SEGURIDAD INFORMÁTICA DEL MODELO VISTA CONTROLADOR (MVC) EN APLICACIONES PUNTO DE PAGO-POS

DAVID FERNANDO ROSERO GUERRERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
EPECIALIZACION SEGUIRIDAD INFORMATICA
SAN JUAN DE PASTO,
NOV 2019

SEGURIDAD INFORMÁTICA DEL MODELO VISTA CONTROLADOR (MVC) EN APLICACIONES PUNTO DE PAGO-POS

DAVID FERNANDO ROSERO GUERRERO

Monografía para optar para el título de Especialista en Seguridad Informática.

Director:

ING. LUIS FERNANDO ZAMBRANO HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

EPECIALIZACION SEGUIRIDAD INFORMATICA

SAN JUAN DE PASTO,

NOV 2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

Dedicatoria:

Este compendio de conocimiento está dedicado a mi Creador, Mi familia, esposa e hijos, que son mi más grande motivación, los amo…

AGRADECIMIENTOS

Agradezco a toda mi Familia, mi madre, mi esposa y mis hijos, quienes, con todo su amor, paciencia y regalándome el tiempo que les corresponde fueron mi apoyo para lograr realizar este sumario rico en conocimientos informáticos, muchas gracias por su apoyo y constante ánimo.

CONTENIDO.

LISTA DE FIGURAS.

Pág.

LISTA DE TABLAS.

Pág.

LISTA DE CUADROS.

Pág.

GLOSARIO.

MODELO: La forma en que está elaborado, un objeto, resultado, sistemas, etc. Para este caso es la forma o arquitectura de programación en que está diseñado una ampliación en capas.

VISTA: Hace referencia el campo visual que una persona alcanza a mirar, hace referencia en este caso al diseño visual de la arquitectura de programación, es lo que el usuario mira en pantalla.

CONTROLADOR: Es un conductor que maneja un objeto, sistema o programa, en este caso se utiliza, para modificar, el procesamiento dentro de la arquitectura de programación con el objetivo de brindar procesos seguros y confiables que usuario realiza a la base de datos.

SEGURIDAD: todas las acciones que protejan un determinado bien o interés, en este caso aplica la seguridad en la informática con todas las barreras de defesa que se utilizan para proteger, datos información sensible para una empresa.

PATRONES: Se define como los datos que se repiten de manera constante durante una investigación u observación, para el caso son las soluciones a los problemas más comunes en el desarrollo de programa de computador y otros espacios referentes al diseño de interacción.

SDL: Son las siglas para designar al ciclo de vida del desarrollo seguro, que es un concepto de control y seguridad que se debe embeber en los proyectos de software. Con el solo ánimo de mejorar la calidad y los riesgos inherentes a esta.

MODELADO: Se refiere a metodología donde se planifica y se bosqueja un diseño que será la pauta a seguir para el desarrollo de un proyecto de software. Esta planificación ayuda en el momento de elegir herramientas, costos, arquitecturas. Etc.

METODOLOGÍA: En los sistemas hablamos de la metodología de diseño, cuando hablamos la forma en que vamos a trabajar, existen las metodologías tradicionales orientada a los objetivos y las metodologías agiles orientadas al cliente.

CICLO DE VIDA: Se refiere al control que se dispone como mecanismo de optimización y seguridad en un desarrollo de software, que permite una mejora continua durante las fases de creación y post producción.

POS: Sistemas punto de pago, son las terminales que permiten el pago en un local comercial, a través de algún medio de pago electrónico, que es un canal comercial entre una tienda y una entidad bancaria.

CAPAS: Es la forma en que está diseñada una arquitectura de desarrollo que puede estar implementada en un proyecto, con el objetivo de brindar líneas de seguridad, aunque varias capas no necesariamente representan mayor seguridad.

VULNERABILIDAD: Son todas las fisuras o vacíos de código que represente debilidades que puede ser explotada por terceros y hacer daños al sistema, por lo cual se debe extender un control de riesgos para el manejo de las mismas.

CONTROL: Se basa en llevar una buena metodología de calidad y seguridad, para garantizar que todo funcione de acuerdo a lo planeado, hablamos de control cuando un objetivo cumple con los parámetros para el cual fue creado.

RESUMEN.

En este estudio se identificaran las vulnerabilidades del sistema POS y posteriormente se realizarán las recomendaciones y correcciones necesarias para reducir los riesgos de seguridad informática y seguridad de la información y amenazas, para garantizar a las compañías que utilizan un sistema POS para controlar inventarios, usuarios, ventas, clientes, proveedores entre otros, y así reducir a corto y mediano plazo los diferentes riesgos informáticos, así como situaciones que involucran a la información, las cuales pueden ser accidentales o provocadas, como alteraciones , accesos no autorizados, perdida de información vital para los consumidores, como nombres, números de cuentas, fechas de caducidad de las mismas, por las que pueden ser víctimas de robo, también afecta la continuidad y control del negocio o vendedor su buen nombre y otras vulnerabilidades.

Palabras clave: bases de datos, contabilidad, empresas, información, Punto de pago, Seguridad, sistema POS, vulnerabilidad.

INTRODUCCIÓN.

La presente monografía tiene como fin principal determinar todos los requisitos necesarios para que el sistema POS, una aplicación web alojada en un servidor, disponible para que los usuarios puedan emplearlo como herramienta y así controlar inventarios, usuarios, ventas, clientes, proveedores, entre otros, de manera permanente, pueda usarse de manera segura, sin poner en riesgo su confidencialidad, la integridad y accesibilidad a la información de los consumidores o clientes de las empresas que lo implementan.

En este documento, primeramente, se presenta la situación actual del entorno internacional y nacional en cuanto a seguridad informática, además se abarcan y se describen situaciones en las cuales las empresas han sido víctimas de hackers y de la delincuencia en línea, también describe las situaciones de los clientes, quienes son las principales víctimas del robo de información confidencial.

También se muestra información sobre la política nacional y las acciones de las autoridades frente a este fenómeno, la descripción de conceptos generales de seguridad informática, entre otros.

Finalmente, se describe la alternativa que se quiere implementar para certificar la seguridad en la información con el uso del sistema POS, haciendo uso del Modelo Vista Controlador los requerimientos tecnológicos, costos, y se compara su eficiencia con otras arquitecturas que también se utilizan en seguridad informática y de la información.

1. PLANTEAMIENTO DEL PROBLEMA.

1.1. DEFINICIÓN DEL PROBLEMA.

El sistema POS es una aplicación web alojada en un servidor, disponible para que los usuarios puedan emplearlo como herramienta y así controlar inventarios, usuarios, ventas, clientes, proveedores, entre otros, de manera permanente. En el sistema POS el acceso a la información es restringido de acuerdo con los niveles y privilegios de usuario que brinda. Su capacidad de almacenamiento de información permite alojar grandes cantidades de datos. Tal como lo menciona Luis Díaz aborda el tema de la arquitectura del sistema SAP como programa con un módulo capaz de realizar un proceso de compra mediante el acceso de los datos.[1]

Sin embargo, esta aplicación puede ser presentar diversas vulnerabilidades tales como ataques SQL, denegación de servicio distribuido DDoS, Ransomware, Malware, accesos no autorizados, que ponen en peligro la confidencialidad, integridad y su accesibilidad de la información de los consumidores o clientes de las empresas que lo implementan. Esto representa además para las empresas pérdidas de tiempo, de dinero y operatividad.

Poder proteger las empresas de perdida de información es vital tener un plan SGSI donde se aborde y contemple toda la seguridad de los sistemas, desde la infraestructura, trasporte de datos, como lo datos mismos y el personal que lo maneja, de tal forma que poder usar un modelo vista controlador, dentro de la programación del sistema POS, es comenzar a tomar buenas decisiones dentro de la gobernanza de los sistemas de una empresa.

---

[1].DIAZ, Luis. Introducción al sistema SAP R/3: formación para el empleo, Editorial CEP 2011.pag: 20.

2. JUSTIFICACIÓN.

El estudio permitirá identificar y corregir las falencias que pueda presentar el sistema POS con el fin de que el almacenamiento y uso de la información de los consumidores o clientes y el funcionamiento y continuidad de las actividades de las empresas que lo implementan, no se vean afectadas debido a perdida o fuga de información, además de pérdidas económicas para ambos.

Si se identifican las falencias, estas deben ser resueltas a través de mecanismos que ayuden a establecer los controles en todos los procesos informáticos que involucran información con el fin de optimizarlos, mejorar la seguridad, registrar y monitorizar el acceso a la información y gestionar el uso de recursos tecnológicos y realizar recomendaciones para buenas y mejores prácticas informáticas.

La programación MVC, es una arquitectura madura en programación que aparta la información, de la interfaz del cliente y la lógica de programación, por eso su manejo en tres módulos: la vista que es lo que el usuario puede ver, el modelo es la maquetación que el sistema maneja, su lógica de la acción y su función, por otro lado, está el controlador que es un mediador entre modelo y vista, regula el flujo de información entre ellos y no permite que la información se filtre. Esta programación permitirá que la aplicación POS y sus bondades, pueda ser implementada por las empresas, de forma sólida, perdurable, segura y compatible.

Las empresas se verán directamente beneficiadas en el manejo adecuado de la información, contribuyendo a la protección de información sensible, irrecuperable e intangible porque la modelo vista controlador, ofrece seguridad, facilidad encontrando errores y manejo simple en la recuperación ante la caída del sistema.[2]

---

[2].Universidad de Alicante, Modelo vista controlador (MVC) Madrid, [Consulta: 10 noviembre 2018]. Disponible en: https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html

3. OBJETIVOS.

3.1. OBJETIVO GENERAL.

Poner a prueba la seguridad de la información en una aplicación web punto de pago POS, con el uso de la programación MVC-modelo vista controlador.

3.2. OBJETIVOS ESPECÍFICOS.

- Identificar los posibles riesgos de la seguridad informática en un sistema POS, mediante un análisis de uso del modelo vista-controlador.

- Determinar las falencias de programación en los modelos convencionales aplicados al POS, los cuales no brindan protección en datos de los usuarios.

- Identificar las vulnerabilidades, fallos e interrupciones que se estén presentado en la implementación del sistema POS convencionales.

- Establecer los controles en todos los procesos informáticos que involucran información con el fin de optimizarlos, mejorar la seguridad, inspeccionar el acceso a la información y gestionar como es el uso de recursos tecnológicos.

- Realizar recomendaciones para buenas y mejores prácticas informáticas, siempre basados en el modelo vista-controlador.

4. MARCO REFERENCIAL.

A continuación, se presenta las el marco referencial donde se presentan los antecedentes y regulaciones respecto a la seguridad informática colombiana, además se mencionan las instituciones que tienen implicación respecto a la incidencia de la seguridad informática de nuestra región.

4.1. MARCO CONCEPTUAL.

Es necesario contextualizar los aspectos que hacen referencia a la seguridad informática con el ánimo de entender este contenido de este documento por tal motivo se presenta el siguiente cuadro comparativo con las temáticas más importantes que nos muestran un panorama adecuada de la seguridad de la información.

Cuadro 1. Temáticas de Seguridad Informática.

Temáticas	Definición	Características	Diferencias
Seguridad de la Información	Son aquellas medidas preventivas y correctivas de un sistema informativo que permita resguardar la información logrando confidencialidad, disponibilidad e integridad de los datos.	Busca garantizar la privacidad entre usuarios. Por ejemplo, los datos de una tarjeta de crédito	La seguridad informática está dedicada la protección de la infraestructura, los usuarios y el tráfico de información a diferencia de la seguridad de la información que solo se encarga de brindar seguridad a la información.[3]
		Debe Garantizar la integridad de la información que se maneja evitando modificaciones no autorizadas.	
		Posee mecanismos para garantizar la disponibilidad de la información.	
Seguridad Informática	Es el área informática y telemática relacionada con la seguridad que se	Se encarga de diseñar normas, procedimientos, métodos y técnicas destinados a conseguir	La seguridad informática se

	enfoca en la protección de la infraestructura computacional, la información y su tráfico a través de una red	que un sistema sea seguro	encarga de crear normas y procedimientos de seguridad de un sistema, mientras que la seguridad de la información evalúa los riesgos, amenazas y vulnerabilidades de la información.[4]
		Identifica las vulnerabilidades, riesgos y amenazas de seguridad.	
		La seguridad Informática está concebida para proteger infraestructura computacional, los usuarios y la información.	
Norma ISO 27001	Es un estándar internacional para la seguridad de la información aprobado en octubre de 2005 por la ISO/IEC.[5]	Fue concebido para planificar, Verificar, Hacer y Actuar en los sistemas de seguridad de la información	Las empresas al cumplir con la Norma ISO/IEC 27001 logran estandarizar su calidad en el código profesional de seguridad, la norma 2002 no logra esta ventaja.
		El cumplimiento de la norma en cualquier empresa otorga un certificado de calidad en seguridad Informática.	A pesar de que la norma 2002 esta estandarizada a nivel internacional, esta no está normalizada en todos los países a diferencia de la Norma 27001
		Una de las características principales de esta norma es que después de su planificación siempre se debe Evaluar el proceso por completo lo cual garantiza la seguridad en los sistemas.	
Norma 2002	Es un estándar internacional para la seguridad de la información modificado el 2013 por la ISO/IEC	Puede implementarse como sistema de gestión de seguridad de la información.	La Norma 27001 está basado en gestión de seguridad cíclica donde se definen controles y medidas a diferencia de la norma 2002 que
		Está compuesta de 14 ítems entre los que se encuentran: control,	

		criptografía, seguridad, usuarios, incidencias y cumplimiento.	solo es una guía para mejorar la seguridad basada en los sistemas de gestión.
COBIT	Es una guía estandarizada dirigida al control y supervisión de tecnología de la información	Usada para gobernar y la gestión de los servicios de la Tecnología de la información basado en negocios.	COBIT describe una guía de que se debe hacer en el control y supervisión de tecnologías de la información, mientas que ITIL describe de manera robusta el cómo se deben hacer las buenas prácticas de servicios de tecnólogas de la información.
		Se preocupa en orientar a las organizaciones en la implementación, operación y mejora de los procesos de gobernanza y gestión de TI.	
		Delimita los principios de una organización según sus necesidades corporativas, principalmente en recursos y activos de las TI	
ITIL	Es un conjunto de conceptos de buenas prácticas usadas para la gestión de los servicios de tecnologías de la información, el desarrollo de nuevas TI y las operaciones involucradas en la misma	Posee tres niveles de certificación: Básico, de Responsabilidad, de director) sin embargo ITIL no certifica, pero al cumplir la norma se logra Certificarse en ISO/IEC 20000.	Estas Normas o guías de control raramente son usadas por separado, puesto que están diseñadas para complementarse entre sí, por lo que es difícil obtener resultados al aplicar las normas de manera individual
		Su diseño está basado en los negocios por lo que implementa una estrategia, diseño, transición, operación y mejora continua del servicio prestado.	

		Está pensado en la gestión de servicios de tecnologías de la información para organizaciones a gran escala; si bien se puede implementar en pequeñas empresas su uso en las mismas recorta de diseño en grande.	
Controles	Los controles son medidas o procedimientos de seguridad que se aplican como barreras para el acceso de la información de un sistema, pueden ser físicos, técnicos y administrativos.[6]	Los controles físicos hacen referencia a mecanismos con el objetivo de detener o prevenir el acceso no autorizado.	Los controles son procedimientos de bajo nivel es decir lleva una tarea de forma detallada, mientras que una política es una determinación de alto nivel donde la visión es a nivel general de la situación.
		Los controles técnicos son basados en estructuras técnicas aplicadas en la red y en el tráfico de datos.	
		Los controles administrativos hacen referencia al registro y control del factor humano de quienes tienen acceso a la información, que es mayor factor de debilidad de un sistema.	
Políticas	Las políticas de seguridad son un compendio de determinaciones que cada entidad se impone así misma con el objetivo claro de proteger, disponer y garantizar la seguridad de la información. Se	Cada organización delimita como va a proteger sus activos de información, según lo crea necesario.	Los controles son aplicados de la misma forma sea cual fuere la dimensión o tamaño de la organización que los implementa, mientras que las políticas tienen la misma magnitud de
		Las políticas tienen la cualidad de ser modificables y actualizables según las circunstancias lo	

	denominan de alto nivel porque son impuestas desde el eslabón más alto, como la gerencia.	ameriten, siempre deben estar en aplicación para su aplicación y seguimiento, las deben conocer todos los miembros de la organización.	acuerdo al tamaño de las empresas, es decir, empresas pequeñas políticas pequeñas o empresas grandes políticas grandes, puesto que intervienen mayor número de personas en estos procesos.
Gobierno TI	Son los mecanismos de gobernabilidad en las tecnologías de la información diseñadas en la alta dirección con el objeto de cumplir con las normativas que permita la gestión en las operaciones y usos de la tecnología de una empresa con miras empresariales.	Su principal característica es la monitorización de las directrices y la toma de decisiones estratégicas de las Tecnologías de la información, su correcto uso y la optimización de sus recursos. Está basada en la gestión de riesgos, rendimiento y recursos de una organización para garantizar una correcta operación. La aplicación de un gobierno TI dentro de una organización le da valor agregado a la misma, que en si es uno de los objetivos primordiales de aplicar estos procesos.	El gobierno TI toma diseña directrices que la organización necesita, lo cual implica una visión general de los temas a abordar, mientras que la gestión de la seguridad, por otro lado, impone los mecanismos específicos o procesos necesarios que garanticen el cumplimiento de dichas directrices
Gestión de la seguridad	Se trata de conocer los riesgos, amenazas y vulnerabilidades de una organización en	Los procesos básicos de la gestión de la seguridad son: Planificar, Hacer, Verificar y Actuar	Los mecanismos de gobierno TI determinan los alcances de los

	cuanto a la tecnología de información y controlar, corregir o mejorar lo que esté causando problemas, está definido en el SGSI (Sistema de gestión de la seguida informática).	El diseño de la gestión de la seguridad de una organización está influenciado por: sus necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización, razón por la cual su dimensión y complejidad se debe ajustar a lo requerido por la misma.	objetivos a lograr mientras que la gestión de la seguridad aplica de manera específica los procedimientos que conlleven a lograr los objetivos que el gobierno determino.
		La gestión de seguridad debe estar documentada como constancia de que se tiene un plan de acción en cuanto a la seguridad informática.	
Riesgos	Determina que tan probable es que se concrete una amanezca sobre los bienes informáticos y al mismo tiempo impacto que pueden causar.	Se aplican métodos que determinan, analizan, valoran y clasifican el riesgo de una amenaza que permitan implementar mecanismos de control y defensa de la información.	El riesgo es la probabilidad latente de que ocurra una amenaza y una amenaza es la materialización del riesgo.
		Identificar los riesgos en una organización dentro de un plan de gestión de la seguridad permite potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado mínimo de riesgos.	

		Controlar un riesgo es a largo plazo una inversión para una organización que garantiza la protección de los bienes informáticos.	
Amenazas	Es una situación o acontecimiento que puede causar daños a bienes informáticos causados por una persona, software, sucesos naturales o de otra índole y representan posibles peligros a la perdida, plagio o divulgación de la información que son debilidades en un sistema.	Las amenazas siempre están latentes alrededor de los sistemas, siempre algo puede salir mal, las amenazas son naturales o provocadas, tiene un enorme potencial de causar daño.	
		Es la materialización del riesgo en las tecnologías de la información.	

Fuente: Cuadro comparativo temáticas Seguridad Informática, elaboración propia.

[3].Seguridad Informática, ministerio de tecnologías. Bogotá [Consulta: 15 noviembre 2018] https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

[4].Oficina para las redes informáticas. [Consulta: 15 noviembre 2018] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

[5].Normas ISO/IEC. ISO 27001 seguridad de la información, Madrid [Consulta: 15 noviembre 2018] https://www.normas-iso.com/iso-27001/

[6].Oficina para las redes informáticas. [Consulta: 16 noviembre 2018] https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

[7].Guía de proyectos. Bogotá. [Consulta: 16 noviembre 2018] https://www.mintic.gov.co/arquitecturati/630/articles-9401_pdf_01.pdf

[8].Sistema de Gestión del Seguridad. SGSI. Madrid. [Consulta: 19 noviembre 2018] Normativa. http://www.iso27000.es/sgsi.html

4.2. MARCO LEGAL.

La legislación colombiana está basada en las leyes de su constitución diseñada en 1991, en donde de forma insípida solo hasta el año 2012 se comienzan a diseñar unas normas y regulaciones para la seguridad informática, que hasta nuestro día continúa vigente, pero que es claro que aún debe mejorarse y detallarse acorde a las nuevas formas de delitos que se vienen registrando.

4.2.1. Ley 1273 de 2009.

A continuación, se describe las leyes que rigen en Colombia respecto de los delitos informáticos causados por la delincuentes o piratas informáticos, que están basados en la ley 1273 de 2009, que modifica la constitución de 1991, donde se expresan las penas y las sanciones, junto con las multas en caso de infringir la ley.

Cuadro 2. Resumen de la legislación colombiana.

Capítulo 1.	
Artículo 269a. acceso abusivo a un sistema informático.	Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv.
Artículo 269b. obstaculización ilegítima de sistema informático o red de telecomunicación	Pena de prisión (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv.
Artículo 269c. interceptación de datos informáticos	Pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Artículo 269d. daño informático.	Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv.

Artículo 269e. uso de software malicioso.	Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv.
Artículo 269f. violación de datos personales.	Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv.
Artículo 269g. suplantación de sitios web para capturar datos personales.	Pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 smlmv., siempre que la conducta no constituya delito sancionado con pena más grave.
Artículo 269h. circunstancias de agravación punitiva	Se otorgará la pena más alta cuando haya sevicia en los procedimientos, se reitere los delitos.[9]
capítulo 2	
Artículo 2691. hurto por medios informáticos y semejantes	incurrirá en las penas señaladas en el artículo 240 de este Código.
Artículo 269j: transferencia no consentida de activos.	Pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 smlmv. Si la conducta descrita es superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.[10]

Fuente: Congreso De Colombia, LEY 1551 DE 2012, resumen elaboración propia.

[9]. Congreso De Colombia, LEY 1551 DE 2012 (Julio, 06, 2012). Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 2012. 15p. ARTÍCULO 7o.

[10]. Congreso De Colombia, LEY 1273 DE 2009 (enero, 05, 2009). Por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios. El Congreso. Bogotá D.C., 2009. 2p. ARTÍCULO 296o.

4.3. MARCO TEÓRICO.

En Colombia y en el mundo, uno de los mayores retos es la lucha contra los crímenes cibernéticos, una acción que constantemente se evoluciona, se actualiza para servirse de cualquier vulnerabilidad en la internet con el fin de secuestrar, alterar o copiar un sinnúmero de datos que en ella están depositados con información importante y confidencial de las empresas y las personas.

Según el balance de las autoridades de la policía colombiana el crimen informático, en el 2017 estos delitos tuvieron un crecimiento del 28,3 %, en relación del año anterior y comprometieron a 446 empresas del país, cifra que es escandalosa respecto a la seguridad. Vigilar esta agresión no es un reto menor, pues las autoridades afrontan un crimen que traspasa la mayoría de los límites, es por ello que actualmente se busca cooperación internacional entre las entidades de seguridad. En Estados Unidos, un 54% de las compañías soportaron ataques de piratas informáticos en sus sistemas en el año 97 ocasionando detrimentos totales de 137 millones de dólares. En organizaciones como CIA, UNICEF, la ONU y otras organizaciones internacionales no han sido ajenas a estos ataques. Un pirata informático puede tardar meses en quebrantar un sistema ya que cada vez más son sofisticados y mejor preparados; pero llegaran a resolver lo, a cometer el crimen y muchas veces con rastros mínimos.[11]

Carlos Castañeda técnico en ciber seguridad, manifiesta que los incidentes de ciber seguridad va en engrandecimiento y el 2019 el crecimiento será considerable. La tendencia de los ataques indica que crecerán en un 35% este año al menos los próximos cinco años; sin embargo, este dato puede no ser tan real, puesto que existen ataques que no son registrados, no son denunciados por las propias organizaciones o víctimas, por tratarse muchas veces de incidentes que comprometen información que no debe tener terceros.

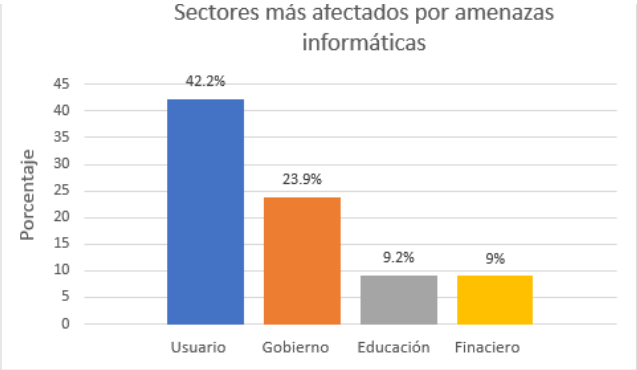
---

[11] El secuestro de información desangra a las empresas del país. Revista portafolio. [Consulta: 16 noviembre 2018] https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

Las empresas minoristas no salen airosas de estos ataques y son este tipo de empresas las que implementan los sistemas POS para controlar sus inventarios, control de ventas, horario de los empleados entre otros. Los sistemas de pago de ponto de venta han sido un punto de ingreso transcendental para muchas filtraciones en el sector de ventas minoristas.

Las nuevas tecnologías en sistemas punto de pago POS, los piratas informáticos han encontrado la gallina de los huevos de oro, porque pueden acceder a los datos de miles de compradores en sus tarjetas de crédito e información personal, con esto fácilmente pueden hacer compras o pagos en páginas no registradas como las que están en la Deep web, con la que vacían los créditos de los clientes y de otra forma venden los datos a otros piratas que a su vez, explotan las bases de datos de los clientes.[12]

Figura 1. Sectores afectados por amenazas.



Fuente: autoría propia.

Ante estos incidentes algunos comercias han optado por mejorar la transmisión de la información cliente -servidor a través de la encriptación AES 256, que es una de las más seguras, ejecución de tokens, apegarse al estándar EMV, testeos de penetración de la seguridad y capacitación en trabajadores enfocado en seguridad de sistemas de POS.[13]

---

12. Riesgos cibernéticos por sector. Marsh, Guadalajara [Consulta 19 enero 2019] recuperado de: https://www.marsh.com/mx/insights/research/riesgos-ciberneticos-por-sector.html
13. Ibid.., p02.

Sin embrago, los diferentes ataques cibernéticos pasan por falta de visión estratégica, aún para muchas empresas no ven el costo-beneficio, esto es debido a que no se dimensiona realmente los alcances y consecuencias que genera un ataque de un pirata informático.

Jorge Bejarano, exdirector de seguridad digital MinTIC hace una reflexión de que la mayoría de las empresas no le dan valor a su información hasta que es muy tarde y se ha generado grandes prejuicios**.** La encuesta del ministerio de la información y las telecomunicaciones afirmo que el 72% de las empresas no capacita la personal en temas de seguridad de la información, el 83 % de las empresas no poseen los protocolos de respuesta a la infracción de manejos de seguridad informática y no cuentan con el personal idóneo ni un área adecuada de respaldo.

Los riesgos mutan y cada vez los ataques son más sofisticados. En la medida que los procesos dependan más de las tecnologías de la información y que haya interese por parte de los delincuentes cibernéticos de obtener ingresos a través de la afectación de las cuentas, el riesgo siempre estará presente.

El departamento de defensa de los estados unidos nos hace entender que toda línea de defensa en contra de los ataques informáticos, son válidos para resguardar la información según las necesidades de cada negocio, generando salvaguardas ante las amenazas y vulnerabilidades, esto se define como seguridad informática.[14]

Las amenazas que los piratas informáticos siempre buscan comprometer datos significativos y sistemas enteros son, estos atacantes son de tres tipos:

---

[14].Cyberseguridad. Washington, Departamento Nacional de Seguridad de los Estados Unidos. [Consulta 24 de enero 2019] https://www.usa.gov/espanol/agencias-federales/departamento-de-seguridad-nacional

1. **Hacker de Sombrero Negro**. Son los piratas de la información con habilidades muy altas en vulnerar sistemas, con el objetivo de realizar una explotación de los datos para un posible comercio ilegal, cuenta con herramientas muy sofisticas.

2. **Hackers de Sombrero Gris**. Generalmente este tipo de atacantes vulnera sistemas sin permiso, muchas veces sin obtener nada, pero se burla de sistemas con bajo nivel de protección, no siempre las intenciones son buenas. [15]

En el momento que los clientes obtienen bienes o servicios de un vendedor y la transacción es procesada por uno de los sistemas punto de venta POS, los dispositivos tales como el equipo denominado datafono de la tarjeta de crédito o débito, el dispositivo debe estar conectado a un pc o móvil en donde los datos almacenados en la banda magnética, los números de cuenta, nombre del cliente de la tarjeta, fecha de caducidad, número de seguridad, son elementos que los delincuentes cibernéticos utilizan para lograr su cometido.

Estos se han orientado a los datos de los clientes en las bases de datos de los POS. A veces, los bandidos conectan un terminal físico al sistema POS para recoger identificaciones de la tarjeta, a esta acción se la denomina ***skimming***.

Otras ocasiones, los piratas cibernéticos distribuyen malware o software malicioso que obtienen la información del sistema POS, Información que luego es enviada a los piratas informáticos. Luego esta información se vende a terceros con intenciones totalmente ilegales.

Los sistemas de puntos de pago habitualmente se conectan a servicios de Internet y correo electrónico. Esta es la entrada por la cual a través de las varias formas de penetración o ataques al sistema entregan frutos a los malhechores y estos fácilmente obtiene los datos de los clientes.

[15.] Tipos de Hackers existente y a que se dedican, Muy Interesante, México [Consulta 24 enero 2019] https://www.muyinteresante.es/tecnologia/articulo/que-es-un-hacker-de-sombrero-gris-831473842564

Esta responsabilidad delincuencial recae directamente sobre los piratas de sombrero negro quienes hacen ataques de phishing, ransomware, y crypto-hacking con el fin de beneficiarse.[16]

4.4. LA SEGURIDAD DE UN SISTEMA POS.

Este sistema no es nuevo el punto de pago se ideo en la década de los ochenta cuando la tecnología fue capaz de hacer una transacción electrónica vía teléfono, sin embargo, a finales del siglo XX, es donde se perfecciona esta técnica, con el uso del software y hardware indicados, que facilitan los procesos del comercio.

Todo esto fue en auge y el uso de los tradicionales sistemas de transición electrónica a través de sistemas POS, empezó a quedar en la ambigüedad, puesto que los sistemas en general si evolucionaron, superando las operaciones realizadas en los puntos de pago, permitiendo hoy en día, estar en un punto de riesgo; aun conociendo este antecedente, el comercio debe continuar sin detenerse, pues apoya a la sociedad y su economía.

Los comercios son sensibles en los malos manejos de los datos, pero esto no debe ser un limitante para que no se beneficien de la tecnología, por el contrario, es una herramienta que permite el crecimiento del mismo, por tal motivo la arquitectura de seguridad se la informática es el uso de MVC-Modelo vista controlador.

Un método de punto de pago, retrata más gastos a las empresas en comparación a un sistema en línea de tiempo real, dado que se necesita pagar una licencia (Costosa), además de capacitación, actualizaciones y mantenimiento.

[16.] Coordinación de Seguridad de la Información incidentes at seguridad. México, [Consulta: 3 febrero 2019] http://www.seguridad.unam.mx ftp://ftp.seguridad.unam.mx)

Por sus tipologías, estos métodos no están acabados en tiempo real en las otras sedes o puntos de venta de la empresa, que los ralentiza y con información caduca, figurando un obstáculo para los patrones del comercio que necesitan tener en cuenta altos niveles de ventas.[17]

Posteriormente, los sistemas de facturación usuales, son programas cegados sin ningún tipo de acceso a internet, es decir que no están en el ciber espacio, lo que implica que los atacantes tengan que ir a realizar los ataques directamente en los comercios. Lógicamente el sistema tradicional no está siendo obsoleto sobre todo en temas de datos en tiempo real.

4.5. SISTEMAS DE PUNTO DE VENTA EN UN HOSTING.

El hecho de que un sistema de punto de venta POS, este funcionando en línea, o desde el momento que fue posible, en ese momento nació el comercio electrónico, porque significaba la realización de una transacción comercial satisfactoria desde cualquier parte del mundo con un pago con cualquier moneda del mundo.

Un software POS en el hosting tiene la gran ventaja, es su habilidad de uso, porque no se necesita más que un computador o móvil conectado a internet para usarlo, permitiendo acceder de manera vertiginosa y simple a un sistema de facturación comercial, desde cualquier lugar en que el cliente este.[18]

La flexibilidad de una transacción de pagos es otra ventaja, existiendo muchas empresas bancarias que ofrecen el servicio, que es fácil e intuitivo de usar, que no requiere la mayor capacitación

---

17. Muñiz, Enrique; Moreno Julio. Economía para las empresas. Madrid, [Consulta: 3 febrero 2019] http://servicios.educarm.es/templates/portal/images/ficheros/etapasEducativas/secundaria/16/secciones/270/contenidos/11947/econoempresa.pdf

18. ¿Qué es un sistema POS? Todo lo que debes saber, Freire Ezequiel, Escuela de Emprendedores, Re https://escuela-emprendedores.alegra.com/ventas/que-es-un-sistema-pos-todo-lo-que-debes-saber/

Garantía es la otra ventaja de los sistemas de punto de pago en línea. Ya que cuenta con respaldo para resguardar datos, sirve como soporte ante caídas del sistema y tiene un funcionamiento de tiempo completo a cualquier hora del día, lo que es una enorme herramienta para los comercios.[19]

Cuando un sistema de punto de venta es incorporado a un e-commerce, esté tipo de empresas recorta sus gastos ya que, al estar automatizado, ya no necesita estar, con un responsable o personal que ayude en él proceso, ya que tiene un asistente virtual o el proceso es tan intuitivo que cualquier persona lo puede hacer sin ayuda.

La arquitectura modelo vista controlador, permite a un sistema de punto de pago, convertirse en una ampliación web poderosa con herramientas que van más allá de la transacción, pues están en la capacidad de ejercer control sobre inventarios, registros de ventas, clientes, proveedores y usuarios en general. [20]

La estar en línea los comercios pueden hacer consultas de las transacciones en tiempo real que le permite reaccionar a una empresa inmediatamente, lo que representa que tiene un dominio o control total sobre sus ventas, inventarios y usuarios. Esto para un comercio representa la optimización ideal de su operatividad, generando los mejores resultados, es la mejor información que puede tener.

Los sistemas de punto de venta de vanguardia, que grandes compañías tienen modularizan no solo las ventas, sino que además poseen módulos contables que realiza operaciones casi de inmediato, y mediante la arquitectura MVC, las empresas trabajan bajo un mejor ambiente seguro.

---

[19].Ortega Lidia, Ramos Miguel Ángel E-commerce y pago seguro. Madrid. [Consultado: 12 febrero 2019] Recuperado de: https://core.ac.uk/download/pdf/44310168.pdf

[20]. Maldonado José, Comercio Electrónico, Chile: [Consultado: 12 febrero 2019] https://www.gestiopolis.com/comercio-electronico-ideas-fundamentales/

Sin duda estar en línea con un sistema de punto de pago no tiene comparación en seguir insistiendo en la utilización de sistemas tradicionales, por la satisfacción en cuanto a mejora de servicios, recorte en tiempo e integridad de datos tanto para el usuario como para la empresa. [21]

Sin embrago, es necesario garantizar la seguridad del mismo, ya que puede llegar ser vulnerado poniendo en riesgo la disponibilidad, integridad y confidencialidad de la información.

4.6. METODOLOGIA DE DESARROLLO MVC.

Todo proyecto de software, debe tener una metodología de desarrollo con el objetivo de planear lo que se va a ejecutar, entender que rumbo va a tomar, midiendo sus alcances, simplificando y optimizando los procesos, esto permitirá un desarrollo con visión profesional, que organice y documente cada parte del proyecto, esto medido en función del tiempo. Existen dos tipos de metodologías de desarrollo, las tradicionales y las agiles, existen marcadas diferencias entre las metodologías mencionadas, pero las más relevantes es que las metodologías tradicionales son secuenciadas, consecutivas y lineales, mientas que las metodologías agiles son variables y se adaptan a los cambios fácilmente, puede realizar varias tareas al mismo tiempo.

La arquitectura de programación modelo vista controlador está basado en las metodologías agiles y su entono de trabajo conocido como framework, admite la adaptación de muchos desarrollos de la comunidad de código abierto, esto permite que muchas herramientas sean añadidas directamente a los proyectos en desarrollo, que es otra notoria diferencia con las metodologías tradicionales, que tienen que desarrollar todo desde cero y no admite códigos de terceros o la adaptación de desarrollos previos, esto implica mayor tiempo en la obtención de resultados.

[21.] T. Gipselly, Por qué es importante tener un sistema POS en la nube, [Consultado: 12 febrero 2019] https://www.loggro.com/blog-software-de-gestion-erp/por-que-es-importante-tener-un-sistema-pos-en-la-nube/

4.6.1. Ventajas y desventajas de las metodologías.

Se mencionan a continuación de manera comparativa las metodologías de desarrollo.

4.6.2. Metodologías Tradicionales.

Las metodologías tradicionales han sido usadas desde hace muchos años, están repletas de formalismos y formato muy estructurado que no les permite hacer trabajos en paralelo, sino que avanza según se trace un plan de desarrollo. Esto conlleva tener una normativa clara y sin espacios a nuevas rutas de diseño, la idea principal es tener control sobre cada paso, lento pero seguro. Además, no hay internación completa del cliente, solo si es necesario, a veces no tienen en cuenta al cliente, ya que satisfacen una población en general.

Cuadro 3. Ventajas y desventajas Metodología Tradicional.

Ventajas	Desventajas
Estructurado y secuenciado: esta metodología, pretende trazar una sola ruta de trabajo, con tiempos específicos, alcances y objetivos.	El trabajo es completamente lineal, no se puede trabajar de forma paralela en otras actividades sin que antes se obtenga resultados esperados en cada etapa.
Orientado a Resultados: si se obtiene un logro o meta se continua con la etapa siguiente.	Al no poder avanzar a otras etapas hasta culminar las que se trazaron durante su diseño y planificación, se requiere más tiempo.
Planificación y Diseño: se hace por etapas, revisiones y aprobaciones.	Durante el desarrollo de la programación de un software se presentan errores o fallas en las pruebas, lo que implica mayor, costo y tiempo porque se debe rediseñar lo planteado.[22]

[22.] Zhu, Hong. Software Design Methodology: From Principles to Architectural Styles, Elsevier Science & Technology, 2005. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=269543.

4.6.3. Metodologías Agiles.

Esta metodología nace con el objetivo de acortar tiempos en desarrollo, fueron pensadas principalmente para realizar tareas de forma simultánea y paralela sin detenerse en ningún momento reduciendo así los tiempos muertos, sin embargo, requiere de muchos roles bien definidos y objetivos claros, esto no implica dejar a un lado los formalismos o los planes de desarrollo, pero su agilidad se basa en ser

Cuadro 4. Ventas y desventajas Metodología Ágil.

Ventajas	Desventajas
Adaptación a los cambios: esto permite que se tenga un respuesta rápida y oportuna en función del tiempo.	Dependencia de los Lideres del proyecto: Los líderes del proceso tomen decisiones rápidamente y de forma acertada, de lo contrario se generan, pérdidas de tiempo y generan altos costos.
La intervención del cliente es fundamental: es muy importante que el cliente esté involucrado en el proceso, para que el desarrollo se convierta en lo que se conoce como software a la medida.	Escasa documentación, por lo general este tipo de proyectos careces de un proceso documental, dejando de lado muchas veces valiosos recursos de desarrollo, que se quedan en el olvido.[23]
Simplificación y tareas a intervalos: Las tareas que son repetidas, pueden simplificarse o readaptarse a un solo proceso, las cuales se cumple por etapas en función del tiempo.	Curva de aprendiza y solución prolongada: muchas veces los proyectos avanzan acorde a lo planificado, sin embargo, en ocasiones resulta, que aprender este tipo de metodología cuesta mucho tiempo y dinero, por lo que un error puede ser solucionado en mucho tiempo.[24]

[23.] Zhu, Hong. Software Design Methodology: From Principles to Architectural Styles, Elsevier Science & Technology, 2005. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=269543.

[24.] Maida, EG, Pacienzia, J. Metodologías de desarrollo de software. Tesis de Licenciatura en Sistemas y Computación. Facultad de Química e Ingeniería “Fray Rogelio Bacon”. Universidad Católica Argentina, 2015. Disponible en: http://bibliotecadigital.uca.edu.ar/repositorio/tesis/metodologias-desarrollo-software.pdf pág. 108

4.6.4. Comparativa metodología Ágil y Tradicional.

Cuadro 5. Comparativas metodologías de desarrollo.

Comparativa	
Tradicional	**Ágil**
Diseño lineal, con una planificación muy estructurada, no permite avanzar otros objetivos o alcances del proyecto sin antes terminar los que estén en ejecución.	Trabaja un diseño en secuencias o fases, permite trabajar de forma paralela los objetivos o alcances del proyecto.
La interacción con el cliente es mínima, se estudia una necesidad, pero no se ahonda en los detalles de su necesidad, por lo que se presenta una solución generalizada para la solución de un problema.	La interacción con el cliente es mayor en esta metodología, se requiere mucho de su participación, cuanta más información de las necesidades el cliente aporte, la ampliación será más específica o a la medida de las necesidades.
La documentación en cada fase es estricta, cada avance debe ser registrado, los cambios se analizan para una futura optimización.	Aunque en esta metodología se puede llevar un registro documental, no es necesaria su implementación, la mayoría realizan comentarios y anotaciones en las propias líneas de código.
El tiempo de desarrollo es mayor, ya que sus fases implican mucho reproceso, a continuación, mencionamos sus etapas: - Toma de requisitos. -Diseño y planificación. -Codificación y pruebas. -Pruebas generales. -Pruebas en el sitio.	El tiempo de desarrollo es menor, se simplifican algunos procesos. Algunas de las etapas de desarrollo son: -Toma de Necesidades. -Codificación Sprint. (planificación y ejecución al tiempo) -Pruebas (todas pruebas se realizan al unísono).

-Corrección de errores (repite todas las etapas anteriores). -Entrega del proyecto. -Parche para correcciones (repite todas las etapas anteriores).[25]	-Corrección de errores. -Entrega final.

Queda claro entonces que la metodología del modelo-vista controlador está basado en una metodología ágil, esto no quiere decir que sea una metodología fácil de utilizar, ya que este modelo primero requiere de su manejo, esto significa que tiene una curva de aprendizaje bastante pronunciada, pues la identificación de los errores, puede ser un tema complejo para quienes no están familiarizados en esta arquitectura de diseño.

4.7. CICLO DE VIDA DEL DESARROLLO SEGURO.

Durante mucho tiempo en el área de la industria de los sistemas ha existido un pensamiento en que se mezclan conceptos de seguridad del software y la seguridad de las aplicaciones, teniendo a unificar los criterios, sin embargo, esto no es correcto ya que existen marcadas diferencias entre estos criterios de seguridad.

Para tener despejado este tema debemos tener en claro que la seguridad del software consiste en crear un software seguro, un equipo de desarrollo idóneo y usuarios capacitados en la incorporación de la seguridad, del otro lado está la seguridad de la aplicación que consiste en proteger el software y los sistemas que lo soportan y lo hospedan, y este tipo de seguridad solo comienza, después de que el desarrollo se completó.[26]

---

[25].Maida, EG, Pacienzia, J. Metodologías de desarrollo de software. Tesis de Licenciatura en Sistemas y Computación. Facultad de Química e Ingeniería “Fray Rogelio Bacon”. Universidad Católica Argentina, 2015. Disponible en: http://bibliotecadigital.uca.edu.ar/repositorio/tesis/metodologias-desarrollo-software.pdf pág. 108

[26]. McGraw, G. (2006), Software Security: Building Security In, Boston: Addison-Wesley, p. 20.

Tiempo atrás, los desarrolladores e inversionistas de software no estaban muy a favor de aplicar seguridad informática a sus desarrollos, por los costos y porque era una tecnología en nacimiento, sin embargo, a través del tiempo se han presentado múltiples formas de vulnerar sistemas con técnicas como cross-site Scripting (XSS), la inyección de código SQL y el desbordamiento de búfer, Esto afecto monetariamente la integridad de muchas compañías informáticas, algunas de las cuales quebraron y pasaron a la historia, pero otras compañías fueron más visionarias y tener un modelo de seguridad que les permitió escalar en su modelo de negocio.

La seguridad inicialmente fue aplicada en los sistemas operativos, luego en la red y por último en las aplicaciones, todo esto genero una necesidad latente de proteger de forma integral los sistemas y la información que estos contienen, es aquí donde nace el concepto del SDL, ideado por Microsoft desde luego, pionero y líder.

El ciclo de vida del desarrollo seguro tiene sus principales características basada en la seguridad donde todos sus componentes desarrollan actividades prácticas para presentar un software robusto y reforzado, a través de un plan de acción, jerarquías de gobernanza con políticas y controles muy específicos, con el solo objetivo de reducir y mitigar las vulnerabilidades explotables dentro de los sistemas creados.

Se debe tener en claro que la implementación de un SDL no se debe aplicar después del desarrollo del software, por el contrario, es un trabajo paralelo al desarrollo desde el inicio aplicado de forma inherente al buen diseño de este. Cuando se aplica este concepto los resultados tangibles se notan y mejoran considerablemente la calidad del trabajo.[27]

[27.] Ransome, James, and Anmol Misra. Core Software Security: Security at the Source, Auerbach Publishers, Incorporated, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1547083. Pág. 20

El modelo SDL permite a los desarrolladores desde las fases más tempranas planificar y solventar soluciones previas ya que esto representa menos costos y menos trabajo, ya que modificar un avance y luego restructurar todo es muy complejo y más costoso.

Figura 2. Ciclo de Vida SDL-Microsoft.

Fuente: recuperado de: https://enriquedutra.files.wordpress.com/2012/01/sdl.png

Este modelo es conocido como Computación Confiable (Trustworthy Computing) que Microsoft ha adoptado como una de sus principales metodologías de desarrollo, existen otros modelos maduros que tiene una estructura similar pero simplificada como la SAMM de OWASP y el BSIMM que es un estudio para organizaciones unidas que trabajan en la seguridad informática, estas métricas son ahora estándares internacionales para muchas compañías en el mundo.

El modelo SDL, tiene como pilar fundamental tres elementos centrales como son la Integridad, Confidencialidad y disponibilidad, conocido también como modelo CIA, que son la base para todo desarrollo informático.

4.7.1. Ciclo de vida del movimiento vista controlador.

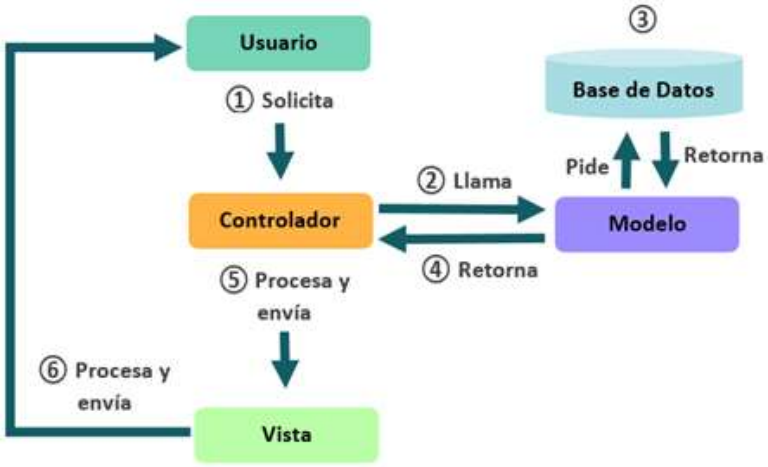
El ciclo de vida de un software es el conjunto de etapas que contemplan su cuidado durante el tiempo que un proyecto va a existir, desde su planeación e iniciación de su

construcción, durante el proceso de madurez y optimización y así como en el momento en que deje de ser funcional, obsoleto o simplemente en desuso.

Estas etapas contemplan al usuario como el medidor tiempo, porque es quien determina hasta qué momento se va a usar un desarrollo de software, este desarrollo en las metodologías agiles este hecho en iteraciones, es decir, basados en la repetición de un proceso, que resulta ser una espiral con tal efecto, que en cada ciclo o iteración se va perfeccionando el código y el desarrollo en sí, para presentar un proyecto de alto nivel.

Por otro lado, el ciclo de vida está implícito en la metodología de desarrollo, sin embargo, se debe tener en claro cada concepto es diferente uno del otro, porque la metodología sirve para el desarrollo de proyecto y el ciclo de vida sirve para mantener, soportar y mejorar la vida útil del software.[28]

Figura 3. Ciclo de Vida del MVC.



Fuente: Recuperado de: http://rodrigogr.com/blog/modelo-vista-controlador/

[28] Axelrod, C. Warren. Engineering Safe and Secure Software Systems, Artech House, 2012. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1115666.

4.7.2. Ciclo de vida seguro SDL en el MVC.

Existe hace ya varios años el concepto de SDL, que es la definición del ciclo de vida de desarrollo seguro de un proyecto de software que consiste en controlar de forma segura cada etapa que conforma el proyecto. Su mayor característica es reducir los riesgos por la vulnerabilidad coexistentes en el software con el objetivo de blindar con varias líneas de defensa los datos sensibles y cada uno de los componentes del proyecto de software.

Las fases por las cuales un proyecto está enfocado en un ciclo de vida seguro SDL, son las siguientes:

- Planeación del concepto: esta es la primera etapa del ciclo de vida de un desarrollo de sistemas, se determinan los perfiles y roles de cada miembro del equipo de desarrollo, este equipo traza una ruta de trabajo, define los alcances del proyecto, determina los recursos, las herramientas necesarias y se identifican tiempo, límites y presupuestos.

- Requisitos de necesidades: es cuando tomamos la información que el cliente nos suministra para tomar un rumbo en el proceso, por tal motivo, es indispensable que el cliente entregue toda la información disponible para que el proyecto sea lo mejor ajustada a la realidad posible.

- Diseño: en esta fase los especialistas en cada rol definido, comienzan a trasformar los requisitos de necesidades en requisitos técnicos, donde de estructura un diseño preliminar teniendo en cuenta cada definición de los requisitos, cuando se ha contemplado todas las necesidades se pasa a un diseño técnico detallado, el cual se toma como la herramienta principal para lograr sus objetivos.

- Desarrollo y pruebas: una vez concebido un primer desarrollo de software como un primer intento de solución definitiva, también antes del comienzo de las pruebas

los directores del proyecto debieron documentar todas las funciones del proyecto, de forma muy específica, esto se conoce como capacitación en donde se entrega una guía de uso con las funciones específicas del proyecto de desarrollo, por otro lado se comienza a realizar las pruebas necesarias en el sitio de trabajo o cliente, donde se hace una prueba en fase beta del producto terminado, si producto cumple con la mayoría de las necesidades se puede pensar en hacer la entrega definitiva, que puede recibir más adelante parches de actualización, de lo contrario se debe ajustar, mejorar y corregir el proyecto.

- Puesta en Marcha: los directores del proyecto, entregan el nuevo sistema a los usuarios que están en primera línea de los requerimientos, con la documentación desarrollada en la anterior fase, la capacitación del personal debe hacerse de acuerdo al área de trabajo, así puedan explotar el uso de la nueva herramienta.

- Operaciones y Mantenimiento: entremos en una fase donde todo lo desarrollado entra en operación total, es decir que todo el desempeño se pone en uso, y como en todos los sistemas puede existir caídas del sistema, errores, ataques que debe ser respaldados, por tal motivo se contempla el mantenimiento de los sistemas de forma periódica y continua, para resolver y tener siempre en funcionamiento el sistema.[29]

- Disposición: esta etapa es una fase en la cual se determina si un sistema es obsoleto, o simplemente, cumplió ya su función para la cual fue diseñado, por lo cual es necesario replantear si generar actualizaciones o desarrollar una versión mejorada de la versión original, esto, aunque parezca no ser efectivo, por lo contrario, es bueno, ya que los sistemas mejoran, la tecnología aumenta y los tiempos se reducen.

[29.] Ransome, James, and Anmol Misra. Core Software Security: Security at the Source, Auerbach Publishers, Incorporated, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1547083. Pág. 20

Como conclusión se puede decir que el ciclo de vida SDL, está implícito dentro de la arquitectura de desarrollo MVC, sin embargo, se debe aclarar que la metodología de esta arquitectura es ágil, lo que quiere decir que la forma en que se aplica no necesariamente lleve el orden antes mencionado, y esto no significa que la esencia del ciclo de vida SDL se pierda, porque las fases van a ser siempre las mismas solo que en distinto orden.

4.8. ALGUNAS DE LAS AMENAZAS INFORMÁTICAS.

Los ataques más utilizados a nivel global son 10 según el OWASP a continuación los describimos los más usados:

Aunque existen otras amenazas computaciones que pueden perturbar a la seguridad de la aplicación web, la defensa de estas principales amenazas bastará para mantener un sitio o aplicación web de manera segura.

4.8.1. Malware.

El malware es un software malicioso, diseñado para corromper un sistema y alterarlo. Su amplio espectro de acción es bastante variado desde virus que pueden dañar un pc, hasta aplicaciones adware que bloquean o modifican un portal web. Una web vulnerada por malware muestra datos confidenciales, contenida la información de los clientes, que realizan sus compras en las bases de datos.

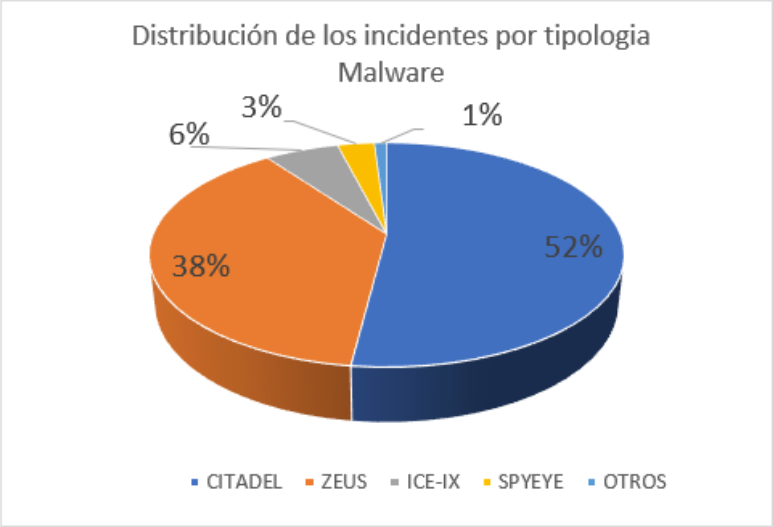
Los ataques son muy dañinos para empresas que tiene bases de datos y resulta muy perjudicial sus impactos, más aún cuando se evasiva es tardía. Un informe de 2018 sugiere que el 65% de aplicativos y páginas web sufrieron ataques por malware, dos de ellos son:

- **Defacement**: Tiene la capacidad de cambiar la maquetación de una página y muchas veces ostenta el atacante con su seudónimo, haciendo caer la página.

- **Redirección maliciosa**: Otra conocida técnica es el Spoofing que redirecciona un sitio seguro, a un sitio falso sin que la víctima se dé cuanta y deposita así información sensible, creyendo el cliente que está en un portal seguro.

A continuación, se muestra la distribución de los incidentes por tipología de Malware.

Figura 4. Incidentes por tipología Malware.



Fuente: Elaboración Propia.

4.8.2. Inyección SQL.

Las vulnerabilidades pueden suceder cuando una página dispone de fallo de seguridad en el código que admite que aquellos con propósitos astutos ataquen o logren el control. Esto es usualmente causado por contrariedades en plugins de WordPress desactualizados u otras herramientas esgrimidas en la web.

La inyección Sql consiste en inyectar líneas de código a través de consultar o querys que se ejecutan en espacios para completar información por parte del usuario, logrando que estos no solo extraigan información básica, sino que logren hacer consultas más abundantes y precisa y así extraer valiosa información.

Si el ataque se ultima con éxito, consiguen robar información del cliente, cambiar o eliminar datos, o para obtener un control absoluto de la web. Esta es una de las amenazas informáticas más desarrolladas en el mundo.[30]

También en este mismo año se detectó que más de 1000 sitios web presentaban ataques de inyección SQL Esta amenaza de seguridad web además está comprendida en los diez riesgos de seguridad de las aplicaciones web más peligrosos de OWASP en 2017.[31]

4.8.3. Ataques (XSS).

Es una amenaza bastante difundida por los atacantes pirata. A diferencia de la Inyección SQL, XSS en consultas a la plataforma de JavaScript que básicamente desarrolla scripts o línea de código que permiten el acceso a información sensible.

Dichos scripts tienen la capacidad de secuestrar secciones de acceso de usuarios y posteriormente robar información al cliente o redireccionar al cliente a páginas falsas, lo que se conoce como Spoofing, y luego extraer datos sensibles del cliente.

4.8.4. Intercepción de datos MITM.

Se basa en la interceptación de la comunicación, cliente -servidor y mediante herramientas con ataques de hombre en el medio, pueden ver los datos de la víctima, así sacar información importante al cliente, luego robarle o vender lo datos para otro le cause daños.[32]

---

30. Tutoría de Seguridad en WordPress, Guía completa, [Consultado 1 marzo 2019] https://www.webempresa.com/wordpress/tutorial-seguridad-en-wordpress-guia-completa.html

31. Inyecciones SQL, [Consulta 4 abril 2019]: https://www.mclibre.org/consultar/php/lecciones/php-db-inyeccion-sql.html

32. Romero Martha, Figueroa Grace, Introducción a la seguridad Informática y el análisis de vulnerabilidades https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf.Pag 18.

En Bélgica por ejemplo con este tipo de interceptación en el año 2015, lograron obtener la información de muchos usuarios, que posteriormente robaron y que la suma de lo que se gastaron oscila los 6 millones de dólares, este hecho no pudo tener un buen término y no hubo resultado de aprensión de la criminalidad.

Google en 2014 avaló la certificación de seguridad SSL como un método de encriptación de alta confianza, que permite la conexión cliente – servidor de manera segura. Esto disminuyo considerablemente los ataques de interceptación.[33]

4.8.5. Ataques de sesión con contraseña.

Algunos piratas informáticos predicen contraseñas o usan herramientas y programas de catálogo para probar por ensayo y error disímiles combinaciones hasta que las localizan una contraseña. Existen ataque de este tipo con elementos sofisticados, como es el caso del keypress, que una herramienta maliciosa, guarda el orden de las teclas que presiono el usuario, incluso con software detecta de acuerdo al sonido producido las teclas que fueron presionadas, así poder capturar una secuencia o contraseña.[34]

Varias páginas web no posee ningún tipo de cifrado o acceso mediante doble confirmación o ingreso con biometría. Por lo que la pagina debe sugerir las siguientes recomendaciones:[35]

- Sugerir Contraseñas más robustas y difíciles de copiar.

---

[33]. Romero Martha, Figueroa Grace, Introducción a la seguridad Informática y el análisis de vulnerabilidades. [Consulta: 4 abril 2019] https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf. Pag 42.

[34].Serrano Francisco. Obteniendo información del evento (objet-event). [Consulta:4 abril 2019] https://uniwebsidad.com/libros/javascript/capitulo-6/obteniendo-informacion-del-evento-objeto-event

[35]. Seguridad en Internet con SSL y HTTPS, [Consulta: 4 abril 2019] https://www.ionos.es/digitalguide/paginas-web/creacion-de-paginas-web/certificados-ssl-y-https-maxima-seguridad-para-tu-web/

- El usuario debe actual periódicamente su contraseña.
- Autenticación en dos pasos para el acceso a través de un móvil o correo electrónico.

4.8.6. Ataque de denegación DDOS.

Un ataque de denegación de servicio distribuido (DDoS) se basa en saturar las consultas que un servidor puede manejar hasta desbordar la ejecución de millones de consultas falsas a la vez, dejando vulnerable el sistema. Para que este ataque tenga un efecto, debe asociar se a varios atacantes, denominados botnet, puesto que hay muchos servidores que tiene la capacidad de rechazar un ataque o simplemente tienen un poder de responder a todas esas consultas. Al estar saturado la página cae y no tiene fuerza para seguir funcionando. Laboratorios Kasperrsky dice que 33% de los ataques son DDoS.[36]

4.9. CONFIGURACIONES INCORRECTAS.

En un comienzo los sistemas se basaban en la confianza, con la premisa inocente, del momento que nadie, se le ocurrir hacer daño a otro, pero sucedió, al contrario, cada vez el tema de ataque creación por lo que los sistemas contienen muchos huecos de seguridad, que poco a poco se van mejorando, pero que muchas veces suceden ataque por la simple falta de una correcta configuración. [37]

A pesar de que llevamos ya viendo varios años que los atacantes no tienen respeto por nada y vemos caer grandes compañías por temas de seguridad como Yahoo, la mayoría de empresas no realiza las correctas configuraciones de seguridad a sus sistemas y jamás realizan mantenimientos, muchas ves hasta cuando ya es tarde.

---

[36]. DDoS Protection, Kaspersky [Consultado 20 abril 2019] https://latam.kaspersky.com/small-to-medium-business-security/ddos-protection

[37]. Gonzales Joseé Ciberseguridad retos y amenazas a la seguridad Nacional, España [Consultado 20 abril 2019] http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Cuando una empresa compra un sistema y deja la configuración predeterminada sin cerrar por ejemplo puestos de red que no usa o servicios que están por default, para los atacantes es mucho más fácil encontrar brechas para poderse colar y corromper un sistema, esta es una mala práctica, pero es muy común en las empresas.[38]

Las pruebas de pen-testing sirven de diagnóstico, no hay otra forma de conocer una vulnerabilidad que hacer ataques en ambientes controlados o hacking ético, puesto que sin probar es muy difícil descubrir con una simple inspección visual que todo esté bien, lo segundo sería poner barreras de defensa y mejorar la seguridad y volver a testear para verificar que las vulnerabilidades fueron controladas.[39]

Es necesidad de cada empresa contar con el suficiente conocimiento para el desarrollo e implementación de la seguridad informática y adaptar la Asus necesidades ya que en cada empresa las vulnerabilidades, amenazas y riesgos serán diferentes o al menos con diferente grado de criticidad.

4.10. SEGURIDAD EN LA INFORMÁTICA.

A continuación, se relaciona algunos datos relevantes de la seguridad de la información.

- 70% de las empresas cree que su riesgo de seguridad progresó ampliamente en el 2017.
- Para el 2020, el número de contraseñas manejadas progresará a 300 billones.
- Los ataques informáticos están enfocados en un 43% a pequeños negocios.

---

[38].Abad Mario, La guía para que no te hackeen, España. [Consulta: 20 abril 2019] https://www.vice.com/es/article/yw5qmw/como-evitar-hackeo-seguridad-ciberseguridad

[39].Riesgos y Vulnerabilidades informáticas, Kaspersky. [Consulta: 21 abril 2019] www.kaspersky.com/documents/vulnerability

- Es muy fácil hoy en día desarrollar malware con conocimientos básicos de programación por la cantidad de herramientas que facilitan el proceso se cree que hay alrededor de 230.000 formas de malware. [40]
- Vanson Bourne experto en seguridad, asegura que el 90% de los ataques que son exitosos no dejan rastros porque los atacantes borran sus huellas.
- Normalmente una empresa detecta en 5 meses una nueva vulnerabilidad.
- En el año 2018 hubo más de 3 millones de cripto-ataques.
- Durante todo el 2017 los cripto-ataques crecieron exponencialmente del 8 al 25%.

4.10.1. Pilares de la Seguridad Informática en Aplicaciones en Línea.

Dentro de la seguridad informática, se defienden los requerimientos básicos dentro de la seguridad informática que se denominan pilares de la seguridad, estos tienen como finalidad garantizar que todos los sistemas estén seguros, entre los cuales están la confidencialidad, la integridad y la disponibilidad de la información. Cuando estos pilares no están o alguno de ellos falta la seguridad informática se ve comprometida.[41]

Para las aplicaciones en línea el fundamento es básicamente el mismo cuidar la información desde este criterio informático, sin embargo, expertos de la compañía Google mencionan que las aplicaciones web deben tener un especial énfasis en su seguridad para garantizar un correcto funcionamiento en sus sistemas. Debido a que los ataques en ciberseguridad cada vez tienden al crecimiento, muchas compañías pasan a ser parte de las estadísticas, donde la afectación económica es muy grande, es así que muchas empresas cierran de forma definitiva solo 6 meses después de un ataque a sus datos e información.

---

[40].Osman, Maddy. 7 tipos de amenazas informáticas que toda pyme debe saber, [Consulta: 24 abril 2019] https://es.godaddy.com/blog/7-tipos-de-amenazas-informaticas-que-toda-pyme-debe-saber/

[41].El malware que ataco a miles de empresas. Ituser, Madrid [Consulta: 24 abril 2019] ituser.es/seguridad/2020/05/el-ransomware-ataco-a-mas-de-la-mitad-de-las-empresas-del-mundo-en-2020

La normativa ISO 27000 define a la seguridad de la información a tres conceptos como pilares a saber, la confidencialidad, integridad y disponibilidad de la información, y que su correcto manejo garantiza que la seguridad sea funcional. Por otro lado, esta norma también define otros conceptos como la autenticidad, la responsabilidad, la irrefutabilidad y la fiabilidad como criterios de seguridad.[42]

Estos pilares se ven afectados antes los riesgos, vulnerabilidades y amenazas de la seguridad, que son inherentes a los sistemas, ya que todos los diseños por manos humanas, aunque tengan una elaboración de alto nivel, siempre van a presentar errores a mejorar, pero esto precisamente hacen que se den mejoras en función del uso y del tiempo.[43]

Figura 5. Pilares de la Seguridad de la información.

Fuente: https://ticsalborada1.fandom.com/es/wiki/1._Principios_de_la_seguridad

La disponibilidad es una propiedad como pilar de la seguridad de la información, que se define como la capacidad de acceder y utilizar la información en cualquier momento por un ente o entidad autorizada, que puede ser accedida desde algún software o directamente por los usuarios.

---

[42]. Rerup, Neil, and Milad Aslaner. Hands-On Cybersecurity for Architects: Plan and Design Robust Security Architectures, Packt Publishing, Limited, 2018. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5520891. Pag-204

[43]. Calder, Alan. ISO27001/ISO27002: una Guía de Bolsillo, IT Governance Ltd, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255172.

La confidencialidad, es otra característica que como pilar implica que no se pone a disposición o no está disponible para cualquier usuario o entidad, ni procesos, ni software, solamente usuarios y entes autorizados.

La integridad por su parte es una propiedad que hace referencia a que la información está completa, es la real, no posee errores y tiene tanto exactitud como veracidad en su estructura.

Cuando una explotación de una vulnerabilidad, amenaza o riesgos de uno de los pilares de la seguridad tiene éxito, tendrá un impacto directo sobre los activos informáticos de los sistemas de una organización, por tal motivo estos impactos deben ser identificados, clasificados, numerados y cuando sea posible cuantificados.

La norma ISO/IEC 27001 es clara al imponer como una política de seguridad donde los impactos deben ser evaluados bajo cada uno de los pilares de la seguridad informática, se debe dar por entendido que una sola amenaza puede explotar varias vulnerabilidades a la vez y poner en riesgo los sistemas de una o varias formas, ahora bien, una explotación podría tener más de un tipo de impacto.

Por otro lado, están de manera más explícita, el software en línea tiene una peculiaridad, de estar más expuesto por ser un espacio público, donde cualquier persona puede atentar a la seguridad, es por ello que el equipo de Think de Google, propone para las aplicaciones en línea 6 pilares de la seguridad de la información, que son: Verificación a dos pasos, Actualizaciones, Backups, Https, Sondeos de Seguridad y Capacitación al personal.

Estos 6 pilares de la seguridad en aplicativos en línea, tiene implícito los pilares básicos de la seguridad informática anteriormente mencionados y descritos, ahora es momento de darle una breve explicación a estos nuevos conceptos.

-Verificación a dos pasos: una de las formas de proteger el acceso de usuarios es la verificación del perfil, como se hace convencionalmente, pero hacerlo a dos pasos garantiza que el usuario es que se logue, también lo está haciendo de forma presencial ya que esto está siendo enlazado a un dispositivo móvil en el cual ya está enlazado. Según Google este tipo de procesos ayudo que el total de los ataques de suplantación o Phising sea nulo, ya que esto exige que el personal o comunity managers y hasta el web master tengan una llave de seguridad para el acceso.

-Actualizaciones: Google presenta una analogía diciendo que un sistema desactualizado es como un cordón del zapato desatado, que, aunque puedas seguir caminando, en algún momento puedes caerte y tropezar muy fuertemente. Se ha convertido en una guerra el hecho de que las amenazas por parte de atacantes vulneren los sistemas y al mismo tiempo que los desarrolladores imponen nuevos parches de seguridad, en este caso no solo se habla de proteger al aplicativos, sino de todos los sistemas que componen o son el alojamiento de la información sensible. Es importante contar con las actualizaciones de contenido (CMS).

-Backups: es indispensable en todo momento contar con una copia de seguridad como un respaldo ante los ataques, que en ultimas es una de últimas líneas de defensa, sin embargo, es complicado mantener en funcionamiento un negocio durante la recuperación de la información, pero tener una copia de seguridad reduce considerablemente el tiempo de la continuidad del negocio.

-HTTPS: este es un protocolo de seguridad en línea que tiene como funcionalidad, verificar la autenticidad de los navegantes y evitar que la pagina o aplicación sirva como puente para saltar a paginas ilegales, este protocolo también lo usan los servidores de alojamiento hosting.

-Sondeos de Seguridad: la recomendación es verificar las vulnerabilidades del sistema, existen múltiples formas de hacerlo y verificar si el aplicativo es seguro, por lo tanto,

Google recomienda el Search Console, que es una herramienta que proporción información del estado del sitio o aplicativo web, con esto verificar todos los sitios web vinculados a la organización.[44]

-Capacitación: Una de las falencias más grandes de las empresas es no invertir en la capacitación de los empleados, ya que ellos son la primera barrera de seguridad de una organización, se debe definir con ellos las reglas, responsabilidades y roles del ámbito de la cultura de seguridad.

4.10.2. Estándar de seguridad ISO/IEC 27001

La norma internacional ISO 27000, es un estándar para la seguridad informática, que está siendo muy utilizada actualmente y se está extendiendo su rápidamente por su versatilidad y adecuado diseño que la hacen muy popular entre las organizaciones.

Esta norma está desarrollada por la Organización Internacional de normalización (ISO) y la comisión Electrónica Internacional (IEC), que en este momento se han convertido en un estándar internacional para las buenas prácticas de la seguridad de la información.

A continuación, se describen los estándares de la normativa y con los cambios y fechas de que han sufrido cambios, dando una breve descripción de sus procesos de las diferentes normas que han surgido a partir de la norma ISO/IEC 27000.

---

[44]. Xavier Morales Trust & Safety - User Education & Outreach Specialist in EMEA [Consulta: 12 mayo de 2019] https://www.thinkwithgoogle.com/intl/es-es/futuro-del-marketing/transformacion-digital/los-6-pilares-fundamentales-de-la-ciberseguridad/

Cuadro 6. Familia de Estándares ISO/IEC 27000.

Series norma ISO/IEC 27000	Evolución	Descripción de la serie
ISO 27000	Publicada en 2005, tiene revisiones en 2007 y 2013.	Es la base de la norma actual, esta versión es gratuita, pero faltan algunas mejoras, sin embargo, tiene la estructura fundamental, así como el vocabulario definido en términos técnicos y de gestión.
ISO 27001	Publicada en el año 2013: con mejoras en la versión publica en el año 2015.	Esta versión contempla todos los requisitos de la SGSI: tienen sus bases en la BS7799-2: 2002, puede certificarse a nivel internacional, contiene un anexo denomino A, el cual contempla los objetivos de control y controles sobre riesgos de seguridad.
ISO 27002	Desarrollada en el año 2007, está basada en la norma ISO 17799 del 2005	Esta norma no es certificable, pero es una guía para las buenas prácticas de la SGSI, que contempla 39 objetivos de control y 133 controles de riesgo.
ISO 27003	Publicada en el año 2010 es la evolución de ISO BS 7799-2:2002 en el anexo B.	Es una guía para implementar las normas SGSI, presenta el modelo PDCA y sus requerimientos.
ISO 27004	Presentada en el año 2009	Tiene como novedad, seguir métricas y medidas de eficacia de la SGSI y sus respectivos controles, dichas mediciones son componentes de las fases de

		Implementación y utilización en el modelo PDCA.
ISO 27005	Publicada en 2008, tiene una actualización en 2011	Esta norma establece las directrices para la gestión del riesgo, está basada en la norma ISO 27001, a través de esta norma las empresas pueden determinar el impacto que puede generar los riesgos y hacer una proyección de los eventos adversos que se puedan presentar.
ISO 27006	Publicada en 2009, tiene una actualización en 2011 y una revisión en 2015	Esta norma es de amplia utilización porque contiene los requisitos para una correcta aplicación del SGSI, además que permite la certificación a nivel internacional, está basado en la ISO 27001 con la versión EA-7/03.
ISO 27007	Publicada en 2011	Se trata de una guía práctica para la aplicación de SGSI en empresas con intereses en seguridad informática, mediante la auditoria en tiempo real en las practicas diarias empresariales.
ISO 27011	Publicada en 2008, basada en la norma ISO 27002	Está enfocada en el sector de las telecomunicaciones, que permite ejercer controles de seguridad de forma específica, basada en la privacidad, disponibilidad e integridad en la infraestructura y servicios de estas empresas.
ISO 27031	Publicada en 2011	Esta norma es muy usada y diversificada en empresas que tienen problemas o que

		han sufrido las consecuencias de los riesgos no controlados, pues se trata de una guía para la operatividad de la misma, mediante el uso de la continuidad del negocio, que es un procedimiento que explica cómo proceder ante las calamidades.
ISO 27032	Publicada en 2012	Ofrece una orientación para fortalecer la ciberseguridad de una empresa, basas en puntos técnicos y estratégicos enfocados en la seguridad en Internet
ISO 27033	Publicada en 2009, tiene una actualización en 2014	Es una derivación de la norma 27001 y ISO 18028 que se enfoca en las redes informáticas en específico en su seguridad, ampliamente utilizada por empresas con grandes volúmenes de información.
ISO 27034	Publicada en 2011	Esta norma orienta la seguridad a los desarrollos de sistemas de ciclo de una organización, tanto para desarrolladores, aplicaciones y sus datos.
ISO 37035	Publicada en el año 2011 y tiene una actualización en 2016	Está orientada a la gestión de incidentes que da lugar a que existan controles de detección y correctivas que están destinadas a reducir los impactos desfavorables y aprender para mejorar el SGSI

ISO 27799	Publicada en 2009, ratificada en 2016 AENOR	Es una, modificación de la norma ISO 27001 que está enfocada en el sector de la salud, esta especificada en un conjunto detallado de controles y buenas prácticas para la gestión en salud y seguridad de la información de las empresas del sector sanitario.[45]

4.10.3. Estructura de Estándar ISO/IEC 27001.

Para determinar o planificar un adecuado diseño de software tiene implícito el manejo de un estándar internacional de seguridad de la información con el objetivo de que su calidad sea de alto nivel y pueda estar en una escala mejor respecto a los diseños que no utilizan los estándares.

Las buenas prácticas del desarrollo informático definen que es indispensable el manejo de un sistema de gestión de la seguridad de la información denominado como SGSI, que consiste en trazar un plan de normas basado en el ISO/IEC 27001 que es un ciclo de mejoramiento continuo, en calidad, funcionalidad y seguridad, donde se realizan auditorias dentro de una organización, realizada bajo un grupo de comité que se denomina Gobierno, este gobierno que entrega roles al grupo de trabajo de una empresa puede tomar decisiones trascendentales en la construcción informática de una organización.

[45]. Calder, Alan. ISO27001/ISO27002: una Guía de Bolsillo, IT Governance Ltd, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255172. Pag 45

Figura 6. Infografía norma Técnica ISO/IEC 27001.

Fuente: Elaboración propia.

La normativa tiene un algoritmo lógico de operación que consiste en ir avanzando en la medida, que se identifique cada factor que pueda estar en contra de la correcta operación, para ello se montan planes de trabajo que sirven como un mapa que indica el rumbo de las metas alcanzables.

Primero se define un gobierno con roles y funciones que son capaces de definir las políticas que serán de estricto cumplimiento, los roles gubernamentales no solo están dispuestas para el área informática dentro de una organización, también la pueden ejecutar las personas de áreas diferentes, pero que estén en las capacidades de entender si una acción está bien realizada o debe corregirse.

Por otro lado, están las políticas, que son las directrices que el gobierno definido en una organización ordena cumplir, que deben ser de estricto cumplimiento y que no da lugar a dudas, no pueden ser saltas o evadidas, por ello, es indispensable que estas políticas sean clara y bien definidas dentro del plan de trabajo dentro del sistema de gestión de la seguridad de la información.

Luego de esto arranca ya un trabajo más práctico, pues se trata de determinar mediante un análisis los riesgos propios de un sistema donde se identifican las vulnerabilidades y amenazas que representan riesgos para la seguridad de la información, con esto poder estar un paso delante de atacantes que pudieran estar interesados en explotar dichas fallas.

Para mejorar las fallas de explotación de un sistema informático es necesario realizar un tratamiento de los riesgos, donde se identifique y se genere controles a los riesgos con las medidas pertinentes para corregir, modificar o eliminar todas aquellas vulnerabilidades que un sistema pueda tener.[46]

Es aquí donde le sistema de gestión de la seguridad de la información toma un rol muy importante para darle sentido a la seguridad, porque una vez identificado los riesgos este sistema de gestión tiene como finalidad diseñar un plan de choque, unos controles muy específicos de la mano de políticas bien definidas para que se pueda tener resultado óptimos, siempre mediante un ciclo que es indispensable, ya que una vulnerabilidad no siempre puede superarse en una primera etapa, se deben realizar varias tareas en función del tiempo para poderlas corregir.

---

[46]. Calder, Alan. ISO27001/ISO27002: una Guía de Bolsillo, IT Governance Ltd, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255172. Pag 52

Es aquí donde la relación costo-beneficio entra a figurar como un concepto importante, ya que, si un riesgo no está importante o al menos su impacto no es de consideración, y realizar una corrección cueste demasiado, lo será necesario corregir el error.

Como sabemos que el sistema de gestión es cíclico, es necesario tener claro el concepto del PHVA, que es el planificar, Hacer, Validar y Actuar, a continuación, la siguiente Cuadro aclara el tema.

Cuadro 7. Proceso PHVA en sistemas de Gestión.

Relación de modelo PHVA con el SGSI.	
Proceso PHVA	**Descripción del proceso**
Planificar: Se trata de elaborar los objetivos, metas, logros y políticas elaborando planes claros y alcanzables.	En este proceso se establecen los planes para ejecutar las SGSI. Se elabora las políticas, objetivos y metas.
Hacer: La puesta en marcha de lo planificado, alcances y consecuencias, costos, planes piloto, buscar mejoras de trazadas.	En esta etapa se comienza a realizar los planes antes trasados para la consecución de la SGSI, con objetivos reales y alcanzables.
Verificar: Se trata de controlar, medir y auditar, cada objetivo propuesto y confirmar si están cumpliendo con lo pactado inicialmente.	En esta etapa se trata de hacer un seguimiento, auditoria y veeduría de los objetivos ya ejecutados en el SGSI, mejorando los planes que no se ajustan a la realidad y se proponen nuevas rutas de planeación, el objetivo es corregir las desviaciones de los planes propuestos.
Actuar: Se busca mejorar el desempeño de los procesos y corregir las desviaciones, es decir perfeccionar el	Es la etapa de maduración, donde se ven los resultados y se mantienen los procesos

modelo planeado, para encontrar mejores resultados, también se debe mantener los procesos que funcionan bien.	que funcionen bien en el SGSI, y corregir lo que no sirve para mejorar el proceso.[47]

Luego de todo este proceso que parece complejo y extenso, pero que en realidad no lo es, y que es necesario implementarlo, se va descubriendo que este sistema es una herramienta muy importante para la seguridad informática, así poder estar siempre con el concepto de la continuidad del negocio al día.

Por lo tanto, es necesario monitorizar, documentar y actualizar constantemente el SGSI y sus planes de manejo de la seguridad, mantener durante todo el ciclo de vida de un sistema este proceso le permite que en tapas posteriores le den al sistema una madurez y solides que diferencie a otros sistemas de los que continúan bajo las buenas prácticas del desarrollo del software.

El éxito de toda organización a nivel informático es el de mantener un correcto plan de SGSI siempre funcional y actualizado.

4.11. COSTOS EN LA SEGURIDAD INFORMÁTICA.

A continuación, se resumen algunos de interese sobre los costos en SI.

- Se espera que el mercado de la seguridad informática crezca un 9% para 2019.
- Las principales compañías se cuidan mucho del malware.
- Para una empresa el costo para recuperar los datos de un cliente oscila los 300 dólares y entre más clientes, el costo de la perdida es más grande.[48]

---

[47]. Calder, Alan. Nueve Pasos para El éxito: Una Visión de Conjunto para la Aplicación de la ISO 27001:2013, IT Governance Ltd, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255165.

[48]. Osman, Maddy. 7 tipos de amenazas informáticas que toda pyme debe saber, [Consulta: 13 mayo 2019] https://es.godaddy.com/blog/7-tipos-de-amenazas-informaticas-que-toda-pyme-debe-saber/Para

- Comercios electrónicos, el activo denominado datos de usuario representa el 43% total de su empresa.
- Una cifra escandalosa es decir que en 2021 se gastarán 6 trillones de dólares en ataques informáticos exitosos.
- Equifax por un simple error de seguridad perdió 4 millones de dólares por ataques informáticos.

4.11.1. Ransomware

- A pesar de que muchas empresas atacadas tenían protección activa, más de 4000 ataques fueron efectivos por ransomware.
- Para el año 2019 el costo de ataques por ransomware llegará a los 12 millones de dólares.
- Se estima que para el año 2019 este ataque se realizará cada 14 segundos.
- Los ataques son más frecuentes es a través de los e-mails, Personal sin experiencia.

4.11.2. Phishing.

- EL mayor riesgo de la empresa es la pesca de usuarios, ataque que se ubica con el 56% de recurrencia.
- En el 76% de la empresa que reportaron ataque a su seguridad informáticas, presentaban ataque de phishing.
- El 30% de los usuarios no puede evitar abrir correos sin verificar, y el 12% les dan clic a links no seguros.
- Kaspersky's ha manifestado 246,231,645 tentativas de phishing en el 2017, y demostró un crecimiento de 91 millones con relación al 2016.[49]

---

[49]. Ciberataques que matan empresas, Diario el País, Bogotá, [Consulta: 25 mayo 2019] recuperado de: https://elpais.com/economia/2020/02/14/actualidad/1581694252_444804.html

5. PONIENDO A PRUEBA LA SEGURIDAD EL MVC.

Se define como la arquitectura madura de programación, que aparta los datos y la lógica de una aplicación web de su maquetación y con un módulo que tramita los eventos y las conexiones. Entonces MVC plantea la cimentación de tres componentes diferentes que son el **modelo**, la **vista** y el **controlador**, es decir, por un lado, define unidades para la representación de la información, y también para la acción del cliente. Esta arquitectura de programación está basa en reutiliza el código y la división de conceptos, su objetivo es buscar abrir la puerta a la seguridad, facilitando el desarrollo de aplicaciones web y su futuro mantenimiento.[50]

El modelo MVC tiene su evaluación en maquetaciones cliente-servidor con conceptos básicos que la programación que ve el cliente es distinta a la programación de servidor, y el concepto de un controlador nace de la necesidad de utilizar varias veces el código.

Trygve Reenskaug maduro la idea de una web personal durante su visita a Xerox Parc en los años 70, sin embargo, Jim Althoff y otros implementaron una versión aun incompleta de MVC, pero con sus características básicas, para la biblioteca del Smalltalk-80. Ya en el 1988, MVC se expresó una programación más refinada, y sobre todo fortalecida, actualmente es un modelo de arquitectura muy utilizado que está maduro y es muy robusto a la vez que versátil.[51]

Inicialmente no se tenía claro el concepto, ya que el controlador hacia la entrada de los datos y la vista la salida de ellos, pero era básicamente cómo funcionan en general las paginas tradicionales.

---

[50]. Estadísticas de seguridad informática, [Consulta: 20 mayo 2019] https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

[51].El modelo vista, el pasado y el presente, traducción, controlador MVC, [Consulta: 20 mayo 2019] https://pdfs.semanticscholar.org/ff2a/da602c96499c0f8a634e26c2c58ef8ec490f.pdf

Sin embargo, luego se definió al controlador como la programación encargada de conmutar datos, dividirlos, controlarlos, revisarlos todo esto con la reutilización del código, de tal forma que los datos de la vista nunca entran directamente al modelo sin ser filtrados antes, de ahí su seguridad.

Desde el 2000 el controlador, es un módulo de código que sirve como un intermediario de la comunicación entre el modelo y la vista, y agrupa la admisión, trayendo llamadas directas o el cliente para desacoplar la conexión entre ellos.[52]

Los modelos actuales del concepto de arquitectura del MVC, han cambiado y se hain ido adaptando a las necesidades actuales dando algunos resultados como.

- HMVC (MVC Jerárquico)
- MVA (Modelo-Vista-Adaptador)
- MVP (Modelo-Vista-Presentador)
- MVVM (Modelo-Vista Vista-Modelo).

De manera genérica, los componentes de MVC se podrían definir como sigue:

- **El Modelo:** es la maquetación del modelo en donde interactúan los usuarios, por lo tanto, tramita todos los accesos a dicha información, tanto las consultas como consultas nuevas de datos, se encarga de hacer el Loguin y permite hacer una escala de privilegios para el acceso de usuarios. Genera respuesta a las consultas que se hacen a través de las vistas. Todas las peticiones de acceso y consulta pasan por el controlador sin excepción.
- **El Controlador** está dispuesto para verificar las consultas que el modelo responde a la vista, la mayoría de ellas están usadas en las conexiones a las bases de datos, como modificar, eliminar o borrar una consulta.

[52.] Modelo Vista Controlador, Microsoft, [Consulta: 20 mayo 2019] http://msdn.microsoft.com/en-us/library/ff649643.aspx»

También se encarga de modelar el maquetado, es decir que está diseñado u optimizado para funcionar en distintos dispositivos, tanto en tamaño como en navegadores, por tanto, es así que no hay otra definición que el controlador es el intermediario entre el modelo y la vista.

- **La vista** es la presentación del modelo su maquetación que es lo que el usuario ve y sirve como plataforma para que se generen las consultas que necesite hacer.[53]

5.1. INTERACCIÓN CON LOS COMPONENTES MVC.

A continuación, se presenta la descripción de la interacción de los componentes del modelo:

1. Comienza cuando un cliente hace un acceso al portal web y genera una consulta.

2. El controlador recibe una consulta, desde la vista del cliente, este gestiona el evento y obtiene una respuesta en el modelo que luego presenta en la vista.

3. El controlador entra al modelo, actualiza las consultas, probablemente modificándolo de forma apropiada a la operación pedida por el cliente, como cuando aumentamos el número de artículos de una compra. Los controladores avanzados están casi siempre arreglados usando un esquema de comando que agrupa las acciones y simplifica procesamiento.

4. El controlador encarga tareas a los objetos de las vistas, está a su vez recibe los datos del modelo donde el usuario recibe la respuesta a una consulta, por ejemplo, puede visualizar un listado de compra, el modelo jamás se entrera de las consultas en la vista.

---

[53]. Modelo Vista Controlador -MVC, universidad de Alicante. [Consulta: 28 mayo 2019] https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html

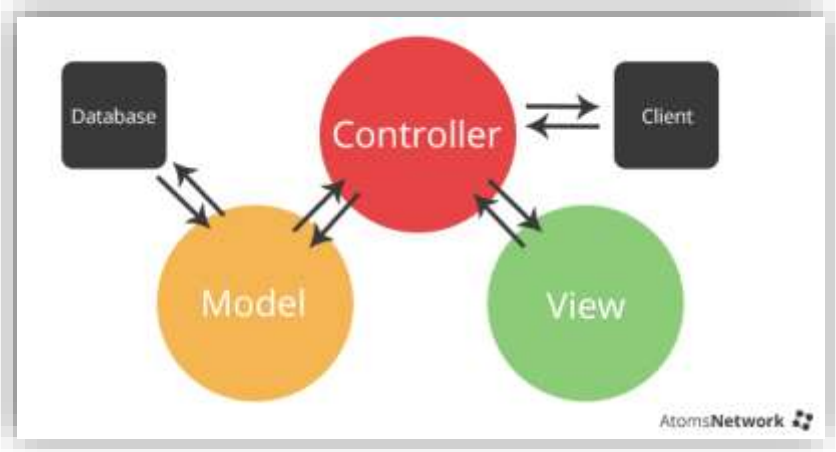
Sin embargo, el controlador es quien hace el proceso de entrega de información, así notifica los cambios que el modelo le presenta y este a su vez a las vistas. Un objeto vista consigue inspeccionar con el modelo y esperar a las consultas, y aunque todo esto pasa en la aplicación el modelo jamás se entera de las consultas de las vistas.

5. En los aplicativos webs convencionales no es posible generar esa independencia pues carecen del controlador, los hackers conociendo esa debilidad muchas veces la vulneran. Por lo general cuando entrega una respuesta a una consulta la vista tampoco esta se entera de los datos del modelo, el controlador solo actualiza los campos usados.[54]

6. La vista esta presta a recibir nuevas consultas, para que el ciclo se repita las veces que se necesite o hasta que el proceso se cierre.

5.2. ARQUITECTURA MODELO VISTA CONTROLADOR.

Figura 7 Modelo Vista Controlador.



Fuente: 21 https://seguridad.cicese.mx/dutic/23/Porque-utilizar-Modelo-Vista-Controlador-(MVC)-en-tus-proyectos

[54].Modelo vista controlador, Marco de desarrollo de la junta de Andalucía, [Consulta: 29 mayo 2019] http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/122

5.2.1. Uso en aplicaciones web.

El concepto MVC fue pensado para aplicaciones de escritorio, ha sido generosamente acomodado como arquitectura para delinear y efectuar aplicaciones web en los importantes lenguajes de programación. Tiene multitud de plugin, comerciales y no comerciales, que efectúan este patrón; estos plugins donde se pueden hacer cantidad de modulaciones. Los primeros plugins MVC para programación web trazaban una orientación de usuario liviano en todas sus sistematizaciones, tanto de la vista, el modelo y el controlador incurrían en el servidor.

Desde ese punto de vista, el cliente hacia una petición de cualquier formulario al controlador y luego recibe de la vista con una página nueva y actualizada, pero como el proceso es tan rápido el cliente no lo nota; todos estos modelos están alojado en el servidor desde donde se completan cada una de las funciones.

Las tecnologías o pluligns que se usa son nuevas pero funcionales bajo el MVC como frameworks, JavaScriptMVC, Backbone, bootstrap o jQuery que funcionan como complementos.

5.2.2. Ventajas la arquitectura MVC.

Las principales ventajas que ofrece esta arquitectura son:

1. Alta seguridad al separar al modelo de la vista, a través de un controlador.
2. Es fácil detectar errores y corregirlos.
3. El proyecto puede ser adaptado y escalado según sea la necesidad.
4. Se puede agregar variedad de datos.

5.2.3. Desventajas de MVC.

Las principales desventajas que ofrece esta arquitectura son:

1. Una numerosa cantidad de archivos para su procesamiento.
2. Aprender esta arquitectura conlleva más tiempo que otros modelos.
3. Aunque es más seguro, el sistema es más complejo que otros.

5.2.4. Comparación de MVC con otros modelos.

Para la comparación del MVC con otros modelos, primero de deben describir algunos conceptos generales y conocer las características básicas de los otros modelos.

5.2.5. Conceptos Generales.

Los patrones: son las soluciones a los problemas más comunes en el desarrollo de programa de computador y otros espacios referentes al diseño de interacción.[51]

Patrones de arquitectura: Es un esquema estructural fundamental para los programas de computadora. Los patrones de construcción, nos permiten conservar un proyecto trasparente, dimensiónable, fácil de conservar y de probar.

Patrones de Diseño: Definen la maquetación de un diseño para su desarrollo, que nos brindan soluciones en estructura, clases y reutilización del código. Estos patrones de diseño aparecieron desde la década de los 70, al menos su concepto, con código estructural de programación para solucionar y maquetar problemas. Hoy es muy usado y difundo en muchos casos para el desarrollo en lenguaje de patrones.[55]

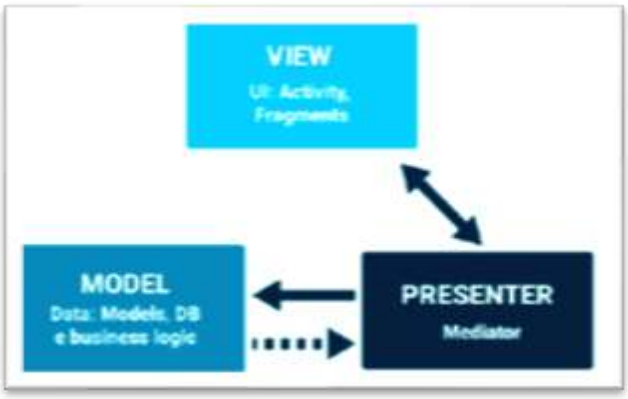
---

[55].Modelos de Interacción, Inaoep, México, [Consulta: 28 mayo 2019] https://ccc.inaoep.mx/~grodrig/Descargas/InteraPatternToCIC.pdf

5.2.6. Otros modelos.

El **modelo-vista-presentar** (**MVP**) es una forma de usar el MVC con la modificación de que la vista se convierte en un presentador, quien muestra los datos que recibe del modelo. Para entender este concepto el siguiente grafico nos hace entender el concepto.[56]

Figura 8 Capas del patrón MVC



Fuente: https://es.slideshare.net/alexmejicanos1/mvc-vs-mvp?from_action=save

5.2.7. Diferencias entre MVC Y MVP.

1. En el modelo MVC, la vista notifica las consultas que el modelo envía a través del controlador, por el contrario, el MVP la vista no conoce nada de consultas solo recibe datos y los presenta.

2. La vista del modelo MVC, tiende a manejar una programación de acceso y en captar lo que el cliente está solicitando, en MVP la vista no contiene programación que valide solo sirve para salida de datos.

3. La lógica del MVC está en el modelo y la vista, mientras que en el MVP la lógica la realiza solo el presentador.

---

56. Morales Ítalo, Que son y para qué sirven los patrones de diseño, [Consulta: 19 Junio 2019] https://platzi.com/blog/patrones-de-diseno/

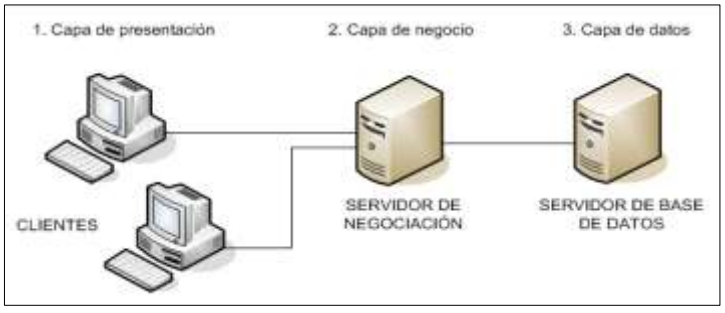
5.2.8. Modelo arquitectura por capas.

Esta programación es un diseño cliente -servidor, donde los contenidos se filtran por capas, sin embargo, carecen de control, de este modo las capas pueden llegar a presentar información con errores.[57]

Los sistemas abiertos poseen este tipo de arquitectura, pero el generar muchas capas puede producir una sobrecarga y posterior caída del sistema, sin embargo, cuando el trabajo no es a gran escala la funcionalidad es óptima y si se presenta un error se estudia al sistema no por completo sino la capa comprometida. Este tipo de diseño permite que los usuarios al igual que su programación puedan tener niveles y de esta forma solo utilizar las capas que le competen, no se entera lo que sucede en otros niveles esto se conoce como API.[58]

Actualmente el diseño por capas es altamente difundido por el mundo, lo que permite, su facilidad en uso, al ser escalable puede modularizarse por capas de acuerdo, a las necesidades de una empresa, el esquema de tres capas es el más usado, pero carece de controlador, por lo que la seguridad debe usarse con otras restricciones.

Figura 9 Modelo de N-Capas



Fuente: https://es.slideshare.net/alexmejicanos1/mvc-vs-mvp?from_action=save

_____

[57]. Arquitectura en Capas, RjCode Advance, [Consulta: 12 junio 2019] https://rjcodeadvance.com/patrones-de-software-arquitectura-en-capas-analisis-completo-ejemplo-ddd-parte-5/

[58]. Que son las API y para qué sirven, [Consulta: 12 junio 2019] https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces.

5.2.9. Comparación modelo MVC y modelo n – capas.

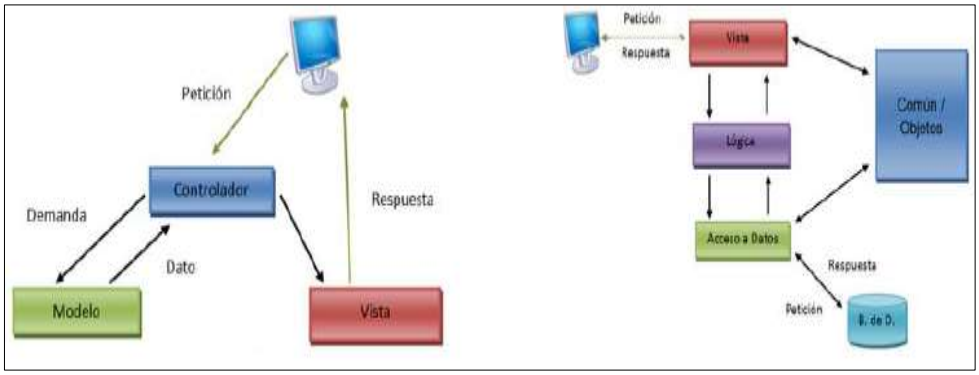
Como ya hemos hablado el MVC es un modelo de capas pero que tiene de diferente es que una de esas capas funciona como controlador de las consultas y de la conexión entre las otras capas.[59]

Por otro lado, la programación de n-capas que está basado en programar de manera independiente cada sección de un programa global, es decir que este hecho de forma modular, lo cual facilita al programador su diseño pues es fácil de entender, además su mantenimiento no es complejo ya que se busca las capas que tienen problemas y se resuelve el asunto.

Se trabaja mucho con diagramas de clase, para facilitar su desarrollo, esto mismo está en el MVC, pero en la sección del modelo, mientras que, a su vez, el controlador que desarrolla toda la lógica, en el modelo de N-capas, este proceso se hace en las reglas de negocio que una capa que se ha desarrollado para tal fin.[60]

Modelo MVC **Modelo N-Capas**

Figura 10. Comparativa de Modelos MVC/ N-Capas



Fuentes: https://es.slideshare.net/alejandrouhu/mvc-vs-pnc-1-revaluacion

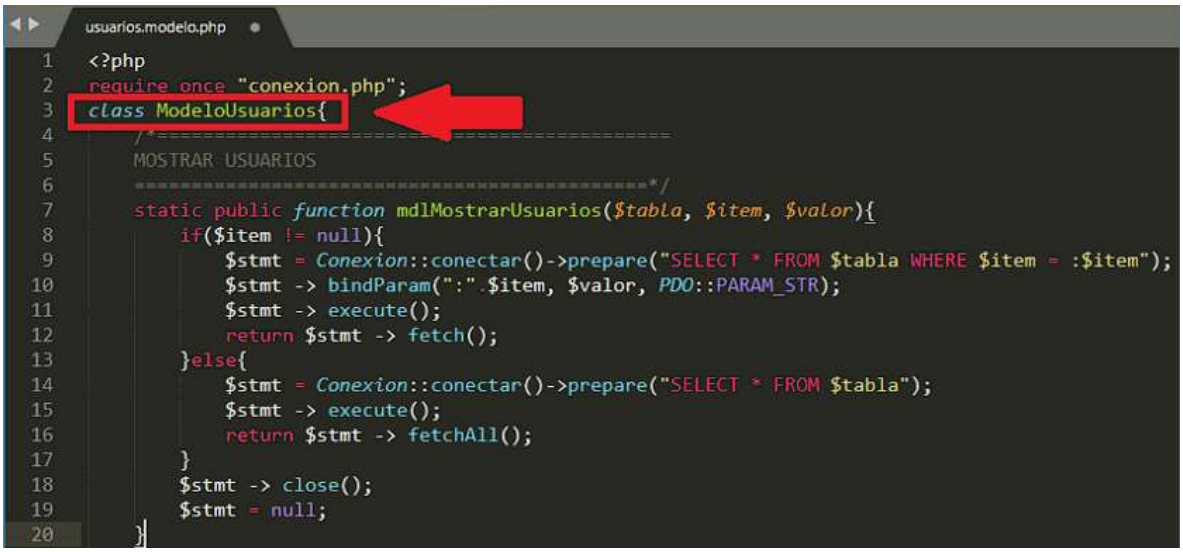
[59]. Introducción al modelo MVC y de N Capas, [Consulta: 12 junio 2019] http://albeverry.blogspot.com/

[60].Implementación del Modelo Vista Controlador (MVC) con Struts 2 [Consulta: 12 junio 2019] https://www.qualitrain.com.mx/implementacion-del-modelo-vista-controlador-mvc-con-struts2-ctfrm02/

5.3. IMPLEMENTACIÓN DEL MODELO MVC.

En este modelo se visualiza o se entienda fácilmente que tiene 3 capas y cada una de ellas su función. Sin embargo, en la realidad del código puede llegar a ser complejo, ya que no es fácil identificar donde empieza y donde termina. Como en los accesos a base de datos y el controlador de encarga de esta consulta, pero es necesario que los datos estén asilados en base de datos.[61]

Figura 11. código Php del Modelo en MVC.



Fuente: Elaboración Propia.

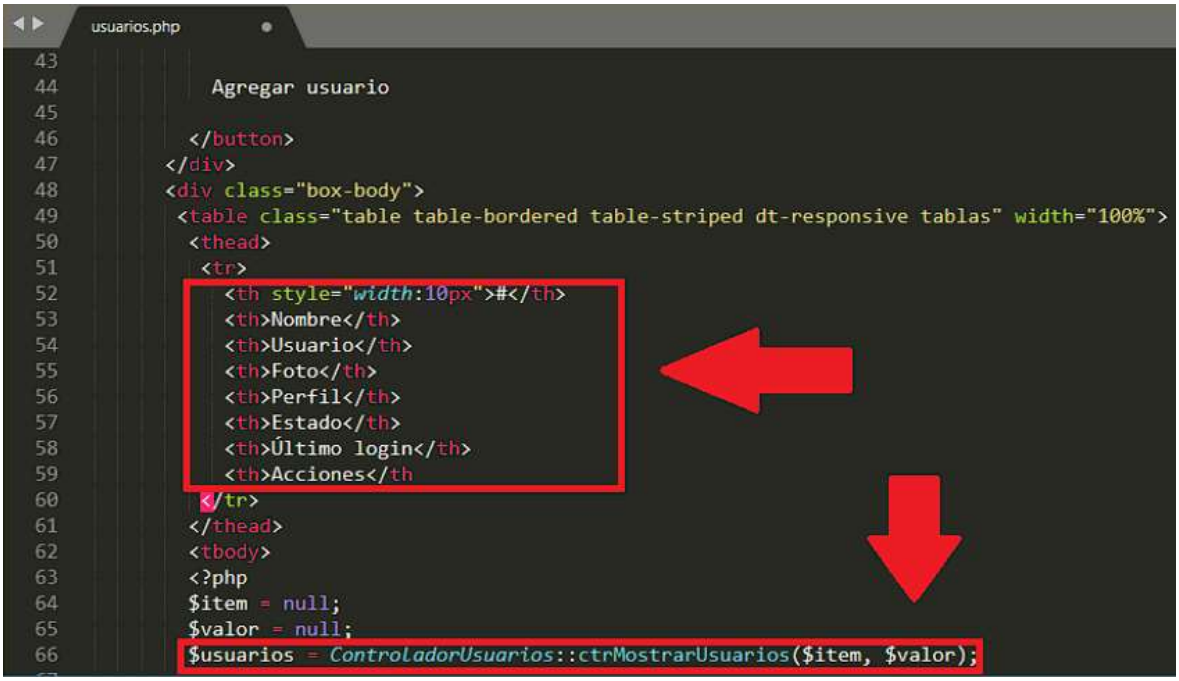
Como podemos ver en la Figura 11, el código nos muestra una sección de la capa modelo, donde el usuario puede ser consultado, aquí el modelo va hacer una consulta al controlador, pero no a la base de datos, ya que es el controlador quien realiza dicho proceso y le devuelve una respuesta lógica un proceso matemático o una respuesta a su consulta.

---

[61]. Upton, David, and Jose Argudo Blanco. CodeIgniter 1.7: Improve your PHP Coding Productivity with the Free Compact Open-Source MVC CodeIgniter Framework, Packt Publishing, Limited, 2009. ProQuest Ebook, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=946937. Pag 62.

Otra de las capas de esta arquitectura es la Vista, esta capa tiene como función interactuar con el cliente, es lo se le va a mostrar visualmente, conta del diseño que recibe y muestra las consultas que hace el cliente, pero jamás hace consultas o procesos, puesto que su labor es solo mostrar y recibir no está encargado de procesar, consultar o calcular, etc.[62]

Figura 12. Código de la capa Vista en MVC.



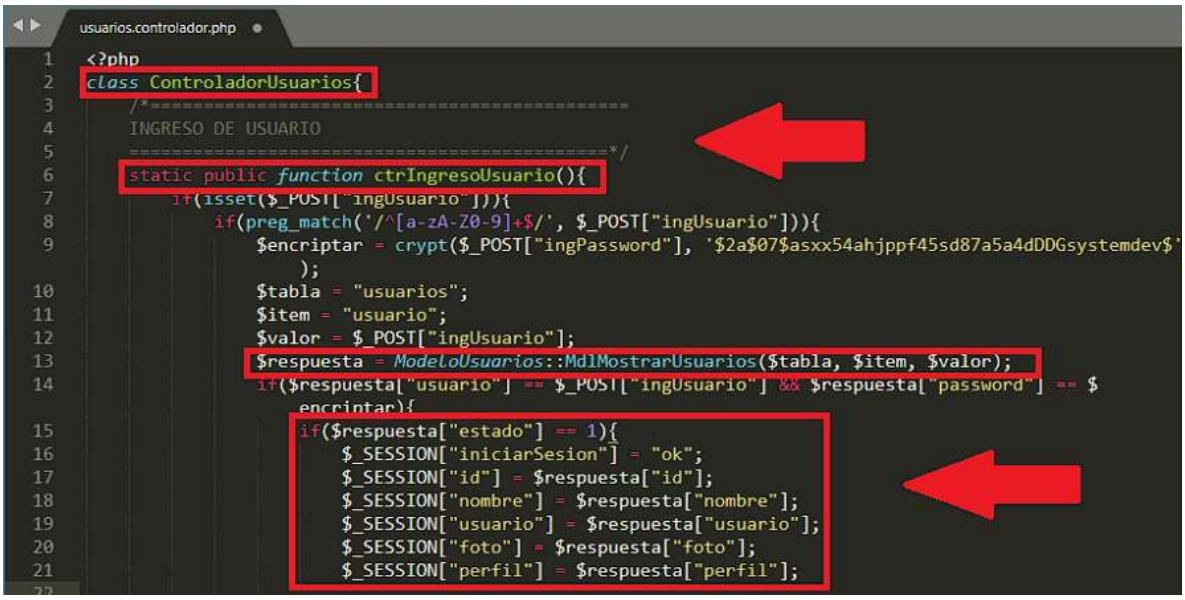
Fuente: Elaboración propia.

En la figura 12, podemos observar la capa vista y el código nos muestra cómo funciona esta capa que es donde, se le presenta a un usuario, en este caso un Loguin de acceso, la información y el diseño necesario para que interactúe y haga una consulta. En la última línea se puede apreciar que el modelo vista convoca al modelo controlador para que este se encargue de las tareas de procesos.

62. Upton, David, and Jose Argudo Blanco. CodeIgniter 1.7: Improve your PHP Coding Productivity with the Free Compact Open-Source MVC CodeIgniter Framework, Packt Publishing, Limited, 2009. ProQuest Ebook, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=946937. Pag 65.

La otra capa en este modelo es el controlador, que tiene varias funciones y es una de las más importantes que es la de recibir las llamadas de la vista, conecta archivos importantes como los diseños del CSS, procesando las consultas que un usuario realice a través de la capa vista.[63]

Figura 13. Código PhP de la capa Controlador en MVC.



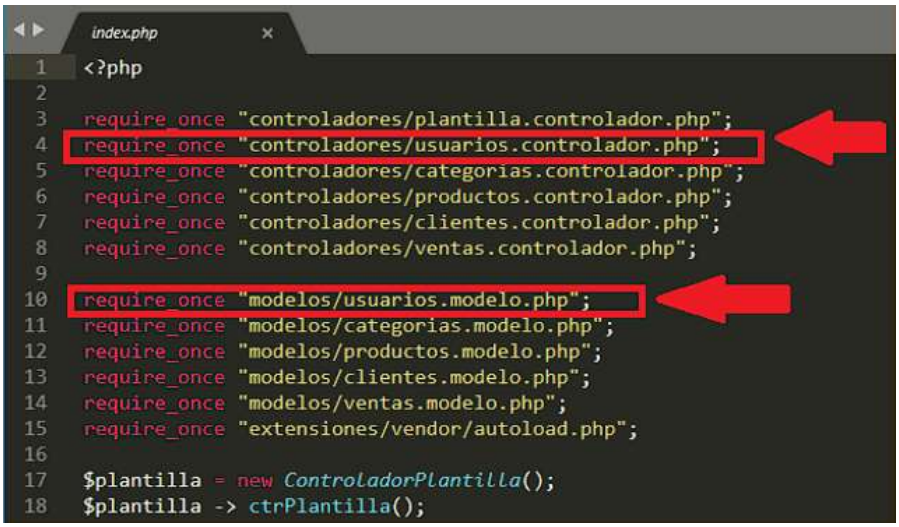
Fuente: Elaboración Propia.

Como podemos ver en la figura 13. La capa llamada controlador realiza varios procesos importantes, en este caso en específico el controlador está encargado de permitir el acceso de un usuario y validar que se logue de manera correcta, adicionalmente verifica que las credenciales de acceso son las correctas y su función no termina ahí, también envía los datos, compara y modifica la información del usuario directamente a la base de datos, las contraseñas nuevas las almacena encriptadas para mayor seguridad. De este modo queda claro que el controlador realiza las funciones importantes de programación.

[63]. Upton, David, and Jose Argudo Blanco. CodeIgniter 1.7: Improve your PHP Coding Productivity with the Free Compact Open-Source MVC CodeIgniter Framework, Packt Publishing, Limited, 2009. ProQuest Ebook, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=946937. Pag 66.

El archivo de indexación está diseñado como un repositorio para convocar tanto al controlador como al modelo, con el objetivo de darle fluidez al proceso, aunque es un archivo especial, este hace parte de la capa modelo, que es la que da forma tanto estética como funcional de la arquitectura MVC.

Figura 14. Índex en MVC.



Fuente: Elaboración propia.

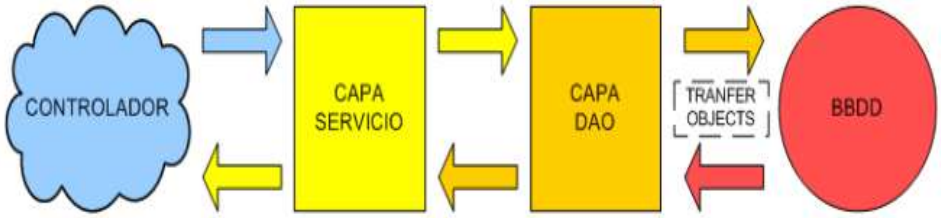
La forma en la que se hace la conexión al en el MVC es a través de un archivo de conexión que tiene como labor enlazar las consultas y las bases de datos como vemos en la figura 15. Este simple código hace la conexión y hace parte de la capa controlador.

Figura 15. Conexión a la base de Datos en MVC.

Fuente: Elaboración propia.

Sin embargo, cuando tenemos la práctica y todo funciona de acuerdo a la teoría, el controlador hará su trabajo y el modelo y la vista jamás tendrán interacción, y es ahí donde se vuelve necesaria asilar las capas para evitar inconvenientes. Este modelo está basado en el patrón DAO y la podemos en la subsiguiente imagen:

Figura 16. Patrón DAO object Data Base.



Fuente: https://es.slideshare.net/alejandrouhu/mvc-vs-pnc-1-revaluacion

5.3.1. Patron dao (object data base).

Este modelo tiene varias capas, una de ellas es la DAO, que se encarga del acceso y consulta a las bases de datos, como lo hace el controlador en el MVC. Y al asociarla a entidades de base de datos, hay muchas formas de manipular las consultas. Pero con la salvedad de que no controla lo que hace solo lo ejecuta, por lo que no es tan segura.[64]

El patrón DTO son los datos trasportados que simulan una trasformación de un objeto a una Cuadro de base de datos. Similar al controlador que es el encargado de llevar a cabo este cometido. En la capa de servicio se aloja la lógica de negocio de las funcionalidades que forman parte del uso de la base de datos y que en cualquier instante el controlador puede requerir. De esta forma el DAO solo hace la consulta, pero jamás controla lo que está haciendo, el proceso es más rápido, pero no es muy seguro.

[64]. Objeto de Acceso de Datos. [Consulta: 12 abril 2019]: http://siul02.si.ehu.es/~alfredo/iso/06Patrones.pdf

Esta arquitectura también se basa en capas, pero para obtener un resultado de una consulta primero debe consultar las entidades en el modelo de programa.[65]

Por otro lado, la MVC, nos mostrará la información formateada y ordenada, es el resultado de todo lo que el modelo interaccione con los datos, este lo muestra mediante la interfaz de usuario, habitualmente llamado la capa de presentación.

En PHP la maquetación esta modularizada con funciones envidas en una sola página, que el modelo reutiliza para rescatar la información de la petición realizada, luego se forma un objeto con las clases que a su vez realiza un llamado al método lista para almacenarlo en arreglos de variables. El modelo entonces debe generar una estructura de directorios en donde almacenará la información que el programa necesita, de esta forma se comprende bien el funcionamiento del modelo MVC, de lo contrario se vuelve complejo y difícil de entender. El controlador también realiza la conexión a la base de datos y es entonces donde se debe crear una clase maestra para el resto de clases que hereden de ella una respuesta, de esa forma mejorara más el código.

6. LOS RIESGOS, VULNERABILIDADES Y AMENAZAS DEL MVC.

Es indispensable que todos los sistemas antes de su puesta en marcha se le realicen pruebas tanto funcionales como de seguridad, para lo cual es necesario contar con un plan de manejo para los riesgos y vulnerabilidades y es ahí donde los estándares de calidad ISO/IEC 27001 juegan un papel fundamental para hacer este tipo de sondeos, para poner en contexto esta situación se presentan las siguientes evidencias de un testeo de penetración al modelo MVC.

---

[65]. TÍTULO DEL TFC: Prototipo de aplicación para la gestión de facturación TITULACIÓN: Enginyeria Técnica de Telecomunicaciones, especialidad en Telemática AUTORES: Luis alcalde Solani llaIvan Fontanals Pérez DIRECTOR: Roc Mesaguer Pallarès [15 de octubre de 2009] pág. 145

6.1. TESTEO DE SEGURIDAD-PENTESTING.

Para poder comprender la madurez y nivel de seguridad es necesario de forma práctica hacer un testeo para poder entender las vulnerabilidades de una aplicación web basada en el modelo vista controlador, para esto es necesario valerse de las herramientas diseñadas para este fin, una de las distribuciones de Linux denominada Kali Linux tiene un compendio de estas aplicaciones.

Kali Linux es una distribución de Linux que es conocida como un sistema operativo para el ataque de sistemas y con estas herramientas podemos hacer ataques basados en el top 10 de los ataques más importantes en el OWASP, cuyo objetivo en específico es poder determinar los riesgos que se presentan en los sistemas concerniente a su seguridad.

Para comenzar a realizar un ataque de seguridad a una aplicación web es necesario recabar toda la información posible para de esta forma realizar un buen ataque. KaliLinux dentro de sus herremientas de ataque a sistemas tiene la posibilidad de realizar instrucciones especificas, entre las que podemos obtener datos de posibles vulnerabilidades que luego permiten desarrollar un plan para explotar esas fisuras de seguridad y convertilas en potenciles riesgos.[66]

Un comando de ejecucción propio para consultar un dominio de una apliación web es el comando whois, que esta envebida en el propio sistema opertativos que permite hacer un rastreo de la información desde un sitio de alojamiento.[67]

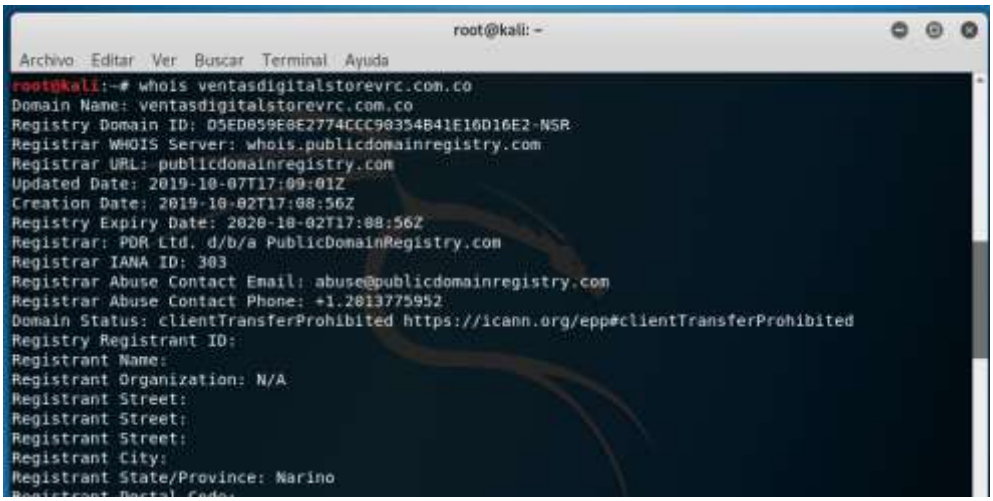
---

66. Pritchett, Willie, and Smet, David De. KaliLinux Cookbook, Packt Publishing, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1389391. Pag 49

67. Información de comando. Madrid, [Consulta: 18 junio 2019] https://www.sysprovider.es/blog/tips-rapidos-usar-comando-whois-linux/#:~:text=Whois%20es%20un%20comando%20que,net%20.

Entonces así se determina el nombre exacto del dominio, su ID, fecha de publicación, región o país desde donde se presta el servicio de alojamiento y otros datos más que puedan ser públicos, estos ya permiten empezar a entender ante quien se realiza el ataque.

Figura 17. Comando Whois muestra información web

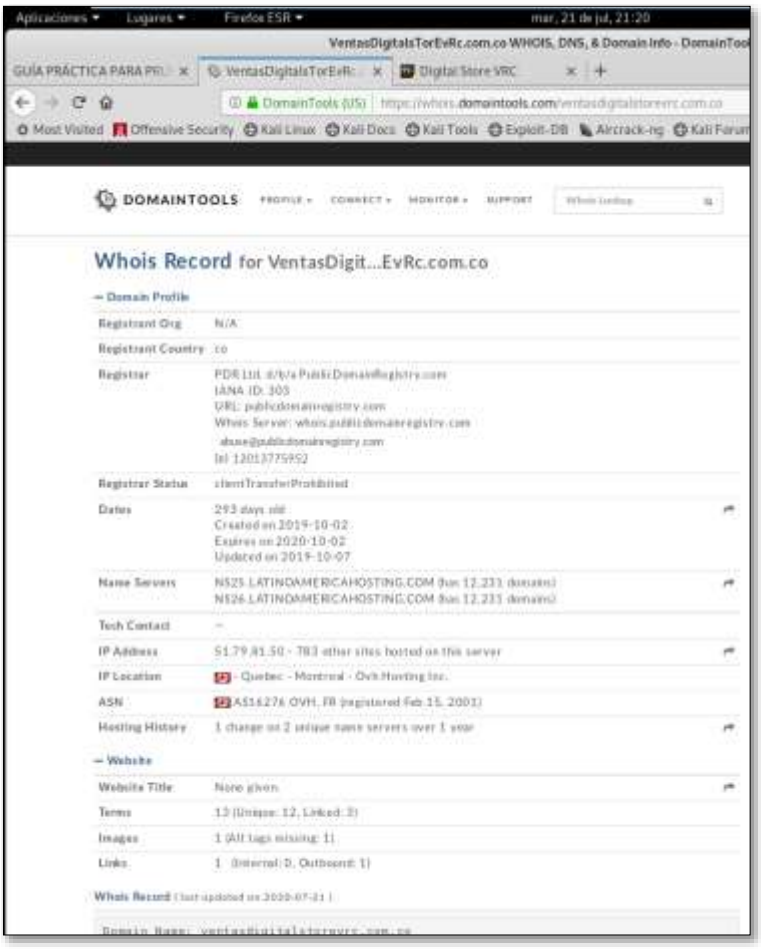


Fuente: Elaboración propia.

Existen otras vías para realizar la misma operación y así poder obtener estos datos que son sensibles para el dueño del contenido, por ejemplo, se pude hacer la misma consulta desde una página en internet que ejecuta el mismo comando con la salvedad de que lo hace en línea, esto demuestra que esta información es publica y que, aunque el servidor que presta el dominio a la aplicación web al tratar de ocultarlo, no es posible ya que mediante esta herramienta la información es fácilmente recuperable.

A continuación, en la siguiente Figura (11) se puede apreciar que la información de un aplicativo web en funcionamiento, ya que esta alojada en un servidor y mediante una página en línea denominada Domaintools, se puede ejecutar el mismo comando de Kalilinux y confirmamos que los datos son los mismos. Con esta información como partida podemos ir tomando un camino claro con un plan de ataque para vulnerar sus debilidades.

Figura 18. Datos del Dominio obtenidos en línea



Fuente: elaboración propia.

Otra aplicación que tiene la capacidad de examinar una red, su transmisión de los paquetes de datos que a través de esta y en general toda la información que pudieran transitar y que con esto se puede hacer un análisis de datos suficientemente grande como para determinar varias vulnerabilidades, esta técnica se denomina hombre en el medio (MitM), cuyo ataque hace referencia a la interceptación de información.[68]

68. Khawaja, Gus. Practical Web Penetration Testing: Secure Web Applications Using Burp Suite, Nmap, Metasploit, and More, Packt Publishing, Limited, 2018. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5436572. Pag. 95

Nikto es una herramienta, que puede realizar ataques o búsquedas de datos por fuerza bruta. Con el objetivo de capturar los datos, este proceso se denomina escuchar una red de datos. [69]

Figura 19. Nikto Herramienta para obtener datos en la red

Fuente: Elaboración propia.

6.1.1. Lectura del Host.

Una de las funcionalidades de nikto es tener la capacidad de leer un host y obtener datos importantes como el tipo de seguridad, el tipo de servidor, el lenguaje de programación del aplicativo que el servidor está alojando, la base de datos que está usando dicha aplicación, también describe si el servidor usa cookies, que pueden representar una puerta de entrada para atacar la aplicación.

Por otro lado, esta herramienta menciona algunas de las protecciones que el servidor posee y las que le pudieran faltar.

[69]. Pauli, Josh. The Basics of Web Hacking: Tools and Techniques to Attack the Web, Elsevier Science & Technology Books, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1222592. Pag 103.

Esto representa para un atacante la información básica pero muy valiosa para poder tomar un plan de ataque y poder vulnerar el sistema que en este caso sería una aplicación web.

Figura 20. Ataque al Servidor

Fuente: Elaboración propia.

Conociendo que la información de un servidor no es completamente oculta y que es fácil descubrir para cualquier persona con conocimientos básicos de informática, es necesario subir las líneas de defensa no solo en un buen servidor, sino que la elección de una buena metodología de programación como la arquitectura son vitales para un correcto funcionamiento, es por ello que el modelo MVC representa una gran ventaja a la hora de ofrecer seguridad.

Figura 21. Detalles de lectura la Servidor

Fuente: elaboración propia.

6.1.2. Interceptación de Datos MITM.

Otra aplicación para ataques a los sistemas es las Suite Burp, que tiene muchas funcionalidades y esta encamina a descubrir las vulnerabilidades de una aplicativo que puede escuchar a través de ataques MitM.[70]

Figura 22. Herramienta Burp Suite para ataques MitM

Fuente: elaboración propia.

Esta herramienta tiene la capacidad de interceptar la información que esta entre el cliente y el servidor, está configurado para trabajar en un puerto proxy que usualmente es el 8080 y desde este puesto escucha la red y sustrae los datos, y está en la capacidad de hacer ataques a las bases de datos, encontrar el árbol de contenido de una aplicación, verificar vulnerabilidades y hacer ataques ofensivos.

Figura 23. Configuración proxy para escuchar con Burp.

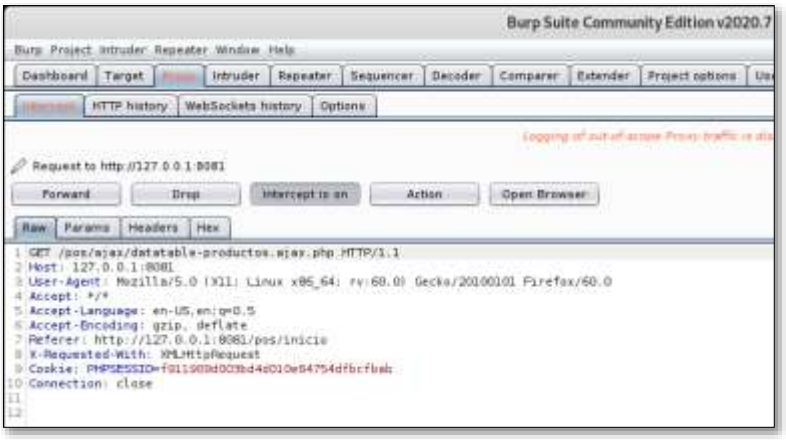
Fuente: elaboración propia.

[70].Dalziel, Henry, and Henry Dalziel. How to Attack and Defend Your Website, edited by Alejandro Caceres, Elsevier Science & Technology Books, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1888757. Pag 4

Inicialmente Burp suite debe ser configurado de tal forma que pueda escuchar una transmisión de datos entre el usuario y el servidor; la información no siempre se presenta de forma clara, es ahí donde se tiene que interpretar lo que la suite presenta, cuando se intercepta dicha información.[71]

Burp suite busca las vulnerabilidades, presenta información como las cookies que pueden ser una entrada fácil para atacar a través de algún medio como un backdoor, aumento en las credenciales de autenticación, copia de la base de datos, entre otros ataques.

Figura 24. Interceptación de datos en BurpSuite



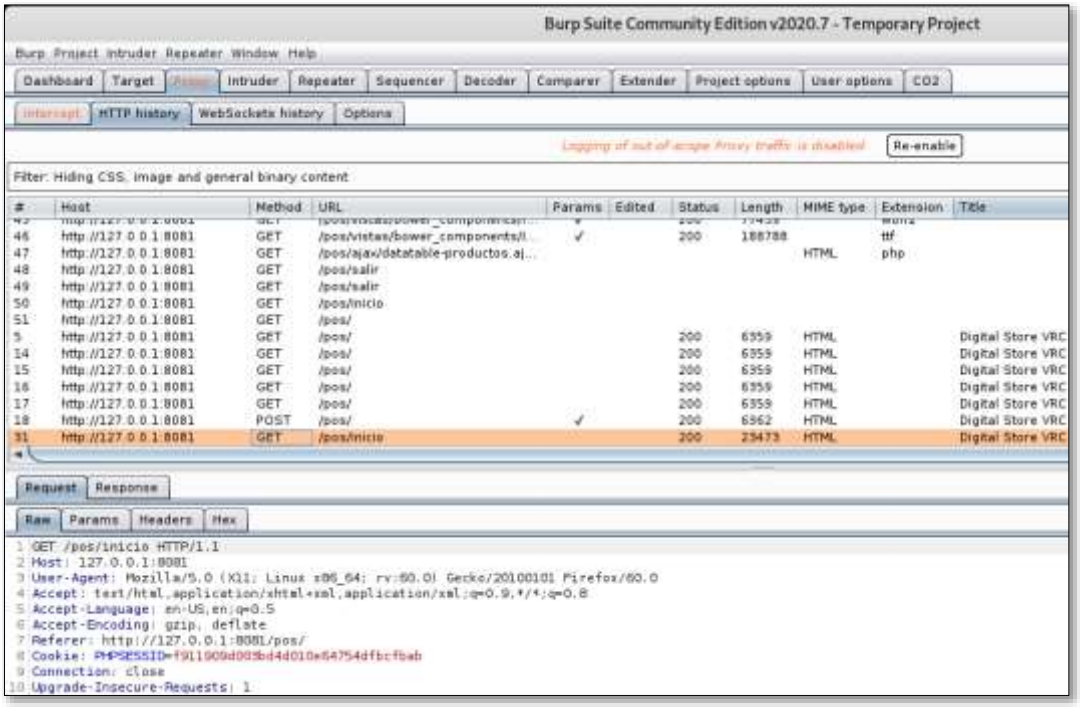
Fuente: Elaboración propia.

Una de las formas en que se hace un ataque es tratar saltar la seguridad de un usuario y contraseña para poder acceder con un perfil de usuario de nivel administrador, así acceder a la información sensible. Primeramente, se buscan los directorios que constituyen a la aplicación web como tal, para determinar mediante el mapa del sitio, con esta información podemos saber específicamente desde que lugar se logue cada usuario y modificar así la forma de acceso, existe un ataque denominado elevación de privilegios que consiste en no poder acceder, sino que además puede tener el nivel de acceso de administrador.

[71].Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. Web Penetration Testing with Kali Linux: Explore the Methods and Tools of Ethical Hacking with Kali Linux, 3rd Edition, Publishing 2018. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5314613. Pag 58.

Con estos privilegios se pueden hacer muchos daños a nivel del aplicativo, asi como secuestrar información, o simplemente modificar una base de datos, para evitar todos estos tipo de incidentes el movdelo vista controlador tiene como objetivo garantizar que estas vulnerabilidades esten seguras.

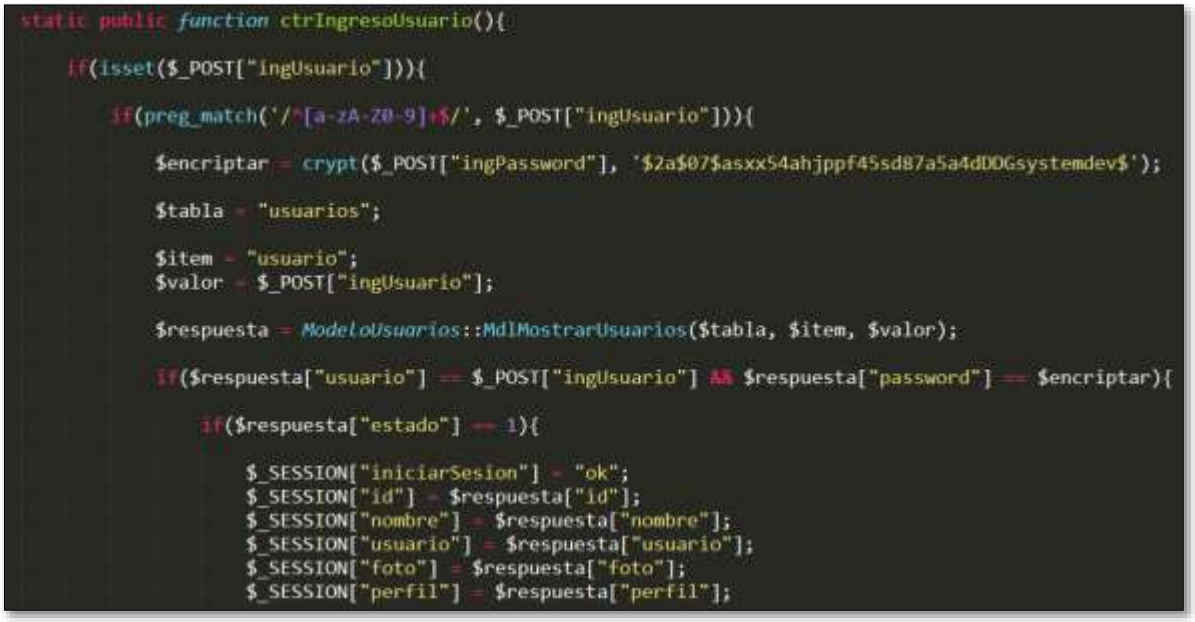
Figura 25. Mapa del sitio – interceptación



Fuente: elaboración propia.

Es en este punto donde la arquitectura MVC entrega una serie de fortalezas que son importantes para que estos riesgos de seguridad no sean capitalizados a favor de instrusos. Entre las opciones más notorias es manejar capaz de seguridad, para que cuando alguien haga una consulta GET, el contrador procese la información sin que esta ingrese a la base de datos o al modelo que es donde esta la informacion sencible, tambien un punto a favor de la seguirdad es que cada contraseña de los usuarios que administran el aplicativo se puede cifrar con comandos basicos en lengiajes PhP, Visual Studio, HTML con la salvedad de que se este manejando dicha arquitectura de seguridad -MVC.

Figura 26. Encriptación de contraseña de usuario.



```php
static public function ctrIngresoUsuario(){

    if(isset($_POST["ingUsuario"])){

        if(preg_match('/^[a-zA-Z0-9]+$/', $_POST["ingUsuario"])){

            $encriptar = crypt($_POST["ingPassword"], '$2a$07$asxx54ahjppf45sd87a5a4dDDGsystemdev$');

            $tabla = "usuarios";

            $item = "usuario";
            $valor = $_POST["ingUsuario"];

            $respuesta = ModeloUsuarios::MdlMostrarUsuarios($tabla, $item, $valor);

            if($respuesta["usuario"] == $_POST["ingUsuario"] && $respuesta["password"] == $encriptar){

                if($respuesta["estado"] == 1){

                    $_SESSION["iniciarSesion"] = "ok";
                    $_SESSION["id"] = $respuesta["id"];
                    $_SESSION["nombre"] = $respuesta["nombre"];
                    $_SESSION["usuario"] = $respuesta["usuario"];
                    $_SESSION["foto"] = $respuesta["foto"];
                    $_SESSION["perfil"] = $respuesta["perfil"];
```

Fuente: elaboración propia.

El proceso es relativamente sencillo, se crea una variable por ejemplo $encriptar y al mismo tiempo se valida las entradas de los caracteres que conforman la contraseña, de este modo se asegura que cuando el administrador cree un nuevo usuario y le asigna o cree una contraseña esta ya no va a ser visible, sino que va estar encriptada y lo único que recibiría un intruso que haga un ataque MITM en la consulta, en lugar de recibir una palabra o contraseña va a obtener una fila de caracteres que no tiene un sentido lógico, sino que son caracteres que el comando crypt pone de manera aleatoria y solo este comando puede desencriptar estos datos, como se aprecia en la Figura 26.

Esta información se aloja en la base de datos, esto garantiza que el proceso sea completamente seguro, ya que esta está estructurada como una capa más de la arquitectura.[72]

[72].Safronov, Mark, and Jeffrey Winesett. Web Application Development with Yii 2 and PHP, Packt Publishing, Limited, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1800650.

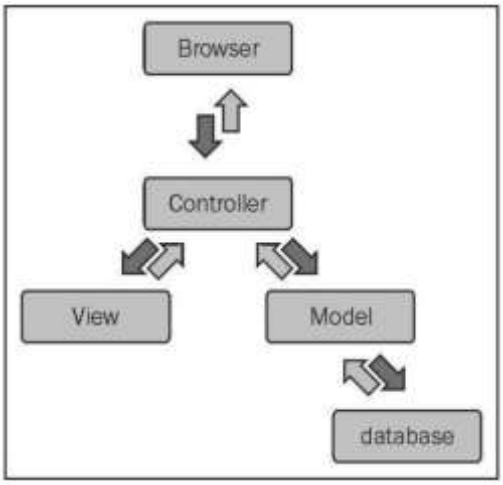
Dentro de las base de datos el comando hace que almacene no la contraseña sino el codigo de encriptación, entoces cuando un intruso despues de saltar todas las capas de seguridad esta en la capacidad de hacer una copia de la base de datos, las contraseñas estarán encriptadas y no podra saber con precion la contraseña. En la ilustracion 27.

Figura 27. Código de encriptación en la base de datos.

Fuente: Elaboración propia.

En la arquitectura MVC la base de datos se la trabaja como otra capa de seguridad que no puede ser consultada por el usuario, ya que el controlador hace las consultas a traves del modelo.

Figura 28. Data base en MVC

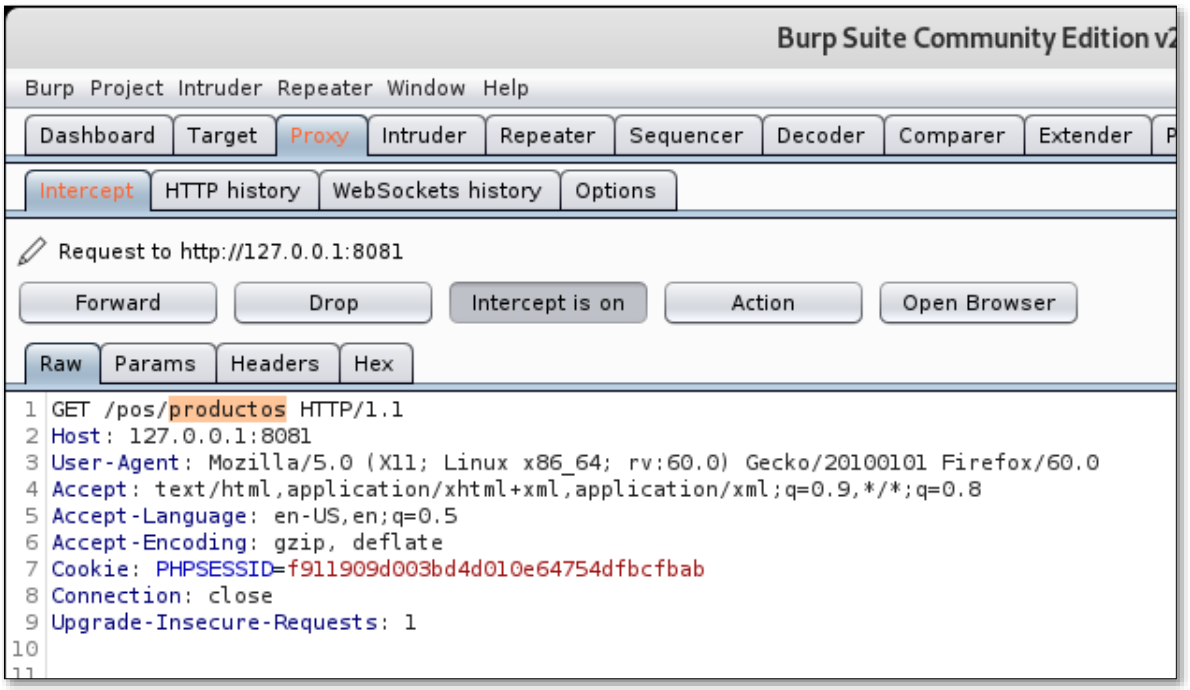


Fuente: Improve your PhP coding MVC. Pag55.

6.1.3. Secuestro de Sesión.

La arquitectura MVC esta pensada en robusteser la seguiridad incluso en las variables de sesión donde se busca esconder la forma la comunicación con el servidor; como sabemos las cokies estan diseñadas para llevar al cliente cierta inforamción que le permite al servidor elaborar un perfil y poder así determinar algunas de las preferencias de navegacion.

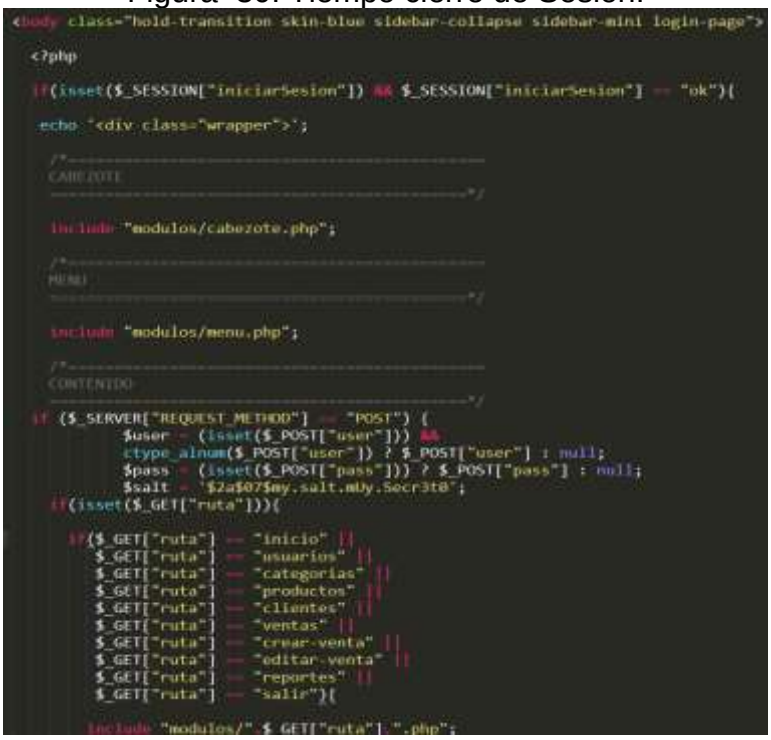
Figura 29. Cookies usuario-servidor.



Fuente: Elaboración propia.

Se hace entonces indispensable que las variables de sección que generan cookies sean seguras y no representen un problema de seguridad en un futuro, por ello que lo mejor es realizar dos cosas de forma simultánea para que brindar seguridad, la primera es que las cookies que se generen estén encriptadas y no puedan ser leídas por el cliente o intruso que pudiera usar algún backdoor, lo segundo sería poner tiempo límite de inactividad, para que la sesión se cierre automáticamente. La Figura 29, muestra una cookie su encriptación de seguridad.

Figura 30. Tiempo cierre de Sesión.



```
<body class="hold-transition skin-blue sidebar-collapse sidebar-mini login-page">

<?php

if(isset($_SESSION["iniciarSesion"]) && $_SESSION["iniciarSesion"] == "ok"){

echo '<div class="wrapper">';

/*=============================================
CABEZOTE
=============================================*/

include "modulos/cabezote.php";

/*=============================================
MENU
=============================================*/

include "modulos/menu.php";

/*=============================================
CONTENIDO
=============================================*/

if ($_SERVER["REQUEST_METHOD"] == "POST") {
        $user = (isset($_POST["user"])) &&
        ctype_alnum($_POST["user"]) ? $_POST["user"] : null;
        $pass = (isset($_POST["pass"])) ? $_POST["pass"] : null;
        $salt = '$2a$07$my.salt.mUy.Secr3t0';
if(isset($_GET["ruta"])){

  if($_GET["ruta"] == "inicio" ||
     $_GET["ruta"] == "usuarios" ||
     $_GET["ruta"] == "categorias" ||
     $_GET["ruta"] == "productos" ||
     $_GET["ruta"] == "clientes" ||
     $_GET["ruta"] == "ventas" ||
     $_GET["ruta"] == "crear-venta" ||
     $_GET["ruta"] == "editar-venta" ||
     $_GET["ruta"] == "reportes" ||
     $_GET["ruta"] == "salir"){

    include "modulos/" . $_GET["ruta"] . ".php";
```

Fuente: Elaboración propia.

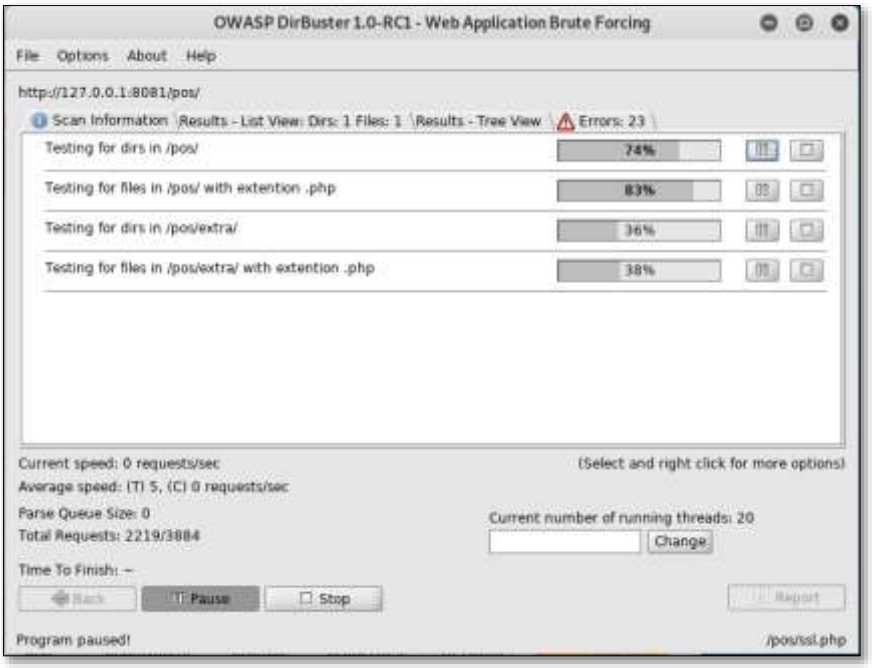
Dentro de la programación corresponde hacer una verificación de usuario, es decir que para que pueda navegar libremente por la aplicación web, un usuario si se autentico correctamente, entonces podrá navegar adecuadamente, de lo contrario por seguridad el sistema se cierra, y no permite navegar entre las páginas que son parte del directorio o estructura del aplicativo web, este tipo de seguridad permite que aunque un atacante o intruso a pesar de que pueda escuchar una transmisión cliente-servidor y conozca las rutas específicas de las paginas no podrá tener acceso a las misma porque la sesión se hará nula; esta verificación se la realiza en función del tiempo, periódicamente y constantemente se está mirando si las credenciales de acceso son correctas de lo contrario cierra la sesión, lo mismo que al no detectar actividad un usuario o cuando hay una intrusión de parte de un atacante que es expulsado al no tener verificación.[73]

[73].Upton, David, and José Argudo Blanco. *CodeIgniter 1.7: Improve your PHP Coding Productivity with the Free Compact Open-Source MVC CodeIgniter Framework,* Packt Publishing, Limited, 2009. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=946937.

6.1.4. Ataque de fuerza bruta.

Otro tipo de ataque es el denominado por fuerza bruta, donde existen muchas aplicaciones para realizar este tipo de ataques, uno de los más utilizados que se encuentra en la distro de Kali Linux es DirBuster que está basado en el top de ataques del OWASP.

Figura 31. Ataque de fuerza bruta.



Fuente: elaboración propia.

Esta aplicación esta específicamente diseñada para realizar un ataque de fuerza bruta sobre los directorios que componen la una aplicación web, esta funcionalidad que tiene esta herramienta permite determinar de forma muy preciosa el mapa del sitio, en aplicativos desarrollados en arquitecturas no convencionales se obtiene fácilmente información vital y se puede eventualmente hacer cambios y daños a nivel del sistema, sin embargo en la arquitectura MVC, esto no sucede y los testeos de fuerza bruta no permiten que exista este tipo de situaciones y los resultado siempre son negativos.[74]

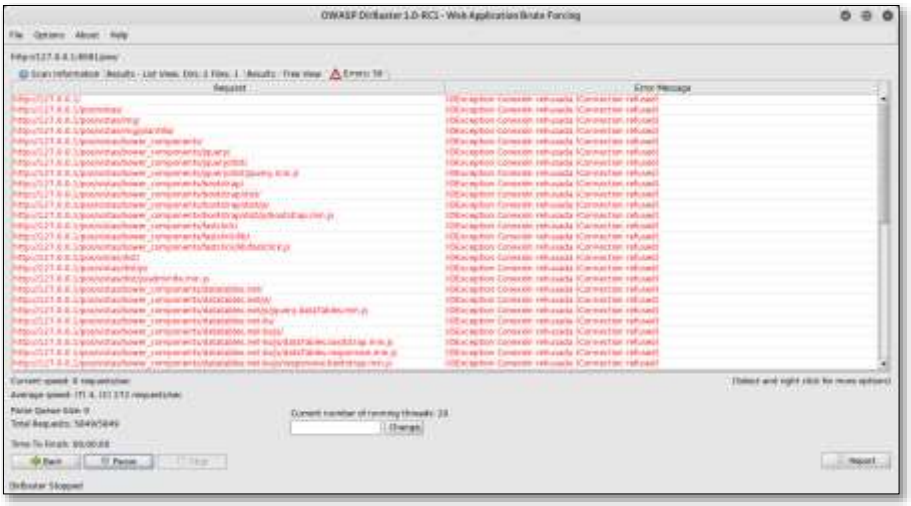
[74] Muniz, Joseph, and Aamir Lakhani. Web Penetration Testing with Kali Linux, Packt Publishing, Limited, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1420531. Pag 148

Figura 32. Análisis de DirBuster.

Fuente: Elaboración propia.

Al realizar un analisis de un sitio web con el aplicativos DirBuster sin embaro se obtienen informacion interesante del sitio y esto plantea que se debe tomar otro rumbo al analizar los resultados. En la Figura 26, se puede ver claramente que el ataque no obtuvo ningun resultado y todasl las conexiones que intento realizar fueron rechazadas, esto evidencia que el MVC es completamente seguro.[75]

Figura 33. DirBsuter sin resultados en MVC



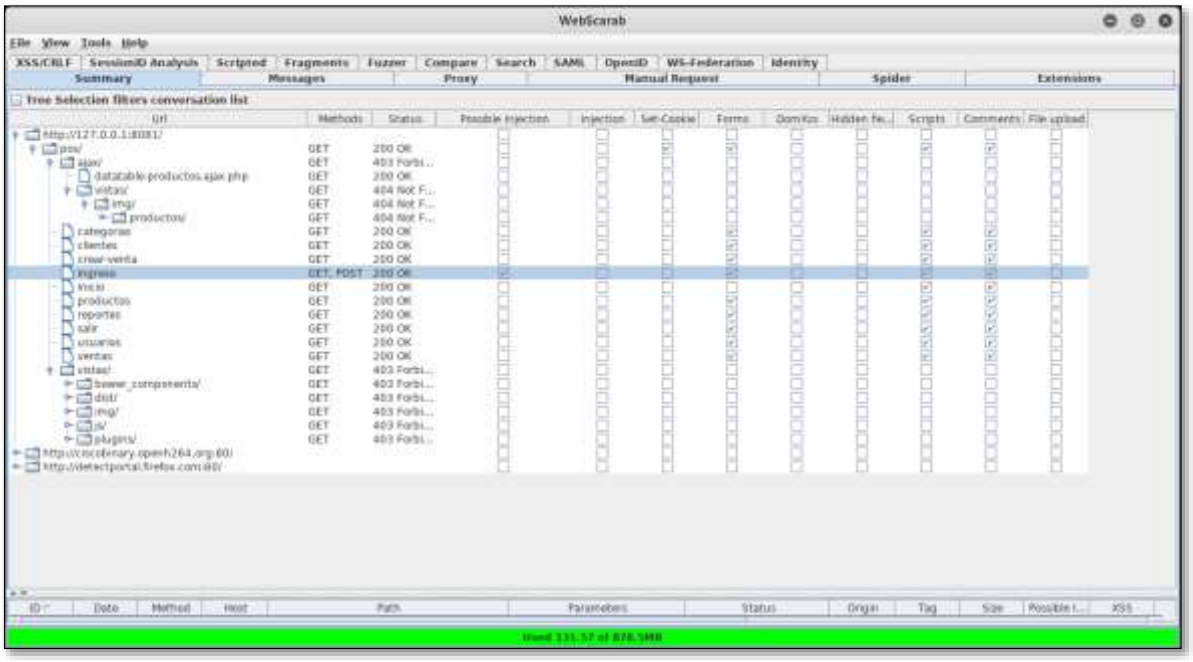
Fuente: Elaboración propia.

[75].Muniz, Joseph, and Aamir Lakhani. Web Penetration Testing with Kali Linux, Packt Publishing, Limited, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1420531.

6.1.5. Análisis de vulnerabilidades.

Ahora bien, no solo existen herramientas que permiten hacer ataques a sistemas web, también existen herramientas que permiten el análisis de las vulnerabilidades de un sistema, en este caso WebScarab, permite verificar a qué tipo de ataques son susceptibles cada página de un directorio web.

Figura 34. Análisis de Vulnerabilidades.



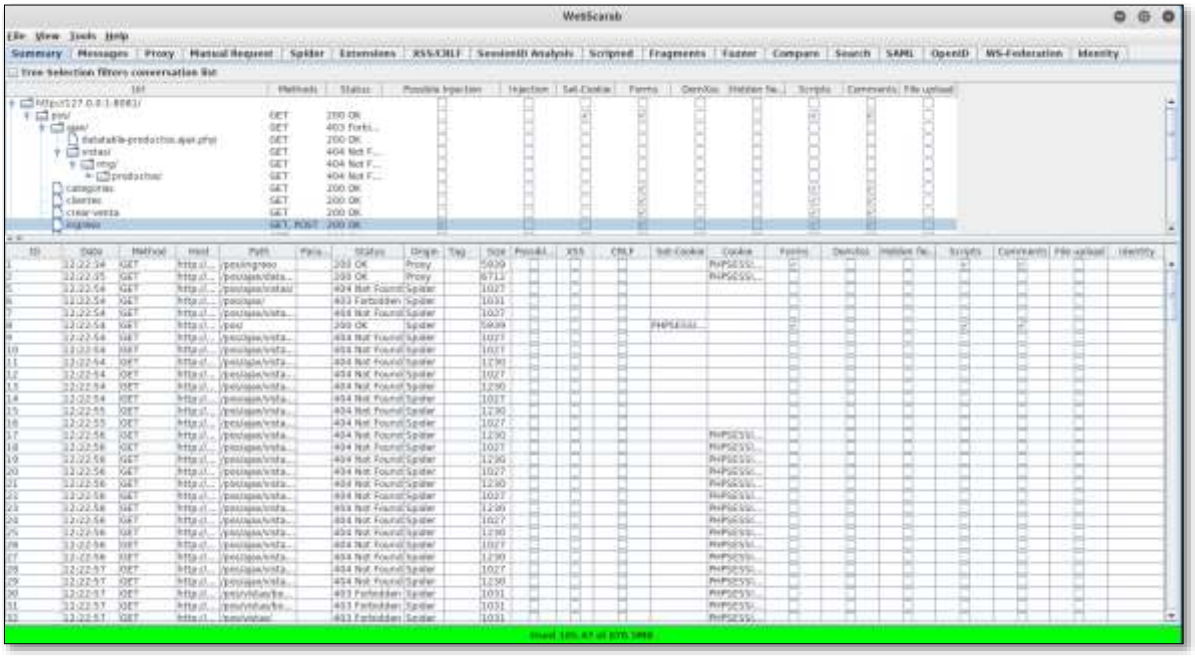
Fuente: elaboración propia.

Esta aplicación presenta un amplio abanico de posibilidades, ya que esta herramienta de forma automatizada comienza a evaluar los riesgos y presenta un análisis con los posibles ataques basados en el top 10 OWASP, esta es una de las alternativas que se toman como base para el mejoramiento de la seguridad.[76]

[76].Engebretson, Patrick. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, Elsevier Science & Technology Books, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1249222. Pag135-150

En el modelo vista controlador, este tipo de analisis permite observar que la programación por capas es muy segura y es por ello que muchos desarrolladores utilizan esta arquitectura por el diseño basado en capaz que repesenta alta segurirdad en todo momento.

Figura 35. Vulnerabilidades presentes en un aplicativo web.



Fuente: elaboración propia.

Figura 36. Detalles del análisis de vulnerabilidades.

ID	Date	Method	Host	Path	Para...	Status	Origin	Tag	Size	Possibl...	XSS
1	12:22:34	GET	http://...	/pos/ingreso		200 OK	Proxy		5939	☐	☐

CRLF	Set-Cookie	Cookie	Forms	DomXss	Hidden fie...	Scripts	Comments	File upload	Identity
☐		PHPSESSI...	☑	☐	☐	☑	☑	☐	

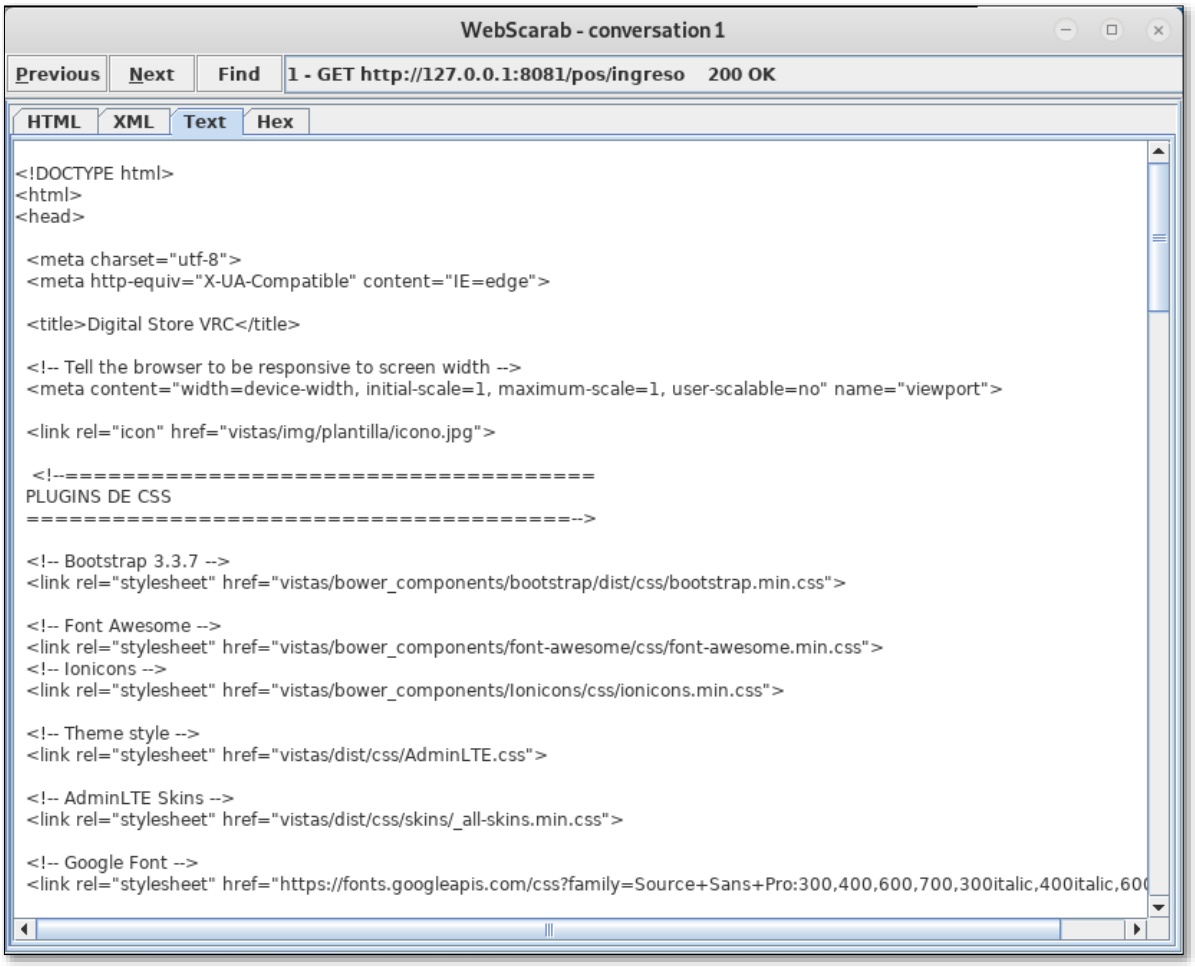
Fuente: Elaboración propia.

Esta aplicación muestra información detallada bajo un código de etiquetado que sus desarrolladores crearon y que es fácil de comprender cuando se trabaja con este programa, un código de estos es el 200, que significa que existen vulnerabilidades.[77]

[77]. Allen, Lee, et al. Kali Linux – Assuring Security by Penetration Testing: Assuring Security By Penetration Testing, Packt Publishing, Limited, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1572946.

Por último, el programa nos presenta un resumen de las líneas de código que alcanzo a tomar durante su acción, por ejemplo, presenta un resumen de la plantilla principal de un sitio web y sus posibles vulnerabilidades, esto nos da el indicio que puede haber una fisura de seguridad, la cual se debe mejorar.

Figura 37. Resumen del análisis.



Fuente: Elaboración propia.

Con todas estas revisiones de seguridad queda claro que la arquitectura MVC, es un modelo robusto y maduro, que permite el desarrollo seguro de aplicaciones web, que son la garantía de que todo va a funcionar según lo esperado.

7. CONTROLES DE SEGURIDAD EN EL MVC.

Una vez Determinadas las vulnerabilidades, debilidades, Amenazas y riesgos que se puedan presentar en el MVC, se debe generar un plan de acción o de choque que contrarreste los efectos adversos de tales situaciones, por ellos se debe plantear un sistema de gestión de la seguridad de la información SGSI.

7.1. POLÍTICAS DE SEGURIDAD EN MVC.

Una Política de seguridad hace referencia a una declaración o acto especifico que traza un plan que se debe cumplir, esto a través de una norma, metas, objeticos y procedimientos adaptables en general a un área específica. Las políticas generan un requerimiento de cumplimiento estricto que en el momento en que no se cumpla con tal objetivo, pueden dar como resultado una acción disciplinaria o una medida correctiva. El plan determina que es inminente la implementación del SGSI, que es una política de seguridad, en el que se establecen las normas y reglas que puedan certificar la confidencialidad, integridad y disponibilidad de la información en todos los procesos, por lo que es vital definirla, aplicarla y trasmitirla a los miembros de trabajo de la empresa.

Los objetivos de control y los controles se han obtenido directamente de los de la NTC-ISO/IEC 27001:2013, con la salvedad de que se usan los que son necesarios para la empresa y están alineados con ellos. Las listas de estas Cuadros, no son exhaustivas y la organización puede considerar que se necesitan objetivos de control que deba crear. Los objetivos de control y controles de estas Cuadros, se deben seleccionar como parte del proceso de implementación de la gestión de la seguridad SGSI.[78]

[78].Norma técnica colombiana NTC-ISO/IEC27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI), [Online], Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Cuadro 8. Políticas de Seguridad.

Políticas de Seguridad	
Política de seguridad de la información	
Objetivo: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.	
Documentos de las políticas de seguridad de la información.	**Control**
	La dirección debe aprobar un documento de políticas de seguridad de la información y lo debe comunicar y publicar a todos los empleados y partes externas pertinentes.
Se debe hacer Revisión de las políticas de seguridad de la información.	**Control**
	La política se debe revisar a intervalos planificados o cuando se producen cambios significativos, para certificar que sigue siendo apropiada, suficiente y eficaz.

Fuente: Elaboración propia.

Cuadro 9. Organización de la seguridad de la Información.

Organización de la seguridad de la información	
Procesar la autorización para los servicios de proceso de información.	**Control**
	Se debe definir e implementar un procesamiento de autorización de la dirección para nuevos servicios de proceso de información.
Acuerdos sobre confidencialidad.	**Control**
	Se deben asemejar y examinar con regularidad los requisitos de confidencialidad o los acuerdos de no-

		divulgación que reflejan las insuficiencias de la organización para el auxilio de la información.[79]
	Contacto con las autoridades.	**Control**
		Se deben conservar contactos convenientes con las autoridades pertinentes.
	Contacto con grupos de interés especiales	**Control**
		Se deben conservar los contactos apropiados con grupos de provecho especiales, otros foros especializados en seguridad de la información, y asociaciones de expertos.[80]
	Revisión independiente de la seguridad de la información.	**Control**
		La dirección de la organización para la gestión de la seguridad de la información y su ejecución (es decir, control, sus objetivos, políticas, procesos e instrucciones para seguridad de la información) se deben revisar independientemente a intervalos concebidos, o cuando ocurran cambios importantes en la implementación de la seguridad.[81]

Fuente: elaboración propia.

---

[79]. Muñoz, Víctor Belmar. Prevención de riesgo - Implantación de un sistema efectivo de control de riesgo, El Cid Editor | apuntes, 2009. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3180200.

[80]. Chicano, Tejada, Ester. Auditoría de seguridad informática (MF0487_3), IC Editorial, 2014. Recuperado de: ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184005.

[81].Gómez, Fernández, Luis, and Rivero, Pedro Pablo Fernández. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2015. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3430311.

Cuadro 10. Gestión de Activos.

Gestión de activos		
Responsabilidad en activos informáticos.		
Objetivo: conseguir y mantener la defensa adecuada de los activos organizacionales.		
	Inventario de activos	**Control**
		Todos los activos deben estar visiblemente identificados y se deben elaborar y conservar un inventario de todos los activos significativos.
	Propiedad de los activos	**Control**
		Toda la información y los activos agrupados con los servicios de procesamiento de información deben ser de una parte elegida de la organización
	Uso aceptable de los activos	**Control**
		Se deben nivelar, documentar y efectuar las reglas sobre el uso admisible de la información y de los activos asociados con los servicios de procesamiento de la información

Cuadro 11. Seguridad de los RRHH

Seguridad de los recursos humanos	
Selección	**Control**
	Se deben ejecutar estudios para la verificación de circunstancias de los candidatos a ser empleados, contratistas o beneficiarios de terceras partes, de acuerdo con las ordenanzas, la ética y las leyes oportunas, y deben ser proporcionales a las exigencias del negocio, la clasificación de la información a la cual se va a tener acceso y los peligros divisados
	Control

Términos y condiciones laborales.	Como parte de su compromiso convenido, los practicantes, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y situaciones de su contrato laboral, el cual debe establecer sus compromisos y las de la organización con relación a la seguridad de la información.

Cuadro 12. Seguridad física y del entorno.

Seguridad física y del entorno		
Áreas seguras		
Objetivo*:* impedir el acceso físico no autorizado, el perjuicio e interrupción a las instalaciones y a la información de la empresa		
	Perímetro de seguridad física.	**Control**
		Se deben manejar perímetros de seguridad (barreras tales como paredes, puertas de acceso intervenidas con tarjeta o mostradores de admisión atendidos) para proteger las áreas que sujetan información y servicios de procesamiento de información
	Controles de acceso físico.	**Control**
		Las áreas seguras deben estar resguardadas con controles de acceso adecuados para afirmar que sólo se permite el acceso a personal acreditado.
	Seguridad de departamentos, espacios e instalaciones.	**Control**
		Se debe delinear y destinar la seguridad física para oficinas, espacios e instalaciones.
	Protección frente a amenazas externas y ambientales.	**Control**
		Se deben diseñar y aplicar protecciones físicas contra daño por deflagración, inundación, terremoto,

		explosión, manifestaciones sociales y otras formas de desastre natural o artificial. [82]
	Trabajo en áreas seguras.	**Control**
		Se deben delinear y aplicar la protección física y las directrices para trabajar en áreas seguras.
	Áreas de carga, despacho y acceso público.	**Control**
		Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.[83]

7.1.1. Gestión del Continuidad del Negocio MVC.

Implementar un sistema de gestión de continuidad de negocio [SGCN]. Un sistema para administrar la continuidad se fundamenta en el ciclo de sistemas de gestión y mejora continua (PHVA) y define el conjunto de políticas, procesos, funciones y estructura que ayudan a establecer el marco de actuación bajo el cual se administra la continuidad. Tanto las políticas como los procesos de administración de la continuidad, son base fundamental para alcanzar un ambiente mejorado y dispuesto en organizaciones que buscan constantemente mantener y facilitar la continuidad de sus operaciones claves que son soporte del negocio.

---

[82]. Chicano, Tejada, Ester. Auditoría de seguridad informática (MF0487_3), IC Editorial, 2014. Recuperado de: ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184005.

[83].Gómez, Fernández, Luis, and Rivero, Pedro Pablo Fernández. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2015. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3430311.

Lograr mantener la continuidad del negocio es una habilidad que requiere la definición de un marco de referencia proactivo que facilite la alineación de las personas, los procesos, la tecnología y las actividades del día a día. El marco de referencia se establece mediante la implantación, adopción y cumplimiento de un sistema para administrar la continuidad, enmarcado en:

• Políticas para Administrar la Continuidad.
• Procesos para Administrar la Continuidad.
• Roles y Responsabilidades. (Cultura Segura).
• Plan de Pruebas.

Cuadro 13. Gestión de la Continuidad del Negocio.

<table>
<tr><th colspan="2">Gestión de la continuidad del negocio</th></tr>
<tr><td colspan="2">Temas de seguridad de la información, gestión y prolongación del negocio</td></tr>
<tr><td colspan="2">Objetivo: anular las interrupciones en las actividades del negocio y resguardar sus procesos críticos contra los efectos de fallas trascendentales en los sistemas de información o contra desastres, y certificar su recuperación oportuna.</td></tr>
<tr><td rowspan="2">Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.</td><td>Control</td></tr>
<tr><td>Se debe desarrollar y conservar un proceso de gestión para la continuidad del negocio</td></tr>
<tr><td rowspan="2">continuidad del negocio y valoración de riesgos.</td><td>Control</td></tr>
<tr><td>Se deben detectar los eventos que pueden originar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichos obstáculos, así como sus consecuencias para la seguridad de la información.</td></tr>
<tr><td></td><td>Control</td></tr>
</table>

Efectuar la documentación de planes de la seguridad el negocio.	Se deben desarrollar y efectuar reglas para mantener o rescatar las operaciones y asegurar la disponibilidad de la información en el valor y la escala de tiempo solicitados, después de la interrupción o la falla de los procesos perentorios para el negocio. [84]
Estructura para la planificación de la continuidad del negocio	**Control**
	Se debe conservar una sola distribución de los planes de continuidad del negocio, para asegurar que todos los planes sean sólidos, y considerar los requisitos de la seguridad de la información de forma estable, así como identificar las prioridades para pruebas y sustento. [85]
Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio.	**Control**
	Los planes de continuidad del negocio se deben someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia. [86]

_____

[84]. Pinson, Linda. Anatomía de un Plan de Negocio: Una Guía Gradual para Comenzar Inteligentemente, Levantar el Negocio y Asegurar el Futuro de su Compañía, Out Of Your Mind . . . And Into The Mark, 2011. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=828142.

[85.] Engemann, Kurt, and Doug Henderson. Business Continuity and Risk Management: Essentials of Organizational Resilience, Rothstein Associates, Incorporated, 2011. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=3400325.

[86].Costas, S. J. (2014). Seguridad informática. España: RA-MA Editorial. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11038505&tm=1456691628756

7.1.2. Políticas para administrar de la continuidad.

Las políticas referentes a las acciones y actividades que ayudan a mantener la continuidad deberán ser ampliadas en el sistema de gestión de continuidad – SGCN –a ser implementado por la organización. Estas políticas deberán estar definidas para cada una de las dimensiones que de alguna forma inciden o impactan la continuidad de las operaciones de los servicios y/o procesos críticos del negocio.

A continuación, se enuncian los componentes que deben de contener políticas que sirvan como base para establecer el programa de continuidad de negocio.

- Compromisos directivos y de participantes.
- Personas.
- Procesos de negocio.
- Instalaciones físicas.
- Infraestructura tecnológica.

7.1.3. Procesos de administración de la continuidad.

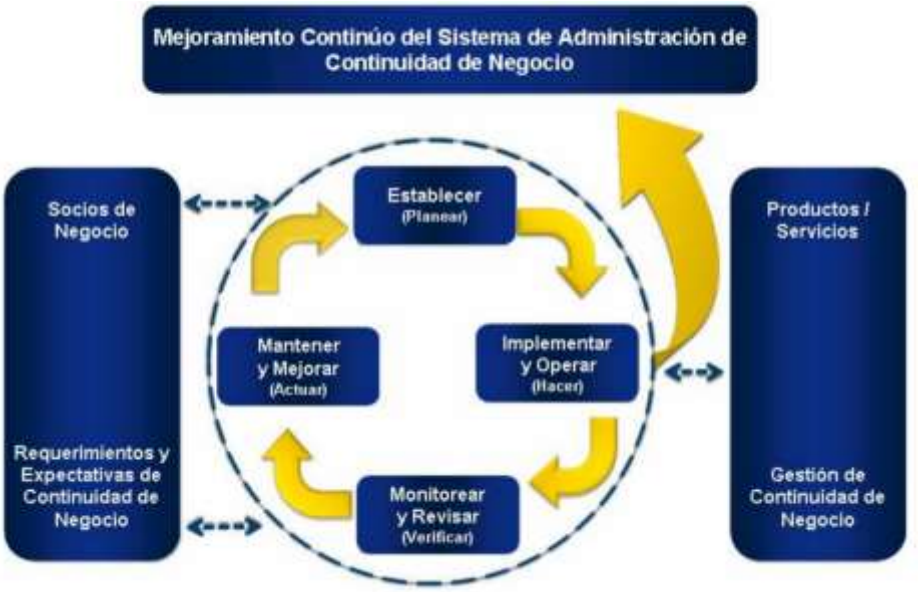
Los procesos de administración de la continuidad se definen como la gestión disciplinada de mejoramiento y monitoreo continuo con el fin de proporcionar niveles de continuidad acorde con las necesidades del negocio.[87]

Los procesos de administración de la continuidad se componen de cuatro fases basadas en el ciclo de sistemas de gestión de calidad, como ilustra la siguiente gráfica del marco de actuación del sistema de administración de la continuidad:

---

[87]. Pinson, Linda. Anatomía de un Plan de Negocio: Una Guía Gradual para Comenzar Inteligentemente, Levantar el Negocio y Asegurar el Futuro de su Compañía, Out Of Your Mind . . . And Into The Mark, 2011. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=828142. Pág 85

Figura 38. Ciclo Continuidad del Negocio.



Fuente: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625709/yarleque_ga.pdf?sequence=1&isAllowed=y

7.1.4. Roles y responsabilidades

Dadas las definiciones de las alternativas por parte de la organización, se debe proceder con la identificación de los participantes y dueños del sistema. Independientemente de la alternativa de estructura elegida por la organización, el equipo de continuidad es el encargado de definir las políticas de continuidad en todos sus aspectos (procesos, personas, tecnología e infraestructura física), participar en las definiciones de estrategias de continuidad a ser incorporadas en organización, advertir sobre riesgos que afectan la continuidad y motivar acciones de control que disminuyan el impacto de interrupciones, además de asesorar en los temas de continuidad. [88]

[88]. Gómez, V. Á. (2014). Gestión de incidentes de seguridad informática. Madrid, ES: RA-MA Editorial. Recuperado del repositorio de la universidad nacional abierta y a distancia UNAD, de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11046422&tm=1465232638601 pág. 60.

Este equipo, según las características de organización y los procesos del SGCN, podrá estar conformado por un líder de continuidad de negocio y de tres a seis analistas de continuidad, con fortalezas en los diferentes temas y dimensiones de continuidad (riesgos, impactos, procesos, cultura, tecnología, infraestructura física, proveedores); sin embargo, en la implementación del sistema de gestión de continuidad se determinará el número más adecuando de personas.

Los roles se describen a continuación: Líder del sistema de continuidad de negocio (LSCN) El Líder del Sistema Continuidad es el encargado de dirigir y liderar todas las actividades relacionadas con el Sistema de Gestión de Continuidad de Negocio (SGCN). 101 perfil: el líder del sistema de continuidad de negocios debe contar con experiencia certificada en temas de continuidad de negocio y debe tener conocimientos detallados de la metodología para gestión de continuidad de negocio implementada en organización.

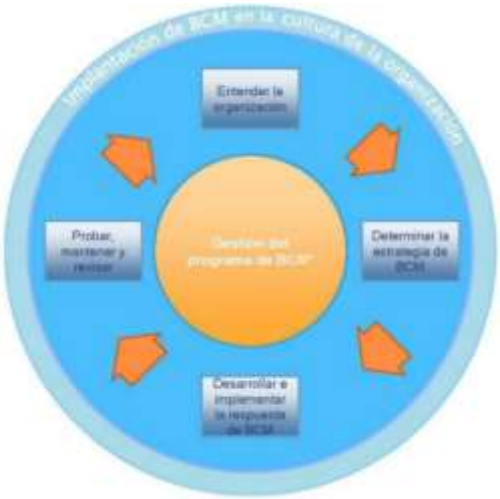
El rol requiere de habilidades administrativas y técnicas, comunicación intensa e información precisa sobre todos los aspectos de continuidad implementados en organización, contar con la visión integral del negocio y liderazgo en cada uno de los niveles de la organización.

7.1.5. Plan de pruebas

En las sesiones de Comité de Desarrollo Administrativo se aprobará y monitoreará el plan de continuidad; las acciones preventivas se llevarán a cabo en toda la entidad según la planificación de las dependencias de Talento Humano (relacionadas con las personas), de Administrativa (relacionadas con la infraestructura) y de Gestión Documental (relacionadas con la información), las cuales estarán coordinadas por la Secretaria General, la Oficina de Tecnologías de la Información y las Comunicaciones (lo relacionado con la infraestructura tecnológica y la seguridad de la información).

Durante la definición de la planificación se definirán y aprobarán los simulacros, interrupción del servicio, evacuación de emergencia o pruebas aleatorias del plan de continuidad, según los recursos económicos con los que se cuente en cada vigencia, los cuales se harán de manera planificada y concertada con el Comité de Crisis; de igual manera los resultados y el seguimiento se realizará dos veces al año ellos Comité Institucional de Desarrollo Administrativo y Directivos.[89]

Figura 39. Ciclo BCM



Fuente: recuperado de: ttps://www.fomentoacademico.gob.ec/wp-content/uploads/downloads/2013/08/plan_de_continuidad_de_negocios.pdf

Se tomará en cuenta el ciclo de vida de la continuidad del negocio descrito en la gráfica anterior, como referencia del procedimiento a seguir en temas de mantenimiento y actualización del Plan de Continuidad, además para tener éxito en integrar los principios de continuidad de negocio dentro de la organización se deberá tener definidas una serie de políticas y procedimientos.

[89]. Gestión de la Continuidad del Negocio", [Consulta: 1 agosto 2019] ttps://www.marblestation.com/?p=650

Todo esto deberá estar principalmente apoyado por:

- ✓ Liderazgo de la alta administración
- ✓ Definición de responsabilidades
- ✓ Creciente conocimiento
- ✓ Capacitación
- ✓ Ejercicios.

El potencial mantenimiento del Plan de Continuidad del Negocio se evaluará cada vez que existan modificaciones o cambios importantes en:

- Procesos,
- Estructura,
- Servicios,
- Proveedores,
- Unidades o líneas de negocios, Productos, etc.
- Eventos externos (ej. cambios en normativas o políticas financieras o de gobierno, desastres naturales, etc.), que afecten la continuidad del negocio.

Además, el mantenimiento del Plan de Continuidad se deberá realizar por las siguientes causas:

- Fase Crítica debido a cambios frecuentes en la institución tanto externos como internos
- Necesidad de estructurar un esquema de procedimientos para el mantenimiento del PCN
- Evaluación periódica de la realización de los mantenimientos al PCN

Adicionalmente, será revisado cuando se materialice una amenaza (evento de riesgo), actuando de la siguiente manera:

- En caso que una amenaza fuera detectada y los controles de riesgo resulten eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficacia.
- En caso que la amenaza esté prevista pero los controles de riesgo sean ineficaces: debe analizarse la causa del fallo y proponer nuevos controles de riesgo.
- En caso de que la amenaza no esté prevista: debe promoverse un nuevo análisis de la Matriz de riesgos. Es posible que los controles de riesgo adoptados sean eficaces para un evento de riesgo no previsto, no obstante, esto no es justificativo para evitar el análisis de lo ocurrido.

Para la realización de ensayos se considerarán los siguientes tipos de pruebas a aplicar dependiendo de la factibilidad y el tipo de plan de contingencia:

a.- Lista de chequeo Ensayo básico revisa la disponibilidad de recursos para la ejecución del plan

b.- Paseo de Revisión Se realizará previo al ensayo de simulación Reunión de equipos y descripción verbal de los pasos

c.- Simulación Simula el tipo de alteración, permite practicar el plan y validar una o más partes del plan

d.- Interrupción completa Activa todos los componentes Parte del hecho de que todos los procesos esenciales se han alterado.

En cada plan de contingencia y procedimiento se detalla el tipo de prueba seleccionada que se ejecutará, además de identificar:

- Recursos requeridos para la prueba
- Recursos Humanos

    - Recursos Tecnológicos
    - Recursos no tecnológicos
    - Documentación formularios de respaldo, Etc.

- Tiempos y actividades detalladas
- Responsables de ejecución de la prueba
- Responsables de control de la ejecución (Internos y Externos)

Todas las líneas o unidades de negocio y operativas comprometidas con los procesos críticos, tienen la responsabilidad de intervenir en los simulacros de contingencia que se programen, a fin de evaluar la eficacia de los procedimientos ya sean manuales y/o automáticos establecidos y estar debidamente capacitados para afrontar cualquier evento y dar una solución rápida, oportuna y simple.

7.1.6. Esquema de Proceso de Pruebas.

Es evidente que toda creación necesita ser probada antes, durante y después de su elaboración con el objetivo de simular un entorno menos probable y ver qué tipos de errores se pueden mejorar, al igual que se garantiza mejorar la calidad durante este tipo de pruebas.

Dentro de los estándares de seguridad se toma como una política de estricto cumplimiento la realización de pruebas, que a continuación se describen como un proceso integral y continuo.[90]

---

[90]. Wilhelm, Thomas. Professional Penetration Testing: Creating and Learning in a Hacking Lab, Elsevier Science & Technology Books, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1115172. Pag 199.

Cuadro 14. Proceso de pruebas

PRE-PRUEBA	PRUEBA	POST PRUEBA
✓ Acciones para preparar la condición de prueba	✓ Prueba Real.	✓ Regresar todo a su lugar
✓ Aviso a usuarios	✓ Movimiento de Personal	✓ Desconectar equipos
✓ Checklist de condiciones, contrato, equipos, otros	✓ Traslado de equipo y datos.	✓ Regresar personal
✓ Definición de medidas de retorno por si algo falla en la prueba y afecta fuertemente la operación.	✓ Simulación de condiciones de desastre	✓ Documentar y evaluar Resultados
	✓ Ejecución de procedimientos del plan	

7.2. ANALISIS DE LOS RIESGOS INFORMÁTICOS Y SU CONTROL.

Se trata de hacer un estudio sobre el sistema de riesgos y control de las vulnerabilidades de un sistema, por lo que es indispensable realizar un SGSI que define las políticas y genera los controles a las amenazas y la continuidad del negocio que es un plan diseñado con el fin de permitir que, aunque se concrete una amenaza el programa siga funcionando.[91]

[91]. Bolaños Duván, Análisis de Riesgos, Universidad Católica de Colombia, Bogotá, [Consulta: 2 agosto 2019] https://repository.ucatolica.edu.co/bitstream/10983/1305

Poder estimar la magnitud de una amenaza a través de controles, entendiendo que el manejo de un riesgo puede producir daños o pérdidas económicas o administrativas a una compañía u organización, es en sí, manejar el negocio. Con el objetivo primario de conservar la integridad, disponibilidad y confidencialidad de la información, los controles deben garantizar la seguridad, por lo tanto, se propone la arquitectura MVC que se adapta muy bien a este tipo de necesidades.

Cada riesgo tiene un contexto único, por lo que cada empresa debe evaluar de forma específica su análisis, y las interrelaciones con otras ocupaciones de negocios, tales que recursos humanos, desarrollo, producción, operaciones, administración, Tecnología de la Información, finanzas, etc.… y los clientes deben ser detallados para lograr un retrato integral y completo de cada riesgo. [92]

Es por ello que la tecnología debe ser usada con responsabilidad en cada empresa, cuya labor es que se identifiquen los riesgos de cada situación que la empresa puede llegar a tener. Por ello es que es menester de cada organización velar por su seguridad de la información.

Tener un plan de riesgo y control es fundamental en el cual el objetivo principal es la seguridad, es vital, porque se está protegiendo a la empresa, sus bienes y su información, dicho proceso está elaborado por profesionales en el tema y por cada miembro que conforma la organización que conocen de primera mano el funcionamiento de la empresa. Cuando un riesgo de vulnerabilidad se vuelve real tiene un impacto negativo, en la medida de que se lleve a cabo. Por lo cual es válido siempre tener un plan de contingencia denominado: continuidad del negocio.[93]

---

[92]. Solarte Francisco Riesgo y control informático, [Consulta: 13 agosto 2019] http://riesgosycontrolinformatico.blogspot.com/

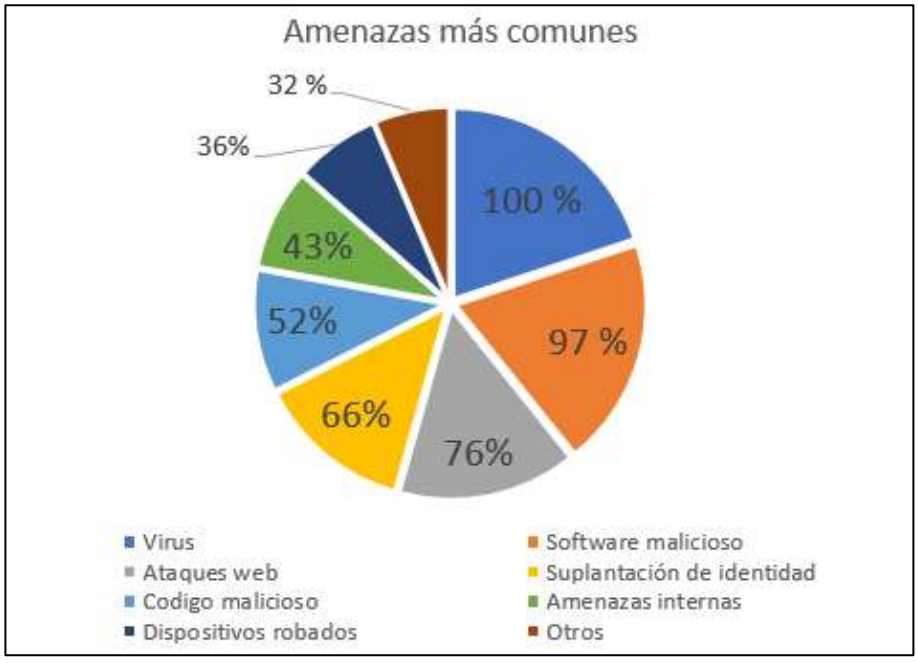
[93]Instituto de ciberseguridad, Gobierno de España, Plan de continuidad de negocio. [Consulta: 13 agosto 2019]https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

En el plan de la continuidad del negocio, se analiza el riesgo que es necesario para identificar si los controles están ayudando a minimizar la probabilidad de ocurrencia y de recurrencia, de no ser así la empresa tiene riesgos no controlados.

El plan de la continuidad del negocio mediante la evaluación del riesgo contempla las siguientes acciones: calcular la magnitud del impacto de un riesgo, nivel de criticidad de un riesgo, priorizar los riesgos de forma cuantitativa y cualitativa para generar una matriz del riesgo.

La siguiente grafica corresponde a los resultados de las amenazas más comunes que una muestra de 100 personas, escogidas al azar, en el cual confluyen empresarios, encargados de seguridad informática, usuarios, entre otros, manifiestan son las más comunes:

Figura 40. Amenazas más comunes



Fuente: autoría propia.

7.3. PROCEDIMIENTO PARA EL CONTROL DE RIESGOS INFORMÁTICOS.

Primero se trabaja en la generación de una matriz donde se identifican y analizan los riesgos. En este documento se exponen los elementos detallados, la forma en que se corresponden y los cómputos realizados. Este análisis de peligro es indefectible para alcanzar una correcta dirección del riesgo. La gerencia del riesgo hace informes a la gestión de los capitales de la organización. Coexisten diferentes arquetipos de riesgos como el riesgo excedente y riesgo general, así como también el procedimiento del riesgo, valoración del riesgo y gestión del riesgo entre otras. [94]

La valoración del riesgo incluye las siguientes diligencias y acciones:

- Identificación de activos de la empresa.
- Identificación de las obligaciones legales y de negocio relevantes para la caracterización de los activos.
- Estimación de los activos reconocidos, habiendo entendido las obligaciones legales y de negocio reconocidos anteriormente, y el impacto de un detrimento de confidencialidad, integridad y disponibilidad.
- Caracterización de las amenazas y vulnerabilidades significativas para los activos reconocidos.
- Valoración del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Cómputo del riesgo.
- Estimación de los riesgos desde una sucesión de riesgo preestablecidos.

Después de verificar el análisis convenimos establecer las labores a tomar en relación a los riesgos excedentes que se identificaron. Las operaciones pueden ser:

- Inspeccionar el riesgo: Vigorizar los controles efectivos y/o añadir nuevos controles.

---

94. Hualde Antonio, Canela José, Análisis Integral de Riesgos en ingeniería, [Consulta: 30 agosto 2019] https://escuela-emprendedores.alegra.com/ventas/que-es-un-sistema-pos-todo-lo-que-debes-saber/

- Eliminar el riesgo: al quitar el activo relacionado y se elimina el riesgo.
- Cooperar en el riesgo: a través, de acuerdos pactados parte del riesgo se trasfiere a un tercero.
- Aceptar el riesgo: Se establece que el nivel de muestra es conveniente y por lo tanto se admite.

La seguridad de una empresa comienza en el núcleo, dentro de sí misma. Capacitando al personal, fundando reglas basadas en estándares, examinando grietas y puntos ciegos en la seguridad lógica y en la seguridad de sistemas de información. [95]

Es fundamental realizar pruebas que se aproximen a la realidad, en escenarios de conflicto controlado, para que se puedan generar medidas de seguridad.

7.3.1. Elementos afines:

- Activo: Recurso tangible e intangible de la empresa que representa un valor comercial.

- Amenaza: Es un suceso que consigue causar un acontecimiento de seguridad en una empresa produciendo pérdidas o daños potenciales en sus activos.

- Vulnerabilidad: Es la grieta, falla o debilidad presenta en un proceso de la empresa.

- Riesgo: es la probabilidad de ocurrencia de una amenaza que esta identificada y que puede contraer grandes consecuencias sino es tratado o evitado.

- Análisis: Es la auditoria, control o veeduría que se realiza sobre los controles a vulnerabilidades existente dentro de una empresa.

---

[95]. Martelo Raúl, Tovar Luis, Maza Diego Modelo básico de seguridad Lógica, [Consulta: 30 agosto 2019] https://scielo.conicyt.cl/pdf/infotec/v29n1/0718-0764-infotec-29-01-00003.pdf

- Control: son los componentes que se definieron en las políticas de gobernanza de un plan de sistema de gestión, que tiene como fin generara una medida de protección antes las amenazas.

Este asunto de administración de riesgo es un asunto perpetúo ya que es obligatorio tasar periódicamente si los riesgos hallados y si estos poseen una afectación, se calcula en qué etapa esta o puede ocurrir un riesgo. Estos controles de riesgo son aplicables en el día a día de la empresa. Por ello es vital realizar este monitoreo para poder controlar la empresa y sus posibles riesgos.

Concurren varias herramientas en el internet con las que se puede afirmar a la hora de valorar los riesgos, primariamente en el asunto de evaluación de estos. Una vez acabado este procedimiento se documenta toda la información alcanzada para su examen posterior. La herramienta a elegir debe dominar por lo menos un módulo de cogida de datos, de análisis de estos y otro de reportes. La calidad de un buen estudio y una coherente presentación de los datos analizados nos transportarán a una segura exégesis de la situación real de los riesgos y, entonces, la elección de los controles que convenimos implementar será la más ajustada en el proceso de elección, economizando costos en elementos y costos de operación igualmente del ahorro de tiempo.[96]

El mercado comercial se ha digitalizado. Estas herramientas tecnológicas se han vuelto indispensables en los mercados como la tendencia primordial globalizada dedicada a satisfacer a las nuevas generaciones facilitando el acceso de compra.

El sustento un software o aplicación, contiene todas las actividades que se corresponden ejecutar para garantizar que se conserve renovado y en trabajo. Una transcendental actividad de sostenimiento a la que muchos no prestan bastante cuidado es la seguridad de la información.

---

[96]. Calder, Alan. Nueve Pasos para El éxito: Una Visión de Conjunto para la Aplicación de la ISO 27001:2013, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255165

Según Kaspersky Lab y Ponemon Institute, el 60% de una mediana empresa o pyme desaparece después de recibir un ataque informático, Es fácil concebir el porqué: la exhibición de información confidencial daña la confianza de los clientes.

Y lo peor, no se requiere un gran coste para resguardar convenientemente el software frente a amenazas informáticas. Lo que se necesita es una orientación proactiva para evidenciar la seguridad del mismo y efectuar medidas para advertir dichas amenazas.

7.4. COSTOS DE IMPLEMENTACIÓN.

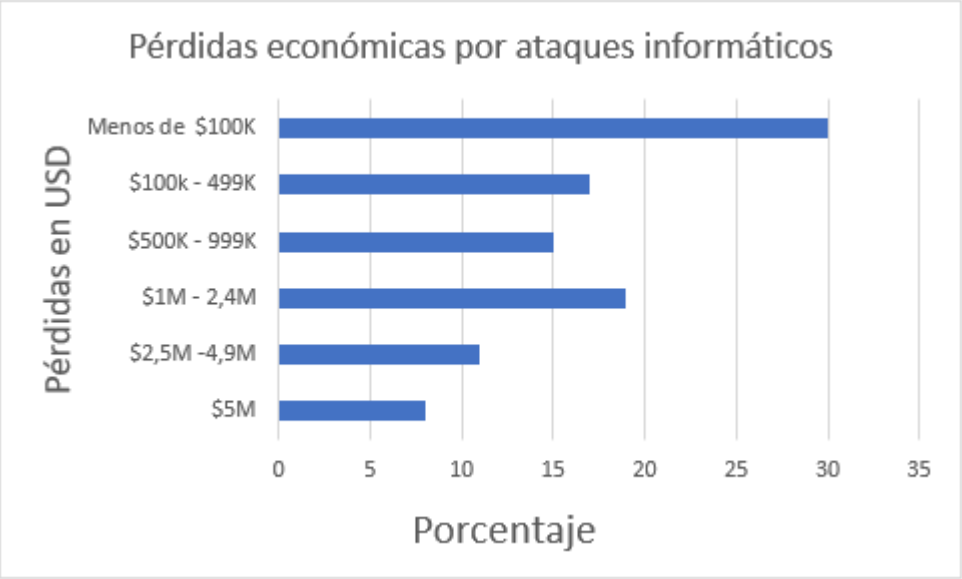
Se presenta el precio como un factor significativo del desarrollo. Se desea construir una aplicación cuyo valor sea bajo, tanto a la hora de implementarla, como a la hora de mantenerla para que esta sea viable. En este orden de ideas será necesario hallar tecnologías de software libre para conseguir este propósito.

Requerimientos: Se debe tener en consideración que la aplicación debe ser accesible desde cualquier sistema operativo. El sistema usará el protocolo http para conectar los clientes y el servidor.

Por tanto, lo más adecuado es el pago de alojamiento de la aplicación web para su correcto funcionamiento, siempre bajo las normas básicas de seguridad de la información como certificados SSL, black list, cifrados 256btis, entre otros.

El navegador podrá funcionar con cualquier resolución igual o superior a 800 x 600 píxel. Para lograr el objetivo de independizar el aplicativo de plataformas o propietarios costosos se hará uso del lenguaje PHP en el diseño y lenguajes como JQuery, Jasón etc. en la implementación.

Figura 41. Perdidas por ataques a nivel mundial



Fuente: elaboración propia.

La maquetación de la página, en su programación de diseño en el módulo vista es amigable, intuitiva y en general fácil de utilizar, con todos los componentes capaces de recibir los datos y consultas que el cliente necesita, debe contener toda la información clara en un diseño minimalista que no sature lo que el cliente está mirando.

Los costos de seguridad, deben asumirse por la empresa como una inversión, ya que, a corto y largo plazo, garantizará que no haya pérdidas millonarias que puedan poner en riesgo la continuidad del negocio. A continuación, se muestran los rangos de pérdidas de dinero en USD que han tenido que asumir las empresas por ataques informáticos a nivel mundial:

A continuación, se presenta un presupuesto tentativo, que varía de acuerdo a los cambios de tecnología, tiempo y recursos, en donde se estima cual es el costo que una empresa debe invertir para el desarrollo de un sistema pos basado en la arquitectura MVC:

Tabla 1. Presupuesto para el montaje del modelo MVC.

Presupuesto					
Componente	**MES1**	**MES2**	**CANT**	**COSTO UNITARIOS**	**TOTAL**
MANO DE OBRA					
Analista de desarrollo de Software	160h	160h	2	$ 1.950.000	$ 3.900.000
Analista de calidad de software	5h	5h	2	$ 950.000	$ 1.900.000
HARDWARE					
Depreciación Computadora Analista de Desarrollo	160h	160h	2		
Depreciación Computadora Analista de Calidad	5h	5h	2		
Servidor Web	$170.000	0	1	$170.000	$170.000
SOFTWARE					
Sublime Text3	$240.000	$ -	1	$ 240.000	$ 240.000
XAMPP	$ -	$ -	1	$ -	$ -
MySQL	$ -	$ -	1	$ -	$ -
PHP	$ -	$ -	1	$ -	$ -
Windows 10	$638.250	$ -	1	$ 638.250	$ 638.250
SERVICIOS					
Energía	16 kW/h	16kw/h	2	$ 115.000	$ 230.000
Internet	1 plan	1plan	2	$ 70.000	$ 140.000
Trasporte	10ga/gas	10ga/gas	20	$ 8.500	$ 170.000
				subtotal	$ 7.388.250
				Imprevistos (5%)	$ 369.413
				Ganancias (25%)	$ 1.847.063
				Total	**$ 9.604.725**

29 Fuente: elaboración propia como ejemplo de presupuesto.

7.5. ESCENARIOS Y HERRAMIENTAS DE DESARROLLO.

1. Apache: Este servidor virtual sirve como una herramienta para el testeo de la maquetación, diseño y puesta a punto de la página en general, se usa como plataforma de servicio de la aplicación, tiene acceso a base de datos y sirve en cualquier navegador.

2. Navegadores: la modelo vista controlador permite estar optimizado en cualquier navegador, aparte de esto como el lenguaje de programación es PHP, uno de los más difundidos lenguajes de programación, cada navegador proporciona soluciones antes los problemas de navegación que se pudieran presentar, por tal motivo, no es necesario especificar que navegador es el mejor, ya que funcionará en todos.

3. Secure Sockets Layer (SSL): Los navegadores ya vienen optimizados para la función de cifrado SSL, y los hostings poseen desde su servicio el cifrado que comprueba que la comunicación es real y segura, es por ello, es que Google que es un motor de búsqueda lo utiliza como un estándar de seguridad.

4.Base de datos MySQL: Esta base de datos que tiene una distribución gratuita permite hacer ensayos desde el servidor virtual, que puede manejar miles de datos sin que se ponga en riesgo la información, por tal motivo, se la ha escogido como la opción más viable y que además está en la mayoría de los servicios de hosting.[97]

5. Lenguaje de Programación: Se ha seleccionado el programa PHP como lenguaje de programación por su versatilidad y por qué se acomoda al modelo MVC, que fácilmente puede adaptar cualquier modulación que realicemos con fácil detección de errores y testeos de la página.

---

[97]. Fuente: ALCALDE, Luis & PEREZ Fontanals Técnica de Telecomunicaciones, especialidad en Telemática DIRECTOR: Roc-Mesaguer PallarèsFECHA:15 de octubre de 2009. Pag 125.

7.6. CRONOGRAMA DE ACTIVIDADES PARA IMPLEMENTAR MVC.

Tabla 2. Cronograma para el montaje del modelo MVC.

ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5
Documentación de la información relevante de las empresas más destacadas.					
Identificación de las vulnerabilidades de los sistemas actuales.					
Documentación de ataques a sistemas en las empresas colombiana con consecuencias graves					
Pruebas controladas de ataques a empresas dispuestas a mejorar sus seguridades.					
Estudiar la programación de las aplicaciones de empresas con sistema POS.					
Documentar todos los procedimientos hallazgos que se obtengan de las practicas antes mencionadas					
Diseño y pruebas del modelo de seguridad propuesto para las aplicaciones web con enfocadas al sistema POS					

Fuente: elaboración propia.

8. RECOMENDACIONES EN LA IMPLEMENTACION DEL MVC.

Para la implementación del modelo-vista-controlador, se recomienda que las personas que estén al frente de la fase de la programación comiencen a recibir capacitación cuanto antes, puesto que, la curva de aprendizaje, es bastante considerable, una vez se tomen los lineamientos básicos, se hará sencillo su montaje.

Se deben compara equipos acordes a la Cuadro de presupuesto, pero se recomienda, mejorar sus características para un trabajo más rápido y eficiente, en su defecto, se debe actualizar los equipos de acuerdo al año en que se comience a trabajar en el montaje del modelo-vista-controlador, así garantizar un desempeño óptimo.

Los presupuestos para el desarrollo de esta tecnología informática, pueden parecer altos, sin embargo, la relación costo beneficio es muy favorable para quien la implemente, por lo tanto, se recomienda hacer esta inversión por que los resultados serán recuperados en el corto y mediano plazo, y a largo plazo todos estos beneficios son ganancias.

Se recomienda implementar un sistema de gestión de seguridad de la información para tener un control optimo del proceso, ya que esto permite un adecuado control sobre los riesgos y amenazas que se van a presentar durante la implementación del modelo-vista controlador, pero que con la continuidad del negocio en caso de ataques o perdida de información sensible sea relativamente sencillo recuperarse ante estas eventualidades.

9. CONCLUSIONES.

La aplicación convencional de una programación sin seguridad es un riesgo altísimo en la seguridad informática, en este caso quien se ve más afectado, es el usuario que realiza una compra a una empresa, puesto que esta entrega sus datos personales y bancarios confiando que la empresa, realizará un manejo adecuado de datos, por tal motivo es indispensable implementar el modelo -vista – controlador.

La arquitectura, modelo vista controlador MVC, tiene grandes ventajas en cuento al manejo lógico y estético de una aplicación web, este concepto en sí mismo representa un modelo de seguridad de la información ya que solo con altos conocimientos informáticos se puede vulnerar la seguridad de su programación, además el modelo permite implementar muchas barreras de seguridad que fortalecen este tipo de arquitecturas, es por ello, que se lo define como un modelo maduro y fiable incluyendo los sistemas POS.

Implementar una arquitectura modelo vista controlador en cuanto a las mejoras TI a los sistemas de la empresa representa, que la calidad en los procesos se mejorará ostensiblemente lo que va a representar una mejora considerable en sus actividades que representa beneficios económicos para la organización.

Uno de los aspectos más importantes dentro de la seguridad informática, es el hecho de que debemos tener los sistemas informáticos y todos sus componentes actualizados y parchados para que las vulnerabilidades existentes puedan ser seguras; sin embargo, parece que este tema que, aunque parece dado por hecho muchas veces se pasa por alto y se las consecuencias son graves.

Aunque la seguridad informática ofrece muchas líneas de defensa para proteger la información sensible, ningún sistema es completamente seguro, y para que los sistemas tengan mejor resultado en su seguridad es vital apoyarse con una inversión en hardware y personal experto para que puedan en tiempo función del tiempo solucionar cualquier inconveniente.

Los registros y monitoreos de ataques a la seguridad informática son parte de las SGSI, dentro de las cuales las políticas de gobernanza deben definir el uso de registros y monitoreos con variables cuantitativas, que posean métricas que permitan hacer un balance adecuado y, por ende, el uso de toma de decisiones, que representen óptimos resultados

10. BIBLIOGRAFÍA.

Allen, Lee, et al. Kali Linux – Assuring Security by Penetration Testing: Assuring Security by Penetration Testing, Packt Publishing, Limited, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1572946.

Bracho, David, and Carlos Rincón. Modelo para la cuantificación del riesgo telemático en una organización, Red Enlace, 2010. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3203066.

Calder, Alan. ISO27001/ISO27002: una Guía de Bolsillo, IT Governance Ltd, 2017. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5255172.

Calder, Alan. Iso27001/iso27002:2013, IT Governance Ltd, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1463579.

Chicano, Tejada, Ester. Auditoría de seguridad informática (MF0487_3), IC Editorial, 2014. Recuperado de: ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=4184005.

Dalziel, Henry, and Henry Dalziel. How to Attack and Defend Your Website, edited by Alejandro Caceres, Elsevier Science & Technology Books, 2014. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1888757.

Gobierno de España (2007). MONOGRÁFICO: Máquinas virtuales - Herramienta de virtualización VirtualBox, Recuperado de: http://recursostic.educacion.es/observatorio/web/fr/software/software-general/462-monograficomaquinas-virtuales?start=2

Gómez, Fernández, Luis, and Rivero, Pedro Pablo Fernández. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, AENOR - Asociación Española de Normalización y Certificación, 2015. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3430311.

Gómez, V. Á. (2014). Gestión de incidentes de seguridad informática. Madrid, ES: RA-MA Editorial. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=11046422&tm=1465232638601

Hernández, Diaz, Lester Reinier. Un modelo para la implementación de la seguridad de una aplicación Web con el uso de la programación orientada a aspectos, D - Instituto Superior Politécnico José Antonio Echeverría. CUJAE, 2012. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3203748.

High Tech. (2015). Sistema de detección de intrusiones (IDS), Recuperado de: http://es.ccm.net/contents/162-sistema-dedeteccion-de-intrusiones-ids

Instituto de ciberseguridad. Gobierno de España, Plan de continuidad de negocio. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

López, M. Y. (2009). Los virus informáticos: una amenaza para la sociedad. Cuba: Editorial Universitaria. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=4&docID=10

357400&tm=1466006227313.

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [Online], Recuperado de: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe 15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-deelementos_es_NIPO_630-12-171-8.pdf

Modelo para el gobierno de las TIC basado en las normas ISO. (2012). España: AENOR - Asociación Española de Normalización y Certificación. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10637138&tm=1456691942576

Muniz, Joseph, and Aamir Lakhani. Web Penetration Testing with Kali Linux, Packt Publishing, Limited, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1420531. Pag 148

Muñoz, Víctor Belmar. Prevención de riesgo - Implantación de un sistema efectivo de control de riesgo, El Cid Editor | apuntes, 2009. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3180200.

Najera-Gutierrez, Gilberto, and Juned Ahmed Ansari. Web Penetration Testing with Kali Linux: Explore the Methods and Tools of Ethical Hacking with Kali Linux, 3rd Edition, Limited, 2018. Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=5314613.

Norma técnica colombiana NTC-ISO/IEC27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI), [Online], Recuperado de:

http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Pinson, Linda. Anatomía de un Plan de Negocio: Una Guía Gradual para Comenzar Inteligentemente, Levantar el Negocio y Asegurar el Futuro de su Compañía, Out Of Your Mind . . . And Into The Mark, 2011. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=828142.

Pritchett, Willie, and Smet, David De. Kali Linux Cookbook, Packt Publishing, Limited, 2013. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1389391.

Rodríguez, G. M. E. (2013). Gestión de datos: bases de datos y sistemas gestores de bases de datos. Barcelona, ES: Editorial UOC. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?docID=10853383

Rojas, C. I. S. (2009). Trabajo de auditoría normas COBIT. Argentina: El Cid Editor | apuntes. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10317247&tm=1456692028784

Ross, J. W., & Weill, P. (2004). Seis decisiones de TI que no debe dejar en manos del departamento de TI. España: Ediciones Deusto - Planeta de Agostini Profesional y Formación S.L. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=1&docID=10063648&tm=1456691972039

Safronov, Mark, and Jeffrey Winesett. Web Application Development with Yii 2 and PHP, Limited, 2014. ProQuest Ebookl, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=1800650.

Sanz, M. P. (2008). Seguridad en Linux: guía práctica. España: Editorial Universidad Autónoma de Madrid. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=8&docID=10844623&tm=1466006678974

Upton, David, and José Argudo Blanco. CodeIgniter 1.7: Improve your PHP Coding Productivity with the Free Compact Open-Source MVC CodeIgniter Framework, Packt Publishing, Limited, 2009. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/bibliouniminuto-ebooks/detail.action?docID=946937.