilidad a los clientes acerca de los datos que ellos mismos proporcionan, ofrece seguridad al interior y da certeza de que los procesos no tendrán problema con la información para funcionar adecuadamente.

2.3.7. Toma de decisiones adecuada

Ya mencionamos que es tan importante asegurarnos de que la información no caiga en manos equivocadas como que la información sea veraz, ¿por qué? Bueno, la realidad es que la toma de decisiones tiene una base sólida en la información con la que contamos.

Supongamos que tenemos la oportunidad de abrir la empresa a nuevos mercados, una decisión que hará más competitiva a la organización y que permitirá tener mayor liquidez; sin embargo, también conlleva un riesgo de estabilidad por la gran inversión que requerirá.

Una decisión necesita contar con la mejor información: completa, veraz y confidencial, de otro modo estaremos apostando a ciegas.

Ahora imaginemos que contamos con esa información, pero un ataque o modificación pone en riesgo su integridad.

La inversión en seguridad de la información no solo es para hacerla más robusta, es una póliza de seguro que nos protege ante situaciones que esperamos que no sucedan, pero pueden suceder.

2.4. QUÉ MEDIDAS PODEMOS IMPLEMENTAR PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN

Existen diversas acciones para garantizar la protección de datos de la empresa, a continuación, te presentamos algunas:

2.4.1. Conoce la información con la que cuentas

El primer paso es tener un control sobre los activos informáticos que tenemos, elaborar un inventario que nos ayude a localizar toda la información de la empresa es indispensable.

2.4.2. Cataloga la información que tienes

Hay información más sensible, valiosa y crítica que otra. Por ello, es importante definir las características de la información para definir cuál es el trato que necesitamos darle. Por ejemplo: limitar acceso, garantizar la integridad o cuidar la disponibilidad de la misma.

2.4.3. Elabora un análisis de riesgos

Siempre hay que asumir el peor escenario posible para estar preparados ante cualquier situación. Define los riesgos que corre la empresa al perder cierta información y al mismo tiempo, establece un protocolo de acción en caso de que suceda, que te permita actuar a tiempo.

2.4.4. Establece controles y mecanismos

Todo esto para que estés protegido y armado para proteger la información: contraseñas de acceso, historial de visualizaciones y modificaciones, firma electrónica, etc.

Esta son parte de las medidas generales para cuidar la seguridad de la información, sin embargo, también existe una medida específica que ha sido la predilecta para muchas empresas. Esta es la utilización de software especializados en la protección de la información.

Estos servicios son útiles, pero existen algunos elementos que se deben considerar y que nos ayudan a llevar un mayor control de la protección, sin poner en riesgo a la empresa:

- **Adaptabilidad:** Es como un anillo a un dedo; en estos casos, nunca adaptas el dedo al anillo. Este es el mismo caso, el software se debe adaptar a la empresa, sus procesos y sus necesidades de seguridad.
- **Monitoreo:** Las amenazas pueden suceder en cualquier momento, por lo que es importante tener un monitoreo constante y continuo, ya que la respuesta ante un ataque debe ser inmediata para contener posibles daños.
- **Respuesta a incidencias:** La respuesta es indispensable ante una vulnerabilidad de seguridad, por ello se debe proporcionar un plan de atención en caso de incidencia.
- **Informes:** Se deben generar informes sobre el estado del servicio, áreas de oportunidad e información general del funcionamiento.

2.5. QUÉ RETOS ENFRENTA LA SEGURIDAD DE LA INFORMACIÓN

Como todo, hay retos y limitantes a las que se enfrenta la seguridad de la información, algunos son los siguientes:

2.5.1. Actualización constante

La tecnología avanza rápidamente en nuestros días, no pone a prueba y nos reta a ir a la par de ella. Este es el caso de la seguridad de la información.

Los avances imponen la necesidad de estar actualizados, ya que cualquier retraso puede ser crucial para la seguridad de las empresas, esto involucra un constante monitoreo de

las novedades tecnológicas y la constante modernización de los mecanismos de seguridad de las instituciones.

2.5.2. Capacitación al personal

La inseguridad de la información, como cualquier amenaza, debe ser una responsabilidad de todo el personal atenderla. Esto involucra desde el primer nivel hasta el personal de menor jerarquía.

Esto también conlleva responsabilidades como institución: enseñarles como cuidar y procurar la seguridad de la información de la empresa, por lo tanto la capacitación en implementación de software o incluso las medidas de seguridad tomadas como política de la empresa deben ser dadas a conocer.

Este es un reto, ya que cualquier grieta al interior puede vulnerar la seguridad total de la empresa.

2.5.3. Diversidad de amenazas

Las amenazas no se limitan al acceso a los sistemas de la empresa, existen muchas formas en que es vulnerable la información de la empresa.

Desde la información que se comparte a través de plataformas de mensajería, los ataques a la privacidad en espacios de trabajo, hasta simplemente las personas a nuestro alrededor que pueden escuchar cierta información que no debían.

Son muchas las amenazas, así como la necesidad de atenderlas.

Por eso es importante la implementación de protocolos y reglamentaciones que prevengan la filtración; pero que también blinden y protejan a las empresas en caso de que sucedan agresiones a su seguridad.

2.5.4. Hacer invisible la amenaza

A nadie le gusta sentir el miedo de ser vulnerable, y por eso es importante que la amenaza que representa la seguridad de la información sea atendida de manera eficiente y consistente, pero invisible para los usuarios y clientes para evitar levantar alarmas.

2.5.5. Falta de especialización en el tema

Aunque cada vez existe mayor demanda, la seguridad de la información sigue siendo un terreno a explorar y en la que todavía no existe una gran diversidad de especialistas en el tema, al contrario, es un campo limitado.

Es probable que en el futuro esto cambie y que se convierta en un área cada vez más importante para el sector empresarial, sin embargo, a día de hoy, representa un reto y problema. (IBERO, 2019)

2.6. MÓDULO DE SEGURIDAD

Dentro de los mecanismos para proteger la integridad de la información tenemos a los códigos QR: El código de respuesta rápida o QR por sus siglas en inglés (Quick Response) está representado en dos dimensiones (2D), esto significa que puede contener información tanto horizontal como verticalmente, algo que el código de barras que es de lectura unidimensional no es capaz de representar

El código QR de forma cuadrada conocido como "2D matrix" se puede identificar con facilidad por los tres cuadros oscuros enmarcados en tres de sus esquinas, que corresponden a un patrón característico de orientación, el cual posibilita su correcta lectura sin importar el ángulo que tenga el dispositivo lector respecto al patrón QR.

2.6.1. Características técnicas del código QR

Es importante resaltar que inicialmente fueron creados para registrar repuestos que se encontraban en el área de la fabricación de vehículos, sus partes y piezas. Llama la atención que los códigos QR, tenían el objetivo de ser aplicados en administración de inventarios de una gran variedad de industrias, además de describir que poseen estándares japonés para códigos QR (JIS X 0510) vinculados en la publicación de enero de 1998 y su correspondiente estándar internacional ISO(ISO/IEC18004) esta ideas expuestas se dieron aprobadas en el mes junio del año 2000.(Anderson, 2016)Resulta así mismo interesante, la inclusión de software que lee códigos QR en teléfonos móviles, para lograr se permita nuevos usos orientados al consumidor, sobre la base, de las ideas expuestas se manifiestan comodidades para el usuario tal como el dejar de tener que introducir datos de forma manual en los teléfonos. Un detalle importante que contribuye al uso de los códigos QR es que, a diferencia de otros formatos de códigos de barras bidimensionales, se caracteriza por ser un código abierto y sus derechos de patente (propiedad de Denso

Wave) no se ejercen. Resulta oportuno acotar que los códigos QR permiten la opción de poder ser leídos desde computadores personales, teléfonos inteligentes o tabletas, además observamos también que mediante los dispositivos móviles se ejecuta la de captura de imágenes en forma de escáneres o cámaras de fotos, esta funcional aplicación permite que estos programas lean los datos QR y las diversas conexiones a Internet para posteriormente ser direcciones al enlace que proporciona la información que posee.

En otras palabras las direcciones web y los enlaces URL se están volviendo cada vez más comunes en revistas y anuncios publicitarios de diversos productos y servicios que nos ofrece la tecnología, así mismo el agregado de códigos QR en tarjetas de presentación también se está haciendo común, lo mismo que permite simplificar en gran medida la tarea de introducir detalles individuales del nuevo cliente en la agenda de un teléfono móvil, contactos pertenecientes a redes social.(solutekcolombia, 2016)

2.6.2. Ventajas de los códigos QR

La comodidad del usuario los códigos QR proporcionan un procedimiento conveniente de un solo paso para dirigir a los usuarios a un sitio web, número de teléfono, direcciones, promociones u otra información.

Respetuoso del medio ambiente los códigos QR pueden hacer un uso más eficiente de los materiales impresos y reducir los residuos.

Rentable los códigos QR cuestan nada para producir su uso está limitado únicamente por su estrategia de marketing.

Versátil los códigos QR pueden ser integrados con una amplia gama de materiales de marketing para cualquier propósito, incluyendo material impreso, pantalla al aire libre y el correo directo, así como las páginas de destino que enlazar, se pueden ver en todos los modelos de teléfonos inteligentes populares y no requieren el desarrollo especial para diferentes plataformas (por ejemplo, iPhone vs Android), como es el caso de las aplicaciones, mensurables acciones desencadenadas a través de los códigos QR pueden ser rastreados con la analítica web y otras herramientas para la medición de campañas de marketing, diferenciación competitiva debido a los códigos QR son todavía respectivamente nuevos, y las empresas han encontrado una forma de diferenciarse en el mercado brindando

2.7. CERTIFICADOS SSL

SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros), la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los delincuentes lean y modifiquen cualquier dato que se transfiera, incluida información que pudiera considerarse personal. Los dos sistemas pueden ser un servidor y un cliente (por ejemplo, un sitio web de compras y un navegador) o de servidor a servidor (por ejemplo, una aplicación con información que puede identificarse como personal o con datos de nóminas). Esto lo lleva a cabo asegurándose de que todos los datos que se transfieren entre usuarios y sitios web o entre dos sistemas sean imposibles de leer. Utiliza algoritmos de cifrado para codificar los datos que se transmiten e impedir que los hackers los lean al enviarlos a través de la conexión. Esta información podría ser cualquier dato confidencial o personal, por ejemplo, números de tarjeta de crédito y otros datos bancarios, nombres y direcciones.

El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL. Si bien aún denominamos a nuestros certificados de seguridad SSL porque es un término más común, al comprar certificados SSL en DigiCert, en realidad se compran los certificados TLS más actualizados con la opción de cifrado ECC, RSA o DSA. HTTPS (Hyper Text Transfer Protocol Secure o protocolo seguro de transferencia de hipertexto) aparece en la dirección URL cuando un sitio web está protegido por un certificado SSL. Los detalles del certificado, por ejemplo la entidad emisora y el nombre corporativo del propietario del sitio web, se pueden ver haciendo clic en el símbolo de candado de la barra del navegador. (DigiCert, 2021)

2.8. NORMAS ISO 27000

Son un conjunto de normas y estándares credos por la ***Organización Internacional para la Estandarización*** (ISO) y ***la Comisión Electrónica Internacional*** (IEC) orientadas al establecimiento de buenas prácticas referente a la implantación, mantenimiento y gestión del ***Sistema de Gestión de Seguridad de la Información*** (SGSI).

ISO 27001.- Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Esta norma es certificable.

ISO 27002.- define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.

ISO 27003.- proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.

ISO 27004.- proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI

ISO 27005.- define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear.

ISO 27006.- establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001

ISO 27007.- es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001

ISO 27008.- define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.

ISO 27009.- complementa la norma 27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivo de hacer más eficaz su implantación.

ISO 27010.- indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas.

ISO 27011.- establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando como implantar los controles de manera eficiente.

ISO 27013.- establece una guía para la integración de las normas 27001 (SGSI) y 20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.

ISO 27014.- establece principios para el gobierno de la seguridad de la información, para que las organizaciones puedan evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información.

ISO 27015.- facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros, tales como servicios bancarios o banca electrónica.

ISO 27016.- proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones.

ISO 27017.- proporciona una guía de 37 controles específicos para los servicios cloud, estos controles están basados en la norma 27002.

ISO 27018.- complementa a las normas 27001 y 27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en cloud para terceros.

ISO 27019.- facilita una guía basada en la norma 27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI (https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/)

2.8.1. Resumen de las normas ISO

Tabla 3-2: Normas ISO

ISO	CARACTERISTICA
27001	Especifica las normas a implementar en un SGSI
27002	Define conjunto de normas a utilizar en el SGSI a implementar
27003	Proporciona la guía para implementar las seguridades
27004	Otorga las pautas
27005	Metodología a emplear
27006	Establece los requisitos
27007	Auditoria Internas
27008	Evalúa las técnicas mitigación de riesgos
27009	Aplicada a sectores específicos
27010	Como tratar la información al momento de ser compartida
27011	Dedicado a empresas de telecomunicaciones
27013	Guía para la integración de varias normas
27014	Establece principios para la evaluación, monitorización
27015	Principios de implantación SGSI entendidas bancarias
27016	Guía para toma de decisiones económicas vinculadas a la seguridad
27017	Guía de 37 controles definidos en la norma 27002
27018	Complementa los servicios en cloud de las normas 27001 y 27002

27019	Complemento de la norma 27002 para empresas vinculadas a la energía

Realizado por: Escobar, M. Alarcón, R, 2023.

2.9. IMPLEMENTACIÓN DE LAS NORMAS ISO EN EL SISTEMA FINANCIERO

En el desarrollo de esta investigación se trata de un sistema informático relacionado a otorgar servicios financieros por lo que se pone énfasis a las normativas de la ISO 270015 dedicada a la seguridad de la información en empresas que ofertan servicios financieros dentro de los cuales se recomienda utilizar varias técnicas de seguridad entre las principales tenemos:

2.9.1. Cifrado

La información confidencial se somete a un proceso de cifrado y se convierte en un código al que solo se puede acceder con la clave de descifrado correcta.

2.9.2. Autenticación de factores múltiples

El inicio de sesión con múltiples formas de autenticación se está convirtiendo en una opción popular, y no solo para los sitios web de servicios financieros.

2.9.3. Distribución y almacenamiento de datos

Almacenar datos en un solo lugar ya no es una opción segura para las empresas, incluso para aquellas que confían en los servicios de nube para almacenar información digital.

2.9.4. Inteligencia artificial (IA)

La IA unida a la biometría, es un método de identificación de los clientes que se basa en las características únicas de cada uno de ellos para obtener acceso a la información de la cuenta. Los reconocimientos ocular, facial y dactilar son funciones de muchos dispositivos inteligentes. Cada vez más bancos ofrecen estas opciones en sus aplicaciones móviles. Esto añade otro nivel más de seguridad, lo que dificulta el ingreso de los delincuentes a los sistemas.

2.10. MARCO CONCEPTUAL

Sistema: un sistema es un conjunto de elementos relacionados entre sí que funciona como un todo. (Significados.com, s.f.)

Modulo: es una serie de procedimientos o funciones capaces de asumir una gran diversidad de tareas, algunas más pequeñas que otras, y que ayudan a organizar el código de un programa. (Significados.com, s.f.)

Seguridad: La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. (Significados.com, s.f.)

ISO: Las siglas ISO representan a la Organización Internacional para la Estandarización; organismo responsable de regular un conjunto de normas para la fabricación, comercio y comunicación en todas las industrias y comercios del mundo. Este término también se le adjudica a las normas fijadas por el mismo organismo, para homogeneizar las técnicas de producción en las empresas y organizaciones internacionales. (Significados.com, s.f.)

Norma: Se conoce como norma a la regla o un conjunto de estas, una ley, una pauta o un principio que se impone, se adoptan y se debe seguir para realizar correctamente una acción o también para guiar, dirigir o ajustar la conducta o el comportamiento de los individuos. (Significados.com, s.f.)

Mitigar: hace referencia a minimizar o aliviar algo. Cuando un fenómeno o un efecto es mitigado, se reduce su intensidad o su rigurosidad. (Significados.com, s.f.)

Código: es una serie de símbolos que por separado no representan nada, pero al combinarlos pueden generar un lenguaje comprensible solo para aquellos quienes lo entiendan. Un código puede ser interpretado si se conoce su fuente (de donde proviene) y cuál es su objetivo (para que sirve), las condiciones sobre las cuales se cree un código son ampliamente variadas, ya que, no sólo los códigos son creados con el propósito de comunicarse, sino también para acceder a sitios en los que no está permitida la entrada de cualquier individuo. (Adrián, Yirda, 2021)

Códigos QR: Los códigos QR son códigos de barras bidimensionales. QR significa «quick response» (respuesta rápida), un término que hace referencia al acceso inmediato a la información que está oculta en el código. Son personalizables, tanto en diseño como en función, y constituyen el mejor canal para conectar los medios impresos tradicionales con cualquier contenido interactivo en línea. (Significados.com, s.f.)

Integridad: Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones

por terceros, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso. Por este motivo se debe proteger la información para que sólo sea modificada por la misma persona, evitando así que se pierda la integridad. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña o mediante huella digital. (ISOTools Excellence, 2017)

Información: es el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador. El procesador del mismo requiere de información para cumplir una orden recibida, y toda tarea computacional implica el intercambio de un dato informativo de un lugar a otro. Esto no sólo ocurre en forma electrónica al interior del ordenador, sino que también es natural a las acciones que un usuario cualquiera ejecute con una computadora. (DefiniciónABC, 2009)

Hardware: Es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y circuitos de luz, placas, utensilios, cadenas y cualquier otro material, en estado físico, que sea necesario para hacer que el equipo funcione. El término viene del inglés, significa partes duras. (Significados.com, s.f.)

Lenguaje de programación: es un idioma artificial diseñado para expresar computaciones que pueden ser llevadas a cabo por máquinas como las computadoras. Pueden usarse para crear programas que controlen el comportamiento físico y lógico de una máquina, para expresar algoritmos con precisión, o como modo de comunicación humana. Está formado por un conjunto de símbolos y reglas sintácticas y semánticas que definen su estructura y el significado de sus elementos y expresiones. Al proceso por el cual se escribe, prueba, depura, compila y mantiene el código fuente de un programa informático se le llama programación. (Cartago, 2012)

Programa: Un programa es una serie de instrucciones ordenadas, codificadas en lenguaje de programación que expresa un algoritmo y que puede ser ejecutado en un computador. (Capouya, 2009)

Sistema Web: Es similar a un sitio web, pero con mucho más dinamismo y funcionalidades muy potentes que brindan respuestas a casos particulares. Las

aplicaciones web son sistemas informáticos complejos, como los programas que antes teníamos en la computadora, pero para internet, es decir, que se codifican en lenguajes soportados por los navegadores web y se alojan en un servidor en Internet. Por ejemplo, un sistema para llevar la administración de una clínica, al que se accede mediante www o una red privada local, es una aplicación web. Las aplicaciones web siempre están en internet, pero pueden manejarse mediante intranets y extranets, depende la seguridad y privacidad requerida por el cliente. (Llamacreativa.com.ar, 2021)

Vulnerabilidades: La vulnerabilidad de seguridad o exploit del ordenador es un componente del código o del software que identifica los defectos de la seguridad de las aplicaciones, sistemas y redes para que los cibercriminales puedan beneficiarse de ellos. Normalmente forman parte de otro software y se distribuyen como parte de un kit, los exploits normalmente están alojados en páginas web afectadas. Los hackers pueden enviar emails de phishing para engañar a las víctimas potenciales para que visiten esas páginas web. (SoftwareLab.org)

2.11. Operacionalización de Variables

Se refiere a la conceptualización de las variables; esto significa pasarla de un concepto abstracto a un concepto cuantificable, para lo cual se deben definir sus dimensiones; esto es, el ámbito de valores que pueda tomar, a fin de facilitar la recolección, con un alto grado de precisión, de los datos necesarios. Se refiere a dimensión, como un componente significativo de una variable que posee relativa autonomía, esto es, un conjunto de cualidades más simples y por lo tanto más fáciles de medir. Las dimensiones de la variable constituyen un referente para establecer los indicadores. Operacionalizar la variable teórica, es someterla a contrastación empírica, y ello constituye uno de los abordajes metodológicos más frecuentes, ya que presenta las dimensiones y los indicadores de la variable teórica, como el resultado de un proceso que vincula la teoría con los hechos observables, mediante la explicación o no de procesos deductivos inherentes. La operacionalización de las variables, está estrechamente vinculada al tipo de técnica o metodología empleadas para la recolección de los datos. Estas deben ser compatibles con los objetivos de la investigación, a la vez que responden al enfoque empleado, al tipo de investigación que se realiza. Estas técnicas, en líneas generales, pueden ser cualitativas o cuantitativas.

2.11.1. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE: IMPLEMENTACIÓN DE UN MÓDULO DE SEGURIDAD EN EL DESARROLLO DE UN SISTEMA WEB

Tabla 4-2: Operacionalización de la variable independiente

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	CRITERIO DE MEDICIÓN	TÉCNICA	INSTRUMENTO	ESCALA
Implementación de un módulo de seguridad en el desarrollo de un sistema web	Técnicas, métodos, procedimientos que apoyan en la gestión y reporte de incidentes de forma automatizada y dinámica.	Disponibilidad Integridad Confidencialidad Autenticación Trazabilidad	Numero de riesgos controlados Número de incidentes atendidos	Cantidad	Observación y Experimentación	Software y Herramientas Informáticas Especializadas en la detección de Vulnerabilidades en un Ambiente de Pruebas	Modelos de Madurez
			Velocidad en el procesamiento de la información solicitada. Identificación a tiempo del número de errores en la información solicitada.	Cantidad	Observación y Experimentación		

Realizado por: Escobar, M. Alarcón, R, 2023.

2.11.2. OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE: MITIGAR Y CONTROLAR LA INTEGRIDAD DE LA INFORMACIÓN

Tabla 5-2: Operacionalización de la variable dependiente

VARIABLE	CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	CRITERIO DE MEDICIÓN	TÉCNICA	INSTRUMENTO	ESCALA
Mitigar y controlar la integridad de la información	Controlar, suavizar el mantenimiento exactitud y completitud de la información y sus métodos de proceso	Seguridad	Numero de posibles vulnerabilidades que puedan modificar la información original entregada.	Cantidad	Observación y Experimentación	Sniffers Software especializado en la modificación de la información impresa.	Modelos de Madurez
		Rendimiento	Numero de mecanismos incorporados para prevenir ataques a la integridad de la información.	Cantidad	Observación y Experimentación	Sistema Web Base de datos Código QR SSL Backup	

Realizado por: Escobar, M. Alarcón, R, 2023.

2.11.3. MATRIZ DE CONSISTENCIA

Tabla 6-2: Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTOS
¿Cómo se puede mejorar la integridad de la información en el área financiera del Instituto de Posgrado Educación Continua con	Desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información del área	H0: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, NO permitirá mitigar y controlar la integridad de la información del área financiera del instituto de posgrado y educación continua de	**Variable Independiente:** Implementación de un módulo de seguridad en el desarrollo de un sistema web.	Numero de riesgos controlados Número de incidentes atendidos Velocidad en el procesamiento de la información solicitada.	Observación y Experimentación	Software herramientas informáticas especializadas en la detección de vulnerabilidades en un ambiente de pruebas Sniffers

implementación de un sistema y módulo de seguridad?	financiera del instituto de posgrado de la ESPOCH	la Escuela Superior Politécnica de Chimborazo. H1: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, SI permitirá mitigar y controlar la integridad de la información del área financiera del instituto de posgrado y educación continua de la Escuela Superior Politécnica de Chimborazo.	**Variable Dependiente:** Mitigar y controlar la integridad de la información.	Identificación a tiempo del número de errores en la información solicitada. Numero de posibles vulnerabilidades que puedan modificar la información original entregada. Numero de mecanismos incorporados para prevenir ataques a la integridad de la información.		Software especializado en la modificación de la información impresa. Sistema Web Base de datos Código QR SSL Backps

Realizado por: Escobar, M. Alarcón, R, 2023

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

La Metodología de la investigación es la ciencia que nos enseña a dirigir determinado proceso de una manera eficiente y eficaz para alcanzar los resultados deseados y su principal objetivo es guiarnos por la estrategia a seguir en el proyecto.

Este capítulo de la investigación se basa en definir la metodología a utilizar basándonos claro está en los objetivos del proyecto, por lo que es necesario dar un paso atrás y observar el panorama general de lo que se quiere alcanzar antes de tomar decisiones metodológicas. Para aquello necesitamos tener claro si la investigación realizada es de carácter exploratorio o confirmatorio.

Tabla 1-3: Metodologías utilizadas en la investigación

METODOLOGIA	OBJETIVO	METODOS
Cualitativa	Exploratorio	Entrevistas Análisis de contenido Sin mediciones numéricas Descripciones Putos de vista de investigadores No tomando en general la prueba de la hipótesis como algo necesario
Cuantitativa	Confirmatorio	Encuestas Análisis estadísticos Utiliza la recolección de datos Medición de parámetros Obtención de frecuencias y estadígrafos para probar la hipótesis.

Realizado por: Escobar, M. Alarcón, R, 2023.

Con los conceptos claros de cada una de las metodologías, además de las metas, objetivo general y objetivos específicos del proyecto, en esta investigación utilizaremos el método cuantitativo, ya que siendo los objetivos específicos el desarrollo de un sistema web y módulo de seguridad, necesitamos verificar si la implementación de estas seguridades en el sistema reducen el número de vulnerabilidades que pudiesen afectar a la integridad de

la información. La manera en que se va a proceder es creando escenarios de pruebas, antes de la implementación de las seguridades y después de la implementación del módulo de seguridad, obteniendo como resultados datos numéricos que servirán para realizar los cálculos estadísticos y aprobar o negar la hipótesis planteada.

3.1. MÉTODOS DE INVESTIGACIÓN

Al momento de realizar una investigación es de suma importancia tener claro el método o los métodos que se pretenden utilizar para obtener los resultados requeridos. Los métodos de investigación son parámetros claves para la construcción de un conocimiento válido sobre un fenómeno particular, por lo que analizar en qué consiste cada uno de ellos, cuáles son sus principales características y de qué depende la elección de uno u otro resulta importantísimo y fundamental para todo investigador

Los métodos de investigación son un conjunto de técnicas que de manera coherente con la orientación de la investigación nos guía a la construcción de un conocimiento válido sobre un fenómeno en particular, por lo que conocer en qué consisten, cuáles son sus características y de qué depende la elección de uno u otro resulta fundamental para todo investigador. Es necesario tener claro la diferencia entre metodología de la investigación y métodos de investigación, ya que la primera se basa en la toma de decisiones coherentes, generales y abstractas por parte del investigador sobre cómo obtener determinados tipos de datos de la realidad que estudia, pero los cuales quedarán objetivamente reflejados en los modos en que se acercara a la realidad, en cambio los métodos de investigación son las técnicas, procesos o estrategias utilizadas en la recolección de datos y evidencias para el análisis, con el fin de descubrir información nueva y disponer de un mejor entendimiento sobre el tema de investigación.

Tabla 2-3: Métodos de Investigación

MÉTODO	DESCRIPCIÓN
Deductivo	Orientación de un enunciado general a lo específico
Inductivo	Se basa en la obtención de un enunciado general por medio de casos particulares.
Histórico	Método que va del pasado al presente para proyectarse al futuro

Descriptivo	Método que se orienta a determinar la realidad del objeto de estudio
Explicativo	Planteamiento de hipótesis explicativas así como diseño explicativo, se plantea preguntas de ¿cómo? ¿Por qué es así la realidad? ¿Cuáles son las causas?
Experimental	De lo ya descrito y explicado predecir de lo que ocurrirá en el futuro, como premisas se afirma que si se realiza cambios en una investigación sucederá tal cosa.

Realizado por: Escobar, M. Alarcón, R, 2023.

El método explicativo será el empleado en la presente investigación, el proceso a utilizar será observando pero principalmente evaluando los diferentes experimentos en escenarios actuales del departamento financiero del instituto de posgrado de la ESPOCH referente a cómo se maneja y registra la información de los cobros de los diferentes rubros para posteriormente realizar los mismos experimentos pero ya con la implementación de los elementos propuestos en esta investigación.

3.2. TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

Las técnicas utilizadas en la presente investigación son las estadísticas para el procesamiento de la información, las que se obtiene mediante los métodos empíricos; la observación, la encuesta, la entrevista y el experimento; y de esa manera llegar a las conclusiones que son altamente generalizables, estas técnicas son las que se aplican en la metodología experimental cuantitativa ya que se sustenta en el positivismo, neopositivismo y el pragmatismo.

3.3. PLANTEAMIENTO DE LA HIPÓTESIS

H0: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, NO permitirá mitigar y controlar la integridad de la información del área financiera del instituto de posgrado y educación continua de la Escuela Superior Politécnica de Chimborazo.

H1: El desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, SI permitirá mitigar y controlar la integridad de la información del área financiera del Instituto de Posgrado y Educación Continua de la Escuela Superior Politécnica de Chimborazo.

3.4. HIPÓTESIS ESPECÍFICAS

- La elaboración del sustento teórico y conceptual fundamenta la investigación.
- La implementación de un sistema web permite mejorar la integridad de la información de los procesos financieros del Instituto de Posgrado.
- La implementación de un módulo de seguridad basado en la norma ISO 27000 en el sistema web financiero si reducirá las vulnerabilidades a la integridad de la información.

3.5. IDENTIFICACIÓN DE LAS VARIABLES

Variable Independiente: Implementación de un módulo de seguridad en el desarrollo de un sistema web.

Variable Dependiente: Mitigar y controlar la integridad de la información

3.6. POBLACIÓN Y MUESTRA

3.6.1. Población

La población estadística es un conjunto, este puede ser de individuos, animales, fenómenos u eventos a considerar en un estudio, experimento o de interés en una investigación, en este caso nuestra población son los ataques informáticos que afectan a la integridad de la información en forma general.

3.6.2. Selección de la muestra

La muestra es una porción que se extrae de la población estadística para realizar un determinado estudio, en la presente investigación como muestra tomaremos a las principales vulnerabilidades que afectan a la integridad de la información en el área financiera del Instituto de Posgrado de la ESPOCH por ejemplo:

- La modificación de la información no autorizada
- Fallas de hardware o software en las computadoras que puede ocasionar sobrescribir parcial o totalmente los datos almacenados.
- Duplicación de datos en forma desorganizada por parte de cada persona que los manipula.
- No contar con una secuencia de la información
- Virus, ataques informáticos.

Las fases para analizar la muestra en estudio en este caso las principales vulnerabilidades que afectan a la integridad de la información son:

1) Implementación de escenarios experimentales
2) Generación de ataques informáticos a los escenarios propuestos
3) Análisis y recolección de datos de los procesos realizados en los escenarios implementados.
4) Aplicación del sistema informático y módulo de seguridad.
5) Validación de resultados.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

Dentro de este capítulo se estudiará los resultados que se obtengan al plantear escenarios de pruebas seguros e inseguros referente a la implementación del sistema web desarrollado en el área financiera del IPEC, también se analizará el efecto al implementar un módulo de seguridad en el mismo sistema web mencionado anteriormente y por último se evaluará si los métodos propuestos en el módulo de seguridad planteado son los correctos o no para ayudar a comprobar la integridad de la información. La información que se obtenga de estos análisis será utilizada como muestra dentro de la estadística descriptiva para realizar la comprobación de la hipótesis mediante la prueba chi-cuadrado.

4.1. PRESENTACIÓN DE ESCENARIOS

4.1.1. Escenario de prueba 1: Implementación de un sistema web en el departamento financiero del IPEC.

Para medir las ventajas o desventajas de la implementación del sistema web en el área financiera del IPEC se tomaron en cuenta varios parámetros entre los principales están: reducción de costos, productividad, disponibilidad, confiabilidad, rendimiento, realizando un análisis individual de cada uno de estos puntos a la hora de obtener los resultados, para después plasmarlos en una tabla de barras.

Reducción de costos: con la adquisición de equipos informáticos necesarios para la implementación de los sistemas web se puede aumentar el servicio a los usuarios finales (clientes) incrementando las ganancias dependiendo el tipo de producto que la empresa otorgue. Ejemplo en el área financiera del IPEC se puede atender con la utilización del sistema web a 5 personas en una hora, sin el sistema web se atiende a 2 personas por hora. (Se refiere a la atención de revisar historial de pagos por diferentes rubros individualmente por cada estudiante)

Productividad: unas de las principales ventajas de la productividad en la automatización de los procesos son: el ahorro de tiempo, acceso a la información con rapidez, simplificación de procesos, trabajo en equipo desde cualquier lugar, oportunidad de crecimiento. Ejemplo en el área financiera del IPEC para encontrar documentación de un estudiante se tiene que buscar manualmente en los repositorios físicos ocasionando una gran demora al realizar este proceso, con el sistema web se podrá encontrar la información

del estudiante con mucha rapidez ya que solo sería cuestión de ingresar el nombre o cedula del estudiante arrojando todo lo referente al historial de pagos del maestrante.

Disponibilidad: es tan importante en la automatización de procesos ya que no necesariamente necesitamos encontrarnos en la oficina para disponer de la información si no que podemos almacenar de varias maneras los datos como en la nube, discos de almacenamiento externos o lo más óptimo acceder al sistema informático con sus respectivas credenciales.

Confiabilidad: es la principal característica de la automatización de procesos, permite manejar tareas complejas de forma dinámica e inteligente, basándose en parámetros predefinidos, asegurándonos que los trabajos no se ejecuten fuera de secuencia, evitándonos además que se genere confusión, caos y usuarios descontentos.

Rendimiento: un software ayuda a mejorar el rendimiento de los procesos en toda compañía ya que la información se maneja de forma más rápida y menos costosa.

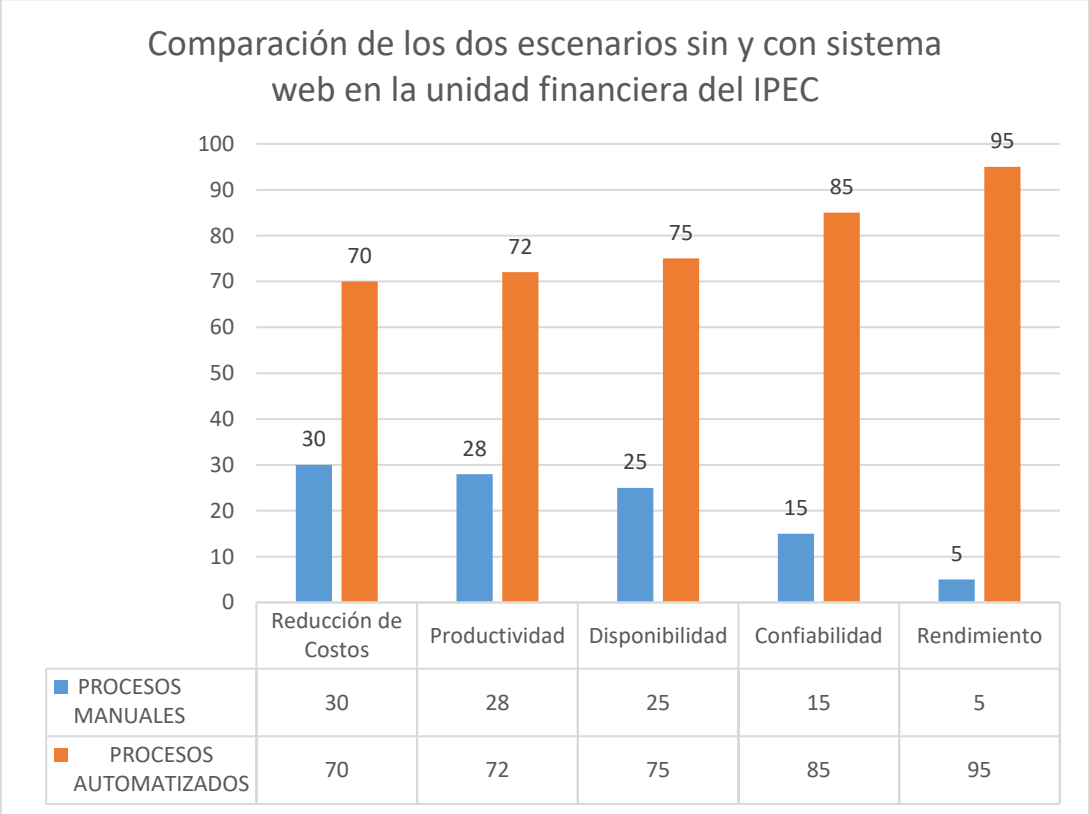


Gráfico 1-4: Comparación de escenarios con y sin sistema web
Realizado por: *Escobar, M. Alarcón R. 2023*

Análisis de los resultados de los principales parámetros de medición al implementar un sistema web en el área financiera del IPEC.

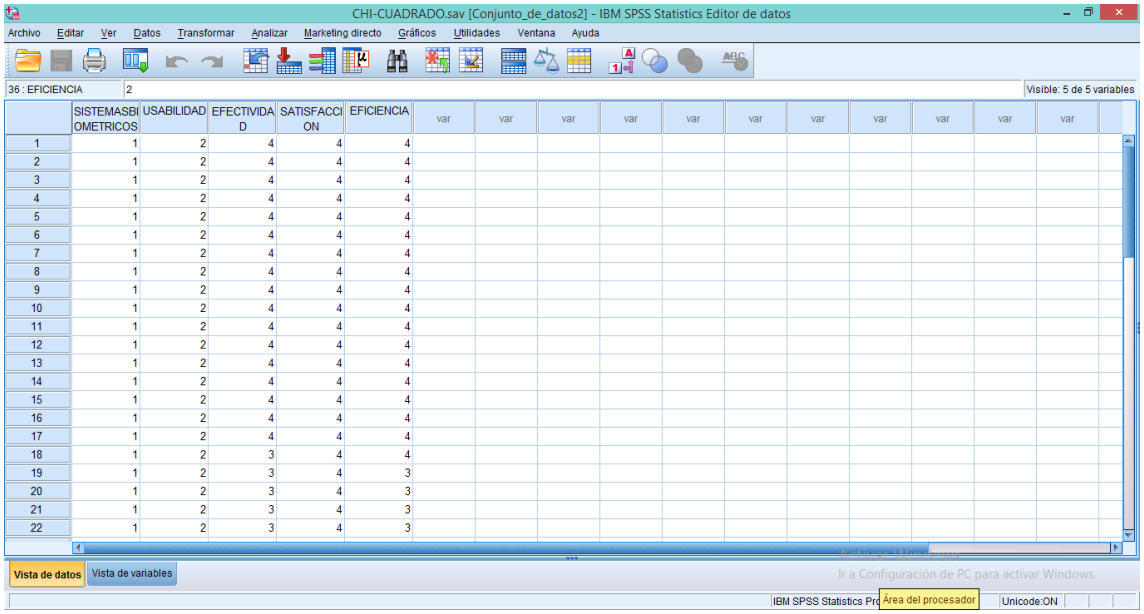


Gráfico 2-4: Vista de variables
Realizado por: *Escobar, M. Alarcón R. 2023*

Tabla 1-4: Resultados de la implementación de escenario con sistema web

	Reducción de costos	Productividad	Disponibilidad	Confiabilidad	Rendimiento
Con sistema web	70	72	75	85	95
Sin sistema web	30	28	25	15	5
RESULTADOS	40%	44%	50%	70%	90%

Realizado por: Escobar, M. Alarcón, R, 2023.

4.1.2. Interpretación de resultados del escenario 1:

Como se puede observar en la tabla existe una mejoría en todos los parámetros analizados al implementar un sistema web en el área financiera del IPEC como es la reducción de costos en un 40%, mejora la productividad en un 44%, aumenta la disponibilidad de la información en un 50%, la confiabilidad de la información sube a un 70% y no se diga del rendimiento que alcanza un 90%.

Análisis e interpretación de resultados:

En este escenario se reduce sustancialmente las posibilidades de sufrir u ataque informático ya que la arquitectura de las aplicaciones es de tres capas en mi ejemplo el sistema de evaluación al docente del IPEC mantiene dicha arquitectura bien definida.

4.1.3. COMPROBACIÓN DE LA HIPÓTESIS ESCENARIO 1

Prueba de hipótesis

La hipótesis que se plantea en el primer escenario es: *"*¿La implementación de un sistema informático en el área financiera del IPEC si influye en una mejor atención a los usuarios de posgrado?*"*.

Para realizar este proceso se utiliza de la estadística inferencial, se asigna los siguientes valores a la variable independiente X, para la comprobación de la hipótesis de investigación:

X = Sistema Informático
X_1 = Mejora la atención a los usuarios
X_2 = No mejora la atención a los usuarios

Para la comprobación estadística de la hipótesis se utiliza Chi-cuadrado (X^2), que es una prueba de hipótesis no paramétrica que compara la distribución observada de los datos con una distribución esperada, estableciendo la hipótesis de investigación *Hi* y la hipótesis nula *Ho* a ser consideradas.

- **Hi:** La implementación de un sistema informático en el área financiera del IPEC SI influye en una mejor atención a los usuarios de posgrado.
- **Ho:** La implementación de un sistema informático en el área financiera del IPEC NO influye en una mejor atención a los usuarios de posgrado.

Mediante encuesta realizada a usuarios comunes en las que se les pregunto: ¿Influye en una mejor atención a los usuarios de posgrado la implementación de un sistema informático en el área financiera?

Tabla 2-4: Parámetros evaluados para comprobar el escenario de prueba

	Rendimiento	Disponibilidad	Atención	Total
Si influye	23	27	10	60
No influye	7	10	20	37
Total	30	37	30	97

Realizado por: Escobar, M. Alarcón, R, 2023.

Cuando se presenta un solo criterio de clasificación dividido en varias categorías el cálculo de las frecuencias teóricas o esperadas es sencillo:

Fe = N/K

N= número de eventos

K=número de oportunidades

En este caso todos tienen la misma oportunidad

Cuando hay dos criterios de clasificación como en nuestro caso (cuadros de doble entrada), las frecuencias teóricas de cada casilla son iguales al producto de las sumas marginales dividido por el número total de sujetos. En el caso de dos categorías con dos niveles de clasificación (podrían ser más) tendríamos:

Aplicación de chi-cuadrado a las frecuencias esperadas calculadas, mediante la fórmula:

- $X^2 = \sum \frac{(FO-FE)2}{FE}$

En dónde:

- *FO:* Frecuencia observada por celda
- *FE:* Frecuencia esperada por celda

$$Ft \implies 23: \frac{30 * 60}{97} = 18{,}55$$

$$Ft \implies 7: \frac{30 * 37}{97} = 11{,}44$$

$$Ft \implies 27: \frac{37 * 60}{97} = 22{,}88$$

$$Ft \implies 10: \frac{37 * 37}{97} = 14{,}11$$

$$Ft \implies 10: \frac{30 * 60}{97} = 18{,}55$$

$$Ft \implies 20: \frac{30 * 37}{97} = 11{,}44$$

Grados de libertad V= (Nº filas-1)*(Nº columnas -1)

V= (2-1)*(3-1)

V=2

$$X^2 = \sum \frac{(f-ft)^2}{ft} = \frac{(23-18{,}55)^2}{18{,}55} + \frac{(7-11{,}44)^2}{11{,}44} + \frac{(27-22{,}88)^2}{22{,}88} + \frac{(10-14{,}11)^2}{14{,}11} + \frac{(10-18{,}55)^2}{18{,}55} + \frac{(20-11{,}44)}{11{,}44}$$

$$X^2 = \sum \frac{(f-ft)^2}{ft} = 1{,}06 + 1{,}72 + 0{,}73 + 1{,}19 + 3{,}94 + 6{,}40 = \mathbf{15{,}04}$$

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Figura 1-4: Percentiles de la Distribución X^2
Fuente: (Statistical Discovery, 2023)

Los grados de libertad utilizados es 2 y el margen de error o nivel de confianza utilizado es 0,05 entonces chi-cuadrado tabla es: $X^2 tabla = 5{,}9915$ y chi-cuadrado calculado es $X^2 calculado = 15{,}04$

$$X^2 calculado > X^2 tabla \implies se\ rechaza\ la\ Ho(hipotesis\ nula)$$

$$X^2 calculado < X^2 tabla \implies se\ rechaza\ la\ Hi(hipotesis\ alternativa)$$

$$X^2 calculado\ 15{,}04 > X^2 tabla\ 5{,}9915 \implies se\ acepta\ Hi(hipotesis\ alternativa)$$

Observando los resultados se puede evidenciar que el chi-cuadrado calculado es mayor que chi-cuadrado tabla, por lo cual se acepta la hipótesis alternativa (Hi) y se rechaza la hipótesis nula (Ho), Es decir **"**La implementación de un sistema informático en el área financiera del IPEC SI influye en una mejor atención a los usuarios de posgrado.**"**

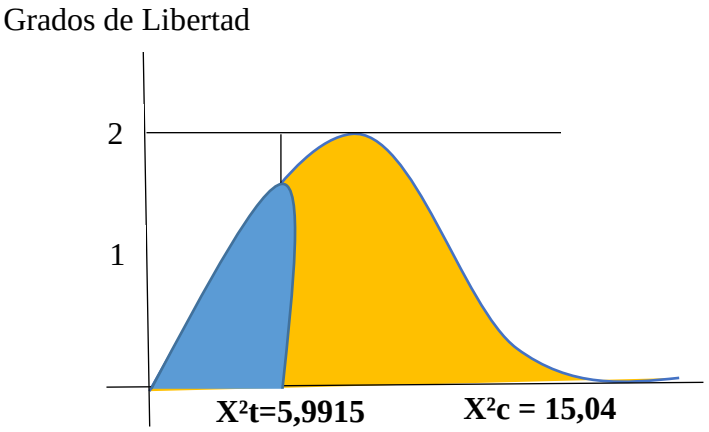


Figura 2-4: Distribución X^2 con 2 grados de libertad
Realizado por: Escobar, M. Alarcón R. 2023

4.1.4. Escenario de prueba 2: Implementación de un módulo de seguridad basado en la norma ISO 27000 en el sistema web del departamento financiero del IPEC.

Para realizar la implementación de un módulo de seguridad en sistemas web tomaremos como referencia algunas normas ya establecidas en la ISO 270000 y 27001.

Figura 3-4: Metodología de evaluación de riesgos
Fuente: (Normas ISO, 2023)

Control de acceso a sistemas y aplicaciones: para garantizar el acceso y verificar la identificación de personas solo autorizadas a la información en el sistema web se tiene que implementar contraseñas fuertes, accesos biométricos, notificaciones de ingreso al sistema al correo electrónico o dispositivos móviles entre los principales controles.

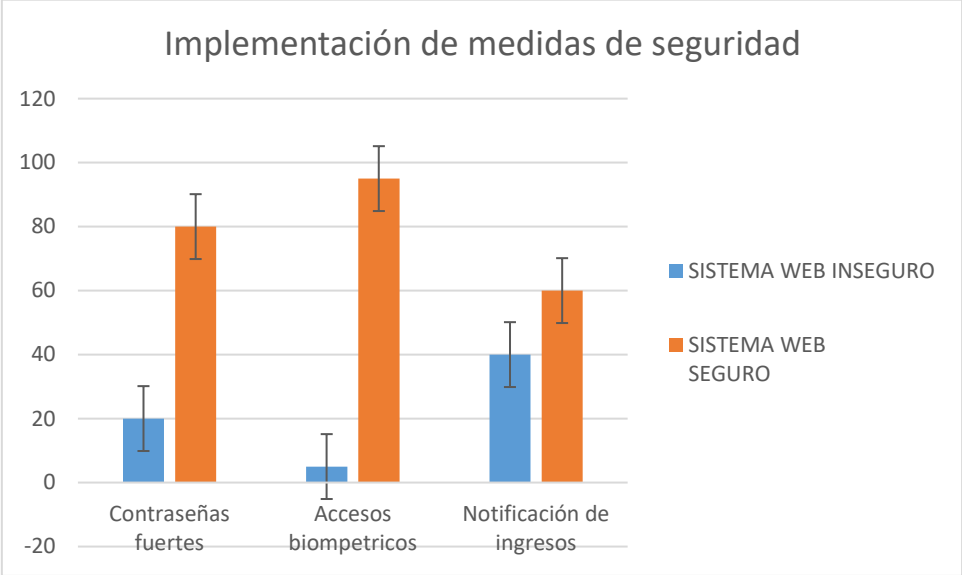


Gráfico 3-4: Implementación de medidas de seguridad
Realizado por: *Escobar, M. Alarcón R. 2023*

La integridad de los datos: es una función relacionada con la seguridad de forma que un servicio de integridad tiene la función de mantener la información exactamente como fue ingresada en operaciones tales como la captura de datos, el almacenamiento, la recuperación, la actualización o la transferencia, dentro de las principales acciones a tomar se encuentran:

- Cifrado de datos, que bloquea los datos por cifrado
- Copia de seguridad de datos, que almacena una copia de datos en una ubicación alternativa Controles de acceso, incluida la asignación de privilegios de lectura / escritura.
- Validación de entrada, para evitar la entrada incorrecta de datos.
- Validación de datos, para certificar transmisiones no corrompidas.

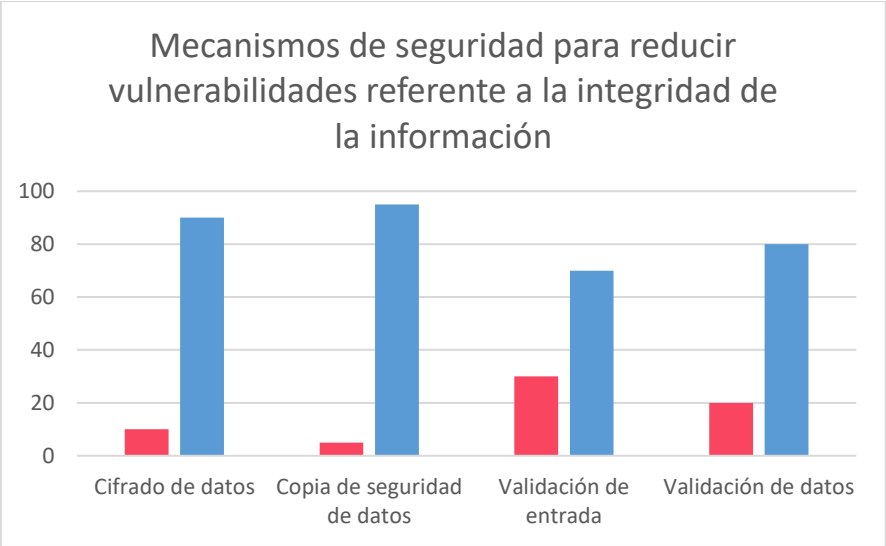


Gráfico 4-1: Mecanismos de seguridad para reducir las vulnerabilidades
Realizado por: *Escobar, M. Alarcón R. 2023*

Códigos QR.- Los códigos QR, acronímico de Quick Response o respuesta inmediata, son pequeños códigos de barras y se utilizan para varios servicios como el de proporcionar información almacenada o redirigiéndonos a un sitio web y también el de iniciar una acción específica en un dispositivo diferente de manera automática. Es importante contar con un mecanismo de seguridad que nos indique que los documentos obtenidos de un sistema web son íntegros y es lo que nos ofrece el código QR ya que no tiene fallas de seguridad y no se puede piratear como tal, pero sí es posible reemplazar un código QR por otro o crear un código QR que redirija a una URL maliciosa, a un sitio de phishing donde los usuarios desprevenidos puedan revelar información personal o financiera o que contenga malware personalizado que luego permita filtrar datos del dispositivo móvil mientras se escanea.

Figura 4-1: Escaneo de códigos QR
Fuente: (Pascual, J. 2015)

El phishing es uno de los métodos de piratería de datos confidenciales más comunes utilizados por los cyber delincuentes y los códigos QR también se utilizan en el phishing.

4.1.5. COMPROBACIÓN DE LA HIPÓTESIS ESCENARIO 2

Prueba de hipótesis.- en este segundo escenario la hipótesis que se plantea es en base a algunos de los mecanismos de seguridad implementados en el sistema web que dicta la norma ISO 27000 y 27001: *"*¿La implementación de un módulo de seguridad en el sistema informático del área financiera del IPEC si reducirá las vulnerabilidades referente a la integridad de la información?*"*.

Para realizar este proceso se utiliza de la estadística inferencial, se asigna los siguientes valores a la variable independiente X, para la comprobación de la hipótesis de investigación:

X = Sistema Informático
X_1 = Mejora la atención a los usuarios
X_2 = No mejora la atención a los usuarios

Para la comprobación estadística de la hipótesis se utiliza Chi-cuadrado (X^2), que es una prueba de hipótesis no paramétrica que compara la distribución observada de los datos con una distribución esperada, estableciendo la hipótesis de investigación *Hi* y la hipótesis nula *Ho* a ser consideradas.

- **Hi:** La implementación de un módulo de seguridad en el sistema informático del área financiera del IPEC SI reducirá las vulnerabilidades referente a la integridad de la información.
- **Ho:** La implementación de un módulo de seguridad en el sistema informático del área financiera del IPEC NO reducirá las vulnerabilidades referente a la integridad de la información.

Mediante encuesta realizada a Ingenieros en sistemas que administran sistemas informáticos en las que se les pregunto si: ¿La implementación de mecanismos de seguridad tales como la utilización de contraseñas fuertes, utilización de accesos biométricos a sistemas web, avisos de ingreso al sistema a dispositivos personales, copias de seguridad de datos, utilización de códigos de barras en los documentos emitidos por el

sistema informático ayudarán a reducir las vulnerabilidades a la integridad de la información?

Tabla 3-4: Encuesta realizada a profesionales de sistemas de la información

	Logeos Biométricos	Respaldo de datos	Cifrado de datos	Utilización del código QR	TOTAL
Si reducen las vulnerabilidades a la integridad de la información	45	20	25	31	121
No reducen las vulnerabilidades a la integridad de la información	5	10	15	29	59
Total	50	30	40	60	180

Realizado por: Escobar, M. Alarcón, R, 2023.

Cuando se presenta un solo criterio de clasificación dividido en varias categorías el cálculo de las frecuencias teóricas o esperadas es sencillo:

Fe = N/K

N= número de eventos

K=número de oportunidades

En este caso todos tienen la misma oportunidad

Cuando hay dos criterios de clasificación como en nuestro caso (cuadros de doble entrada), las frecuencias teóricas de cada casilla son iguales al producto de las sumas marginales dividido por el número total de sujetos. En el caso de dos categorías con dos niveles de clasificación (podrían ser más) tendríamos:

Aplicación de chi-cuadrado a las frecuencias esperadas calculadas, mediante la fórmula:

- $X^2 = \sum \frac{(FO-FE)2}{FE}$

En dónde:

- *FO:* Frecuencia observada por celda
- *FE:* Frecuencia esperada por celda

$$Ft \implies 45: \frac{50 * 121}{180} = 33.61$$

$$Ft \implies 5: \frac{50 * 59}{180} = 16.38$$

$$Ft \implies 20: \frac{30 * 121}{180} = 20.16$$

$$Ft \implies 10: \frac{30 * 59}{180} = 9.83$$

$$Ft \implies 25: \frac{40 * 121}{180} = 26.88$$

$$Ft \implies 15: \frac{40 * 59}{180} = 13.11$$

$$Ft \implies 31: \frac{60 * 121}{180} = 40.33$$

$$Ft \implies 29: \frac{60 * 59}{180} = 19.66$$

Grados de libertad V= (Nº filas-1)*(Nº columnas -1)

V= (2-1)*(4-1)

V=3

$$X^2 = \sum \frac{(f - ft)^2}{ft}$$

$$= \frac{(45 - 33.61)^2}{33.61} + \frac{(5 - 16.38)^2}{16.38} + \frac{(20 - 20.16)^2}{20.16} + \frac{(10 - 9.38)^2}{9.38}$$
$$+ \frac{(25 - 26.88)^2}{26.88} + \frac{(15 - 13.11)^2}{13.11} + \frac{(31 - 40.33)^2}{40.33} + \frac{(29 - 19.66)^2}{19.66}$$

$X^2 = \sum \frac{(f-ft)^2}{ft} = 3.85 + 7.90$+0,001+0.04+0.13+0.27+2.15+4.43= **18.77**

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Figura 5-4: Percentiles de la Distribución X^2
Fuente: ***(Statistical Discovery, 2023)***

Los grados de libertad utilizados es 3 y el margen de error o nivel de confianza utilizado es 0,05 entonces chi-cuadrado tabla es: $X^2 tabla = 7{,}81$ y chi-cuadrado calculado es $X^2 calculado = 18{,}77$

$$X^2 calculado > X^2 tabla \implies se\ rechaza\ la\ Ho(hipotesis\ nula)$$

$$X^2 calculado < X^2 tabla \implies se\ rechaza\ la\ Hi(hipotesis\ alternativa)$$

$$X^2 calculado\ 18{,}77 > X^2 tabla\ 7{,}81 \implies se\ acepta\ Hi(hipotesis\ alternativa)$$

Observando los resultados se puede evidenciar que el chi-cuadrado calculado es mayor que chi-cuadrado tabla, por lo cual se acepta la hipótesis alternativa (Hi) y se rechaza la hipótesis nula (Ho), Es decir **"**La implementación de un módulo de seguridad en el sistema informático del área financiera del IPEC SI reducirá las vulnerabilidades referente a la integridad de la información.**"**

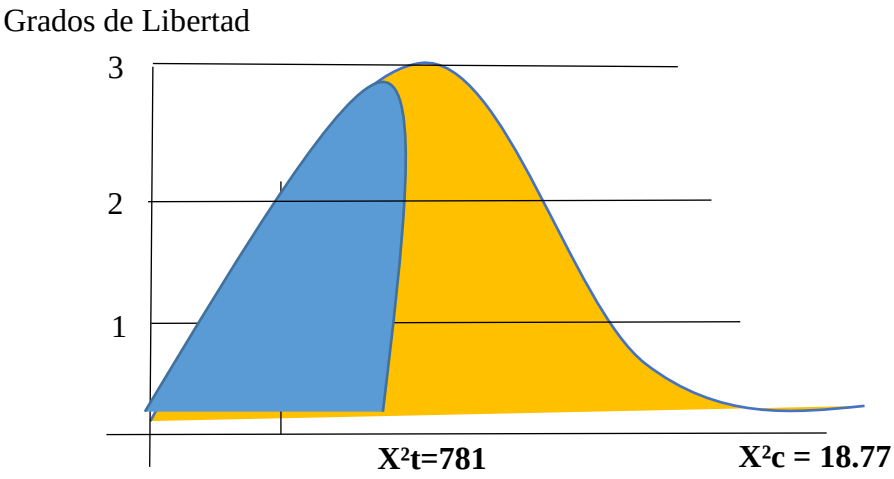


Figura 6-4: Distribución X^2 con 2 grados de libertad
Realizado por: Escobar, M. Alarcón R. 2023

CAPÍTULO V

5. PROPUESTA

5.2. Determinación de la propuesta

El departamento financiero del IPEC, no cuenta con un sistema automatizado propio que almacene el historial detallado de la información referente a los pagos que realizan los estudiantes de los diferentes programas de posgrado, razón por la cual la propuesta de este proyecto de investigación es instalar un sistema informático con sus debidas seguridades basados en la norma ISO, que sirva como una herramienta para almacenar, organizar, acelerar los procesos financieros que en este departamento se realizan.

5.3. Descripción del sistema Informático

El sistema informático de cobros del Instituto de Posgrado y Educación Continua desde ahora denominado SICOIPEC está desarrollado con los siguientes componentes:

5.3.1. Lenguaje de programación

Java que es uno de los lenguajes más populares y utilizados a nivel mundial aquí algunas de sus principales características:

Tabla 1-5: Características del lenguaje de Programación Java

CARACTERÍSTICAS	DESCRIPCIÓN
Multiplataforma	Funciona en cualquier sistema operativo
Orientación a objetos	Permite que el código sea reutilizable
Código robusto	Comprobación temprana de todos los posibles errores y excepciones.
Versatilidad	Utilizado en millones de aplicaciones, en todo tipo de sistemas operativos y dispositivos.
Sencillo y fácil de aprender	Facilidad de uso, fácil de escribir, compilar, depurar y aprender, menos complejo que los lenguajes como C y C++
Aplicaciones accesibles	Tecnología para aplicaciones web dinámicas corren en todos los navegadores posibles.
Aplicaciones distribuidas	Mediante la función de red integrada la computación distribuida es factible y fácil de utilizar logrando así disminuir la latencia en determinadas aplicaciones.

Lenguaje seguro	Las brechas de seguridad de las aplicaciones Java son menores que las de otros lenguajes de programación.
APIS	Las APIs consisten en un conjunto de librerías de código compilado listas para que sean usadas por todos los desarrolladores o programadores, dispone de un rico conjunto de API.
Herramientas poderosas	IDE's (Integrated Development Environment) como Eclipse y Netbeans facilitan en gran manera el desarrollo de las aplicaciones.
Es gratuito	Gran ayuda para los desarrolladores

Realizado por: Escobar, M. Alarcón, R, 2023.

Interfaz de Netbeans IDE utilizado para el desarrollo del sistema

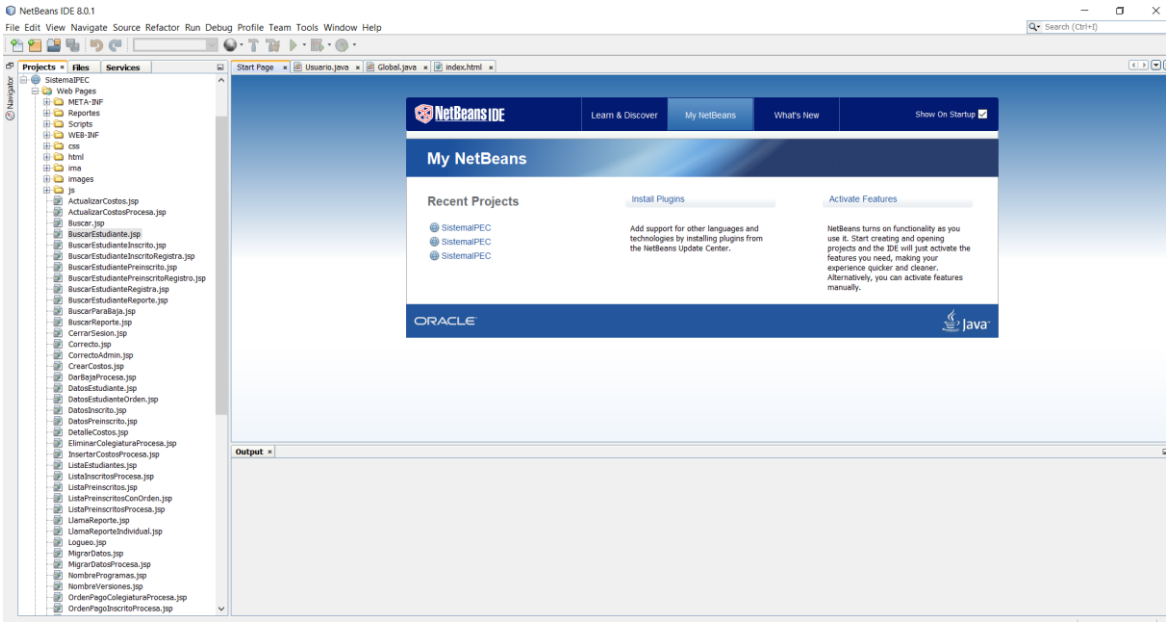


Figura 1-5: Interfaz del IDE de desarrollo Netbeans
Realizado por: *Escobar, M. Alarcón R. 2023*

5.3.2. Motor de base de datos Postgresql

Es un gestor que trabaja con bases de datos relacionales y que está orientado a objetos. Se trata de un programa de código abierto u *open source*, es decir, no está bajo el control de ninguna compañía particular,

Tabla 2-5: Características del motor de base de datos Postgresql

CARACTERÍSTICAS	DESCRIPCIÓN
Instalación ilimitada y gratuita:	Se puede instalar en cualquier equipo que queramos, independientemente de la plataforma y la arquitectura que utilicemos Unix, Linux y Windows, en 32 y 64 bits es decir multiplataforma.
Gran escalabilidad:	Capaz de configurarse y ajustarse al número de CPU y a la cantidad de memoria disponible de forma óptima logrando una mayor cantidad de peticiones simultáneas a la base de datos de forma correcta.
Orientado a objetos	Gestor de bases de datos relacionales, soporta diferentes tipos de datos y está orientado a objetos
Código Abierto	Es de código abierto, es decir, cuentan con una comunidad de desarrolladores que implementan mejoras o resuelven errores de forma altruista.

Realizado por: Escobar, M. Alarcón, R, 2023.

Interfaz de Postgresql motor de bases utilizado en el desarrollo del sistema

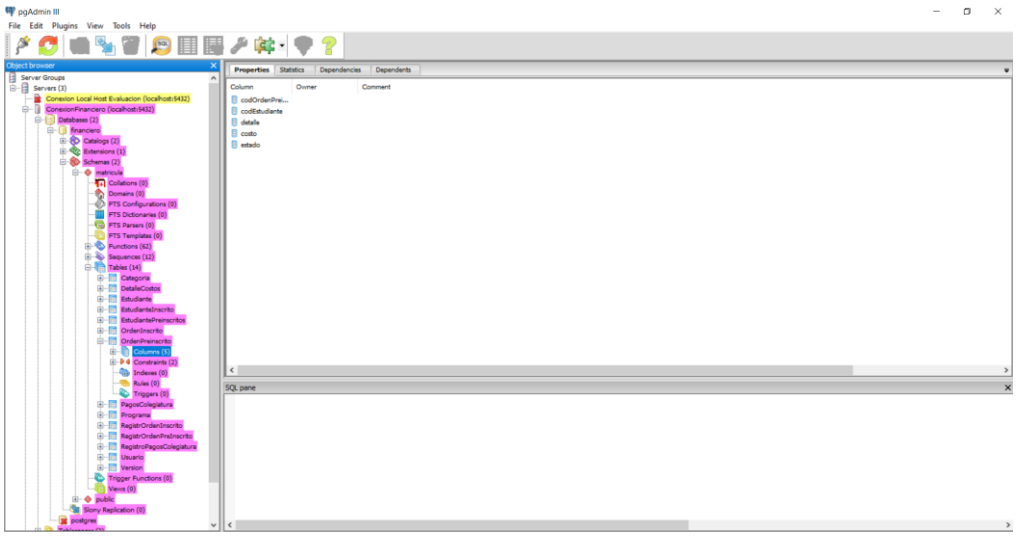


Figura 2-5: Interfaz del Motor de base de datos Postgresql
Realizado por: *Escobar, M. Alarcón R. 2023*

5.3.3. Servidor de Aplicaciones Apache Tomcat

Es un servidor de aplicaciones completo de código abierto, es una opción mucho mejor para sitios web dinámicos, líder indiscutible cuando se trata de sitios basados completamente en JSP utilizado en el desarrollo del sistema financiero de posgrado.

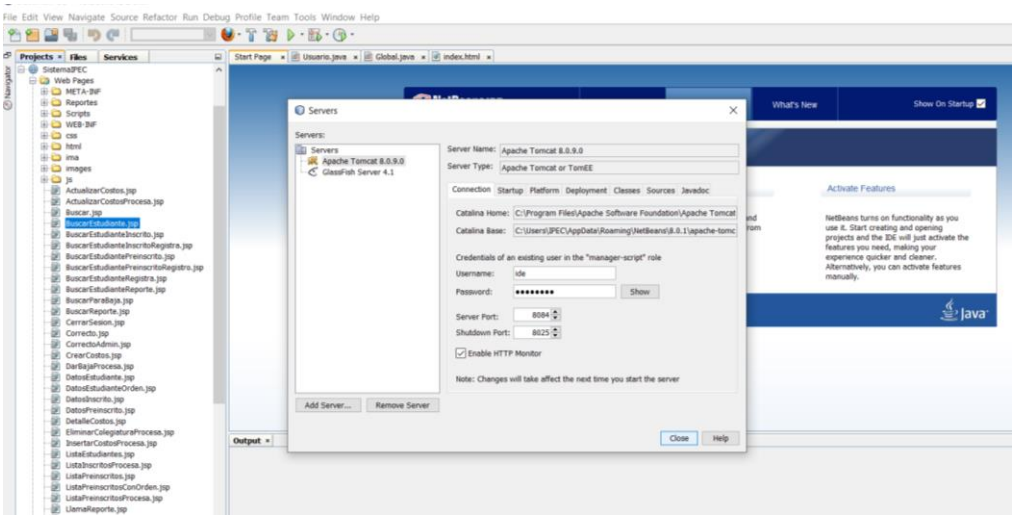


Figura 3-5: Servidor de aplicaciones Apache Tomcat
Realizado por: *Escobar, M. Alarcón R. 2023*

5.4. FUNCIONAMIENTO DEL SISTEMA FINANCIERO

Un sistema informático dinámico que se utiliza en la vida diaria en cualquier empresa debe mantener una estructura funcional segura dentro de todos sus procesos:

- ✓ Recopilación de datos
- ✓ Depuración de los datos
- ✓ Almacenamiento de toda la información ingresada
- ✓ Procesamiento de la información
- ✓ Entrega y distribución de la información

Y mucho más si se trata de un sistema que procesa información financiera los cuales son más susceptibles a los ataques informáticos, por todas estas razones el SICOIPEC se lo divido en dos interfaces graficas con sus propios menús la una para la administración y la otra específicamente para la emisión de las órdenes de pago sin que ninguna de las interfaces estén entrelazadas entre sí.

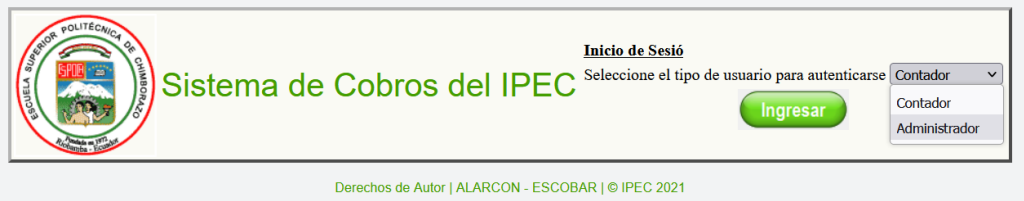


Figura 4-5: Interfaz de inicio de sesión del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Para proteger la privacidad del acceso al sistema por parte del usuario contador quien es el que realizará las actividades de registrar los cobros de los diferentes rubros de todos los programas de Posgrado, dentro de la programación se ha incorporado el cifrado de la clave misma que es ingresada por el propio usuario una vez que el administrador le asigna los roles de contador siempre y cuando cumpla también con otra seguridad implantada que es el estado del usuario que debe ser de ACTIVO.

Figura 5-1: Interfaz cifrado de claves del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

5.4.1. MENÚ ADMINISTRADOR

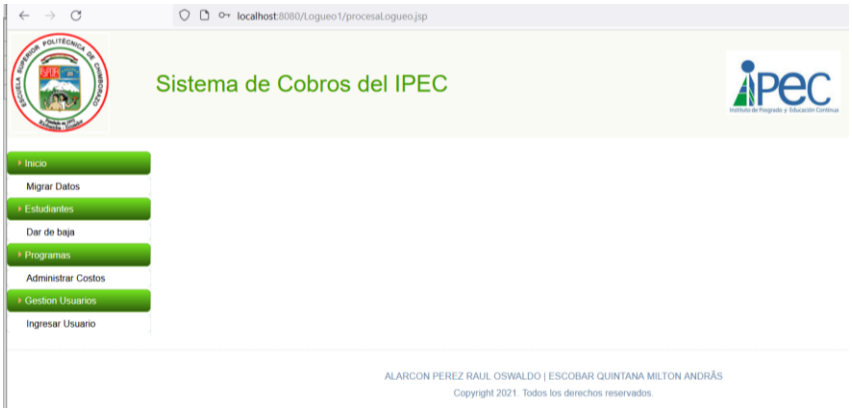


Figura 6-5: Interfaz del menú del administrador del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

La interfaz del administrador cuenta con un menú formado por Inicio, Migrar Datos, Dar de baja, Programas, Administrar Costos, Gestión de Usuarios.

Migrar Datos: esta opción sirve para listar todos los programas que se han creado en el sistema académico del IPEC https://sisipec.espoch.edu.ec:

Figura 7-5: Interfaz de la implementación de web service del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

los mismos que son migrados al SICOIPEC mediante web services, es decir cuando se crea una maestría en el sistema académico de posgrado para su inicio se sube el nombre completo del programa resoluciones, además que registra estudiantes pre inscritos, en resumen se genera todo lo concerniente a información referente al inicio de un programa de maestría, la cual es migrada al sistema de cobros con toda la información que en este sistema se encuentra almacenada hasta el momento de transferir, manteniendo la integridad de la información que es una parte fundamental de esta investigación, evitándonos así tener que volver a ingresar información en el SICOIPEC, además de correr el riesgo de que se ingrese la información de forma diferente a la original ocasionando un total desfase en la información además de duplicidad de la misma, es decir que después de haber realizado la migración del programa en una primera parte y existen estudiantes nuevos que se pre inscriben en el sistema académico del IPEC para ingresar a un programa de maestría se vuelve a realizar esta acción de migración y automáticamente se actualizara la información en el sistema de cobros sin duplicarse.

Sistema Académico del IPEC en donde se crea todos los nuevos programas de maestrías, se realizan los procesos de matriculación, ingreso de notas, procesos de titulación, etc.

Figura 8-5: Interfaz del sistema académico de posgrado
Realizado por: *Escobar, M. Alarcón R. 2023*

Interfaz del sistema de cobros del IPEC previo a la migración de la información.

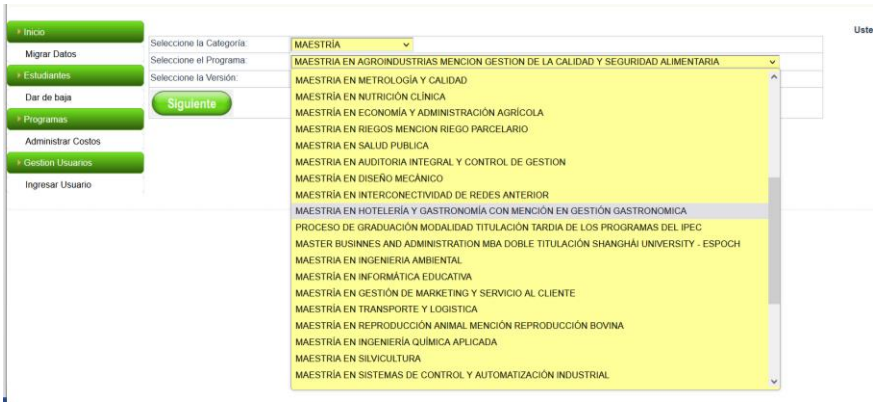


Figura 9-5: Interfaz del consumo de los servicios web en el sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Interfaz del sistema de cobros del IPEC con toda la información a migrar, en esta parte del proceso previo a la migración de la información se puede desmarcar a estudiantes que se pre inscribieron por equivocación o que definitivamente no desean seguir en el proceso de ingreso a la maestría.

Figura 10-5: Evidencias de la migración exitosa de datos al sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Dar de Baja: una vez que los estudiantes son migrados y realizan los respectivos procesos de admisión y matricula y cuenta con los justificativos adecuados en la opción dar de baja se procede a buscar al maestrante ya sea por cedula o nombres y se procede a eliminar de la base de datos del sistema.

Figura 11-5: Interfaz para dar de baja a los usuarios del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

5.4.2. Administración de Costos

En esta opción se ingresa los valores por concepto de examen de admisión, inscripción, matrícula y colegiatura es decir todos los valores que el estudiante paga para cruzar la maestría. Estos valores ingresados aquí por el administrador pueden ser editados siempre y cuando ningún estudiante haya realizado el pago.

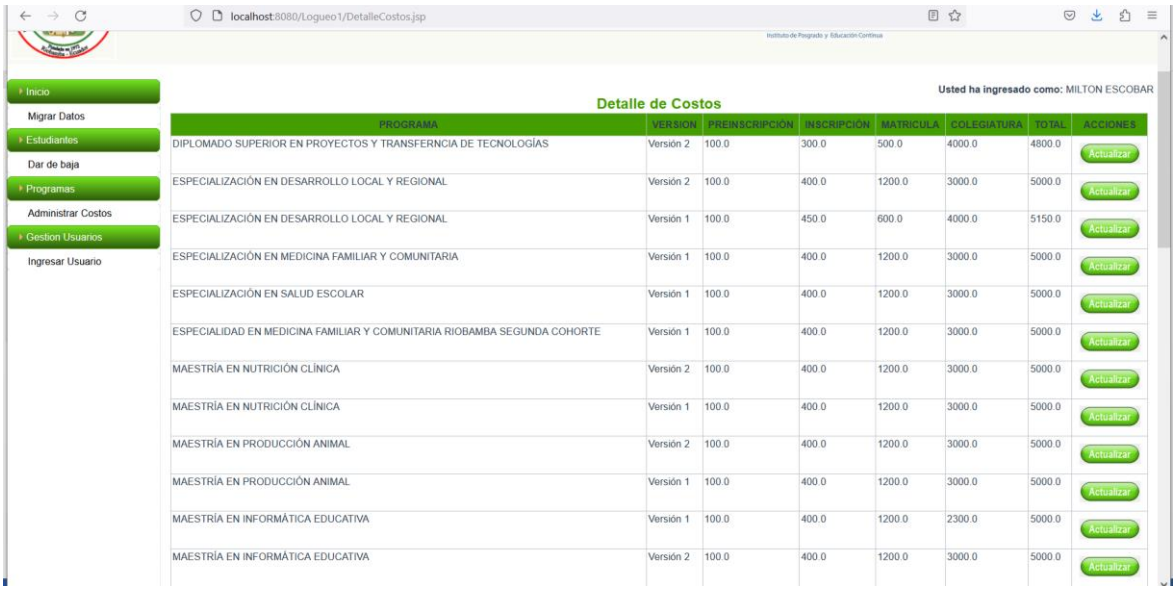


Figura 12-5: Interfaz de los valores ingresados del sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Figura 13-5: Interfaz de generación de pagos en el sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

5.4.3. Gestión de Usuarios

Como su nombre lo indica sirve para ingresar a los usuarios del sistema con el rol de contador siendo esta información datos personales, así como el nombre de usuario y clave que es la cedula de identidad que se asigna automáticamente en los dos campos y por último el estado ACTIVO o NO ACTIVO. Las credenciales de acceso aquí asignadas son modificadas por el usuario contador sin que el administrador tenga conocimiento de este proceso.

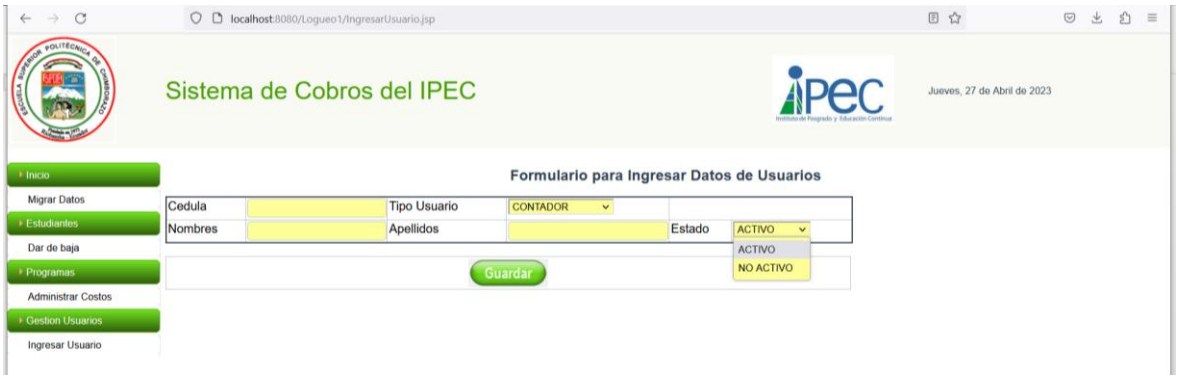


Figura 14-5: Interfaz de ingreso de usuarios al sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

5.4.4. Menú Usuario Contador

En este menú del lado de la persona que va a realizar las ordenes de cobro a los estudiantes se ingresa por primera vez con el número de cedula tanto en nombre de usuario y clave presentándole la siguiente interfaz gráfica.

Figura 15-5: Menú usuario contador en el sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Preinscripciones: las acciones que se realiza dentro de esta opción es el de buscar al estudiante por cedula o nombre de la lista de personas pre inscritas en el sistema académico del IPEC en un determinado programa de maestría y que posteriormente fueron migradas hacia el SICOIPEC, una vez encontrado el estudiante se le genera la orden de pago por concepto del examen de admisión.

Figura 16-5: Interfaz de la generación de orden de pago en el sistema de cobros
Realizado por: *Escobar, M. Alarcón R. 2023*

Registrar Pago: Aquí se registra el pago del derecho del examen de admisión de una forma detallada es decir se almacena el nombre de la maestría, versión, nombres completos del estudiante, numero de cedula, numero de factura, fecha de pago y el valor pagado.

Cambiar ha inscrito: en esta parte del menú se realiza en cambio de estado de todos los estudiantes que rindieron el examen de admisión y entrevista y están aptos para proceder ingresar a la maestría, por eso se lo tiene que realizar manualmente porque se tiene que evaluar todo lo mencionado anteriormente.

Figura 17-5: Interfaz gráfica del cambio de estado a inscrito de los aspirantes
Realizado por: *Escobar, M. Alarcón R. 2023*

Inscritos-Generar Orden Matricula: las acciones que se realiza dentro de esta opción es el de buscar al estudiante por cedula o nombre de la lista de personas que luego del proceso de admisión están aptas para matricularse en un determinado programa de maestría y generar su respectiva orden de pago con los valores previamente ingresados en la parte del administrador mismos que fueron tomados del proyecto de maestría aprobado.

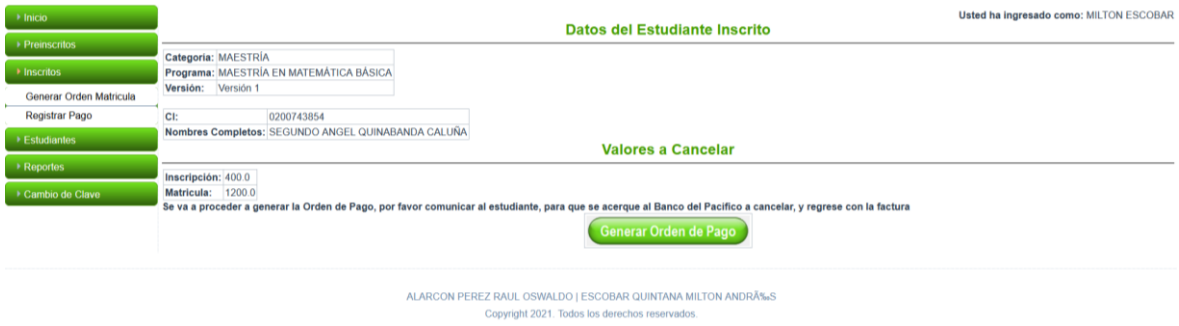


Figura 18-5: Generación de orden de matricula
Realizado por: *Escobar, M. Alarcón R. 2023*

Inscritos-Registrar Pago: Aquí se registra el pago de la inscripción y matrícula de una forma detallada es decir se almacena el nombre de la maestría, versión, nombres completos del estudiante, numero de cedula, numero de factura, fecha de pago y el valor pagado.

Estudiantes-Generar Orden Colegiatura: esta opción está separada de la opción del registro del pago de la inscripción ya que por ser el valor más grande a pagar por parte del estudiante como es la colegiatura, el Posgrado puede autorizar el financiamiento hasta

en 3 cuotas haciéndole más accesible el pago a los estudiantes. En el reporte de este campo se evidencia igual todos los pagos realizados por parte del estudiante y en observaciones se evidencia si mantiene deuda o no con el Posgrado.

Figura 19-5: Generación de orden de colegiatura
Realizado por: *Escobar, M. Alarcón R. 2023*

Como se puede evidenciar en la siguiente imagen del SICOIPEC existen dos opciones para generar el pago de la colegiatura, la primera opción que tienen los estudiantes es por el valor total:

Figura 20-5: Opciones para generación orden de colegiatura
Realizado por: *Escobar, M. Alarcón R. 2023*

Y la segunda para pagos de la colegiatura por cuotas en donde se ingresar el monto a cancelar.

Figura 21-5: Opciones para generación orden de colegiatura por partes
Realizado por: *Escobar, M. Alarcón R. 2023*

En la opción de reportes se puede revisar toda la información generada en detalle por cada uno de los estudiantes y también en forma general.

Figura 22-5: Interfaz gráfica de los reportes
Realizado por: *Escobar, M. Alarcón R. 2023*

CONCLUSIONES

- El desarrollo de un sistema web como herramienta para almacenar los procesos realizados por la persona encargada de gestionar los pagos que realizan los maestrantes del Instituto de Posgrado por varios rubros es un recurso necesario ya que en estos momentos el Instituto no cuenta con un mecanismo automatizado que realice estos registros y se ha convertido en un problema importante cada vez que se cambia de persona que realice estos trámites, ya que cada quien almacena la información de manera diferente que solo es entendido por sí mismo y no queda claro para la persona que toma la posta.

- El desarrollo de un sistema web para almacenar información financiera requiere de varias protecciones de seguridad ya que se maneja información sensible y delicada razones por las cuales se ha implementado un módulo de seguridad basado en la norma ISO 27000 y 27001 en aspectos relacionados con métodos de acceso al sistema, transferencia de datos e integridad de datos.

- Es importante la inserción de mecanismos de seguridad en los resultados obtenidos, en este caso se ha implementado el código QR en la impresión de los reportes con información del Instituto de Posgrado que puedan evidenciar que efectivamente son una impresión exacta del sistema web.

RECOMENDACIONES

- Se recomienda la implementación del sistema web con el módulo de seguridad propuesto en el Instituto de Posgrado previo a realizar diferentes validaciones en ingreso de datos, accesos al sistema y la manera de transferencia en la red.

- Se recomienda la utilización de accesos biométricos al sistema web ya que se reduce por lo menos en un 60% el peligro de vulnerar el sistema por usuarios no autorizados ya que con este tipo de autenticación necesariamente se necesita que la persona que registró en el sistema una característica propia suya sea quien valide dicha prueba y pueda ingresar.

- Al ser un sistema nuevo que aún no se encuentra en producción se recomienda primero que se pase un tiempo mínimo de 4 meses en la fase de pruebas para poder detectar fallos: en el ingreso y almacenamiento de datos, cálculos matemáticos y todos los procesos que están involucrados.

GLOSARIO

- **Confidencialidad:** La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.
- **Integridad:** Garantía de exactitud y fiabilidad de la información.
- **Disponibilidad:** Se refiere al área del conocimiento y la práctica informática dentro de la seguridad de la información que facilita el acceso a los datos de personas y organizaciones con los cuales se puede trabajar.
- **Información:** Es cualquier dato obtenido por una persona, independientemente de su forma de presentación.
- **ISO:** Es la Organización Internacional de Normalización, cuya principal actividad es la elaboración de normas técnicas internacionales.
- **Norma:** Regla o un conjunto de estas, una ley, una pauta o un principio que se impone, se adopta y se debe seguir. Sirve para realizar correctamente una acción o también para guiar, dirigir o ajustar la conducta o el comportamiento de los individuos.
- **Telemática:** La combinación de la informática **y** de la tecnología de la comunicación para el envío y la recepción de datos.
- **Mitigar:** Es el proceso de reducir amenazas o riesgos potenciales a los que se expone un negocio o proyecto
- **QR:** Quick Response, es un código de respuesta rápida.
- **Software:** Es un conjunto de reglas o programas que dan instrucciones a un ordenador para que realice tareas específicas.
- **Neomorfismo:** Es un estilo de diseño de interfaces que combina sombras y luces para crear un efecto de profundidad en los elementos de la interfaz.
- **Microinteracciones:** Pequeños momentos en que el usuario y el diseño interactúan.
- **5G:** Quinta generación de las redes móviles.
- **Crítica:** Esto quiere decir que la información es indispensable para el funcionamiento y operación de la institución o empresa.
- **Valiosa:** Como lo mencionamos, son activos indispensables de las instituciones, por lo tanto, deben ser resguardadas y protegidas para evitar poner en riesgo el futuro de la organización.
- **Sensible:** Esto significa que solo debe ser conocida por las personas autorizadas por la organización.

- **Hacker:** Persona curiosa, inconformista y paciente que busca su superación continua aprovechando las posibilidades que le brindan los sistemas.
- **Cracker:** Hacker dañino.
- **Phreaker:** Persona que engaña a las compañías telefónicas para su beneficio propio.
- **Pirata Informático:** Persona que vende software protegido por las leyes de Copyright.
- **Insider:** Personal interno de una organización que amenaza de cualquier forma al sistema de la misma.
- **SSL:** La sigla SSL significa Capa de sockets seguros**,** es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada.
- **TLS:** Seguridad de la capa de transporte, es un protocolo de cifrado que se utiliza para la transmisión de datos en Internet.
- **ECC:** Código de corrección de errores, se utiliza para verificar transmisiones de datos localizando y corrigiendo errores de transmisión.
- **RSA:** Es un sistema criptográfico que permite enviar mensajes cifrados sin tener que intercambiar una clave privada y es el más utilizado para este fin.
- **DSA:** Algoritmo de Firma digital, es un algoritmo creado como propuesta para el proceso de firmas digitales. Se utiliza para firmar información, más no para cifrar ésta.
- **HTTPS:** Hyper Text Transfer Protocol Secure, es el protocolo a través del cual se envían datos entre el navegador y el sitio web al que se está conectado, todas las comunicaciones entre el navegador y el sitio web están codificadas y con un certificado SSL.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información, es un conjunto de políticas de administración de la información.
- **Cifrado:** Es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos.
- **Metodología:** Plan de investigación que permite cumplir ciertos objetivos en el marco de una ciencia**.**
- **Cuantitativa:** Hace referencia a una cuantía, una magnitud, una porción o un número de cosas.
- **Neopositivismo:** Movimiento filosófico que resalta la importancia de la comprobación científica de los conceptos filosóficos y cuyo principal tema de preocupación es el análisis de la significación por medio de un análisis lógico del lenguaje.
- **Pragmatismo:** El pragmatismo es una corriente de pensamiento clásico en el que se establece la validez y pertinencia de determinados conceptos e ideas en relación con su

utilidad práctica. Se trata, por tanto, de una filosofía orientada hacia una experiencia utilitaria de la realidad.

BIBLIOGRAFÍA

Adrián, Yirda (2021) ConceptoDefinición

https://conceptodefinicion.de/codigo/

Tibor Moes SoftwareLab.org is part of Momento Ventures Inc. © 2014-2021. All rights reserved. https://softwarelab.org/es/que-es-una-vulnerabilidad-informatica/

ISOTools Excellence (2017) https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

Victoria Bembibre (2009) DefiniciónABC
https://www.definicionabc.com/tecnologia/informacion.php

Llama Creativa (2021)
https://www.llamacreativa.com.ar/clientes/index.php?rp=/knowledgebase/3/iQue-es-una-aplicacion-o-sistema-web.html

https://dspace.ups.edu.ec/bitstream/123456789/12298/1/UPS-GT001626.pdf

https://www.iso27000.es/sgsi.html

Blog especializado en Sistemas de Gestión de seguridad de la información [En línea] 2015

https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Copyright 2019 Universidad Iberoamericana IBERO

https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

© 2021 DigiCert Administre sus certificados en DigiCert® CertCentral

https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

B-Secure. (2015). *B-Secure*. Obtenido de https://www.b-secure.co/infografia-herramientas-ddos

CERN. (27 de 11 de 2016). *CERN*. Obtenido de https://home.cern/

CIOSPAIN. 2017. CIOSPAIN.ES. [En línea] 2017. http://www.ciospain.es/movilidad/cisco-telepresence-permite-a-los-medicos-realizar-consultas-virtuales.

Fernández Sorribes, J. (Julio de 2016). *Universidad de Castilla-La Mancha.* Obtenido de http://www.esi.uclm.es/www/cglez/downloads/students/pfc/2006_jafernandez.pdf

Foster, I., & Kesselman, C. (2003). *"The Grid 2: Blueprint for a New Computing.* Morgan Kaufmann.

Globus.org. (2017). *Globus.org.* Obtenido de http://toolkit.globus.org/toolkit/about.html

Grant, R. (2004). *Dirección Estratégica. Conceptos, técnicas y aplicaciones.* Madrid: Civitas.

Grönroos, C. (1994). *From Marketing Mix to Relationship Marketing: Towards a Paradigm Shift in Marketing.* NY: Management decision.

Hernández, C. (2009). *El plan de marketing estratégico.* México: Gestión 2000.

Instituto Nacional de Estadística y Geografía. (14 de 05 de 2015). *Instituto Nacional de Estadística y Geografía.* Obtenido de http://www.inegi.org.mx/saladeprensa/aproposito/2015/internet0.pdf

Jiménez, D. (2014). *Comunicación Integral de Marketing:Análisis del fenómeno desde una perspectiva Teórico-Práctica*. Recuperado el 16 de julio de 2016, de aedemo: http://www.aedemo.es/aedemo3/socios/revista90/rev_90_02.pdf

Kreps, G. (2012). *La Comunicación en las Organizaciones.* Madrid: Addison-Wesley.

Lopez de Lara, E y Luevano, E. 2014. Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación. [En línea] 2014. https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiXjp-9193SAhXDNSYKHR8mDBQQFggYMAA&url=http%3A%2F%2Fwww.oei.es%2Fhistorico%2Fcongreso2014%2Fmemoriactei%2F939.pdf&usg=AFQjCNFWZo840xUA7OYCF5lsUJlsw5JZjw&bvm=bv.149760088,d.eWE&ca.

Mendoza Acevedo, E. (2005). *UTM.* Obtenido de http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis_Emmanuel.pdf

Mendoza, M. (2007). *Gicoge Udistrital.* Obtenido de http://gicoge.udistrital.edu.co/elearning/pdfs/miguel_mendoza.pdf

MercadoLibre. (2017). *MercadoLibre*. Obtenido de http://computacion.mercadolibre.com.ec/disco-duro

Morgan, J. (2007). Customer Information Management (CIM): the Key to Successful CRM in Financial Services. Boston: Journal of Performance.

NewEraCracker. (2016). *GitHub*. Obtenido de https://github.com/NewEraCracker/LOIC

ÑACATO ESTRELLA, DIEGO RAMIRO. 2014. Escuela Superior Politécnica de Chimborazo. [En línea] 2014. http://dspace.espoch.edu.ec/bitstream/123456789/3622/1/108T0106.pdf.

Pérez, J. (2016). *Definición de.* Obtenido de http://definicion.de/cluster/

Quishpe, H. (2016). *Repositorio UNL*. Obtenido de Análisis de Vulnerabilidades en la Red LAN Jerárquica de la Universidad Nacional de Loja, en el Área de la Energía, Industrias y los Recursos Naturales No Renovables": https://dspace.unl.edu.ec/jspui/bitstream/123456789/16039/1/Quishpe%20Malla,%20Henry%20David.pdf

Reyes Días, Dailos. 2014. Universidad de La Laguna. [En línea] 2014. https://riull.ull.es/xmlui/bitstream/handle/915/633/TFG%20-%20Robot%20Android%20y%20Telepresencia..pdf?sequence=1&isAllowed=y.

Rodríguez, P. (18 de 08 de 2011). *Departamento de ciencias de la computación Universidad de Chile.* Obtenido de https://www.dcc.uchile.cl/node/833

SALVADOR SALVADOR, GUSTAVO ADOLFO. 2007. Escuela Superior Politécnica Nacional. [En línea] 5 de 2007. http://bibdigital.epn.edu.ec/bitstream/15000/8403/3/CD-0728.pdf.

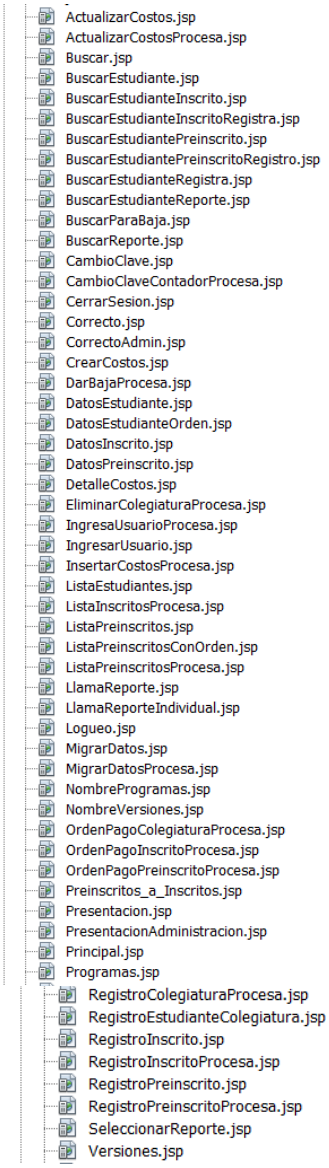
Sampieri, R. (2007). *Fundamentos de metodología de investigación.* México: McGraw-Hill.

https://www.normas-iso.com/iso-27001/

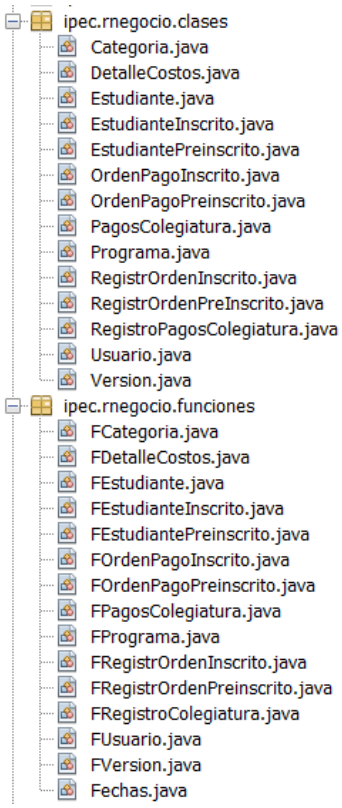
https://normaiso27001.es/referencias-normativas-iso-27000/

ANEXOS

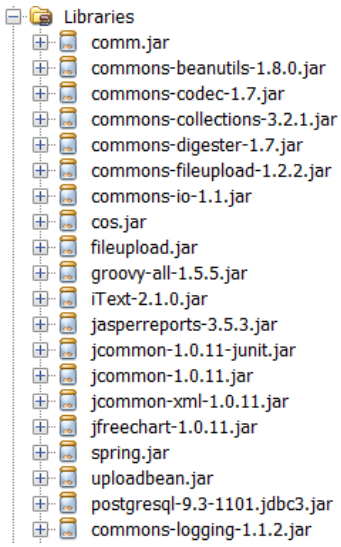
ANEXO A: LISTA DE PÁGINAS JSP DEL SISTEMA INFORMÁTICO FINANCIERO



ANEXO B: LISTA DE CLASES DEL SISTEMA INFORMÁTICO FINANCIERO



ANEXO C: LISTA DE LIBRERÍAS JAR UTILIZADAS EN EL SISTEMA INFORMÁTICO FINANCIERO



ANEXO D: EJEMPLO DEL CÓDIGO DE PROGRAMACIÓN DE LA CLASE ACTUALIZACOSTOS.JSP DEL SISTEMA INFORMÁTICO FINANCIERO

```
<%@page import="java.util.ArrayList"%>
<%@page import="ipec.rnegocio.funciones.*"%>
<%@page import="ipec.rnegocio.clases.*"%>
<jsp:useBean id="ubDetalleCostos" scope="page"
class="ipec.rnegocio.clases.DetalleCostos"/>
<jsp:useBean id="ubUsuario" scope="page" class="ipec.rnegocio.clases.Usuario"/>
<%
   String idUsuario="";
   HttpSession sesionVerifica = request.getSession();
   if (sesionVerifica.getAttribute("idUsuario") == null)
   {
%>
      <jsp:forward page="CerrarSesion.jsp"/>
<%
   }
   else
   {
    idUsuario = sesionVerifica.getAttribute("idUsuario").toString();
   }
%>
<%@include file="html/Encabezado.html" %>
<%@include file="html/MenuVerticalAdmin.html" %>
<!--para buscar a los estudiantes preinscritos-->
<%
   Integer idUser= new Integer(idUsuario);
   ubUsuario=FUsuario.ObtenerDatosUsuario(idUser);
%>
```

```
<p align="right"><%out.println("<b>Usted ha ingresado como:
</b>"+ubUsuario.getNombres()+" "+ubUsuario.getApellidos()); %></p>

<form action="ActualizarCostosProcesa.jsp" method="get">

<center>

   <%

      Integer id= new Integer(request.getParameter("cod"));

      ubDetalleCostos=FDetalleCostos.sp_obtener_detalle_costos_dado_id(id);

   %>

<h1><center><font color="449E00" >Datos del Programa</font></center></h1>

<hr>

  <table>

     <tr>

     <td>Categor&iacute;a:</td>


<td><%out.println(ubDetalleCostos.getCodVersion().getCodPrograma().getCodCategor
ia().getNombreCategoria());%></td>

     </tr>

     <tr>

     <td>Programa:</td>


<td><%out.println(ubDetalleCostos.getCodVersion().getCodPrograma().getNombrePro
grama());%></td>

     </tr>

     <tr>

     <td>Versi&oacute;n:</td>


<td><%out.println(ubDetalleCostos.getCodVersion().getNombreVersion());%></td>

     </tr>

  </table>

<h1><center><font color="449E00" >Costos</font></center></h1>

<hr>
```

```
<table>
   <tr>
      <th style="background-color:#449E00;">PREINSCRIPCI&Oacute;N</th>
      <th style="background-color:#449E00;">INSCRIPCI&Oacute;N</th>
      <th style="background-color:#449E00;">MATRICULA</th>
      <th style="background-color:#449E00;">COLEGIATURA</th>
      <th style="background-color:#449E00;">TOTAL</th>
   </tr>
   <tr>
<%
     out.println("<td><input type=text name=txtPreinscripcion value="
+ubDetalleCostos.getPreinscripcion()+" /></td>");
     out.println("<td><input type=text name=txtInscripcion
value="+ubDetalleCostos.getInscripcion()+" /></td>");
     out.println("<td><input type=text name=txtMatricula
value="+ubDetalleCostos.getMatricula()+" /></td>");
     out.println("<td><input type=text name=txtColegiatura
value="+ubDetalleCostos.getColegiatura()+" /></td>");
     out.println("<td><input type=text name=txtTotal
value="+ubDetalleCostos.getTotal()+" /></td>");
     out.println("<input type=hidden name=idCosto value="+id+" />");
     out.println("<input type=hidden name=codVersion
value="+ubDetalleCostos.getCodVersion().getCodVersion()+" />");
%>
   <tr>
   <td colspan="5"><center><input name="" type="image" src="images/guardar.bmp"
/></center></td>
   </tr>

            </tbody>
   </table>
```

```
</center>
</form>
<%@include file="html/PiePagina.html" %>
```