UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

BackOffice en Plataforma de Cobranza Electrónica

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

José Antonio García Rojo

ASESORA DE INFORME

M.C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2021

Tabla de contenido

Índice de Figuras

Introducción

Con el crecimiento exponencial del uso de Internet en las últimas décadas, se han abierto posibilidades para mejorar la calidad de vida de las personas automatizando procesos que anteriormente tomaban mucho tiempo realizarlos, para el caso del presente trabajo se hace mención de manera particular a procesos referentes a transacciones bancarias.

La posibilidad de comprar algún producto desde el otro lado de la ciudad, en otra parte del país o inclusive desde otro país y otro continente era muy difícil por la distancia a recorrer, actualmente eso se puede hacer con un par de clics y una tarjeta bancaria en la mano.

Ni hablar de pagar impuestos o servicios estatales, era hacer filas interminables tanto en los bancos como en las tesorerías, igualmente esto ya se puede realizar desde un smartphone y con una conexión regular de Internet.

Sin embargo, con el aumento de este tipo de transacciones han incrementado los riesgos de sufrir fraudes y robo de información personal, entre otros; con esto surgió la necesidad de crear plataformas que procesen los cobros de una manera segura evitando que la información utilizada por los usuarios de estos servicios caiga en manos de personas no deseadas y hagan mal uso de ella.

Para crear, mantener y actualizar plataformas, sistemas o aplicaciones con estas características, se requiere de personal altamente capacitado o invertir en capacitar personal para que cumpla con las actividades antes listadas.

Este reporte va ligado a una plataforma que tiene más de diez años haciendo uso de la tecnología y cumpliendo con los más altos estándares de seguridad para el procesamiento de la información bancaria y personal, se ha posicionado a la vanguardia de los pagos en línea, procesando los impuestos de las 32 entidades que conforman el país, así como la mayoría de los municipios de cada uno de ellos, teniendo clientes reconocidos nacionalmente como son un portal de ventas de productos entre usuarios, portales de viajes y universidades de gran prestigio, donde se apoya para llevar a cabo el cobro de su tienda virtual, pago de congresos, cursos y más, esto por citar algunos de los aproximadamente 900 clientes que actualmente se tienen afiliados.

En las siguientes páginas se presenta una descripción de la empresa, que se denominará en este reporte como “Pagos.mx” y se expone un marco general de las tecnologías de la información que se usan para llevar a cabo los procesos que se realizan en sus diferentes plataformas.

También se muestra un listado de varios proyectos pertenecientes a la empresa, los cuales, su principal finalidad es el procesamiento de los pagos, pero con diferentes tecnologías (tanto de hardware como de software) para cubrir las necesidades de los clientes y sus plataformas en línea.

Se describe con mayor detalle un proyecto realizado para cumplir necesidades puntuales de un cliente y las cuales no se tenían implementadas dentro de la plataforma.

Finalmente, en la sección de resultados se exponen evidencias de la experiencia laboral obtenida dentro de la empresa, así como de las habilidades desarrolladas con el fin de realizar las tareas encomendadas para el cumplimiento del trabajo dentro de una empresa relacionada con la tecnología y cómo los conocimientos obtenidos dentro de la Facultad de Ingeniería me permitieron incorporarme al campo laboral exitosamente y acrecentar estos con la experiencia laboral obtenida a través del tiempo transcurrido desde mi egreso.

1

Antecedentes

La importancia de la seguridad de la información es un tema crucial hoy día y a la par la importancia de que las plataformas de pagos en línea cuenten con estándares de seguridad por los datos que se usan en este tipo de transacciones. Como muestra, se puede mencionar lo ocurrido en 2019, un área del FBI recaudó casi medio millón de quejas referentes a crímenes hechos por Internet, estas quejas se traducen en pérdidas financieras, que en ese año fueron por 3.5 billones de dólares.

El tipo de crimen que más víctimas tuvo fue el phishing/vishing/smishing/pharming, que a grandes rasgos es hacerse pasar por alguna empresa de renombre, financiera principalmente, esto lo realizan los perpetradores mediante algún correo electrónico o una página web, para lo cual se usa la imagen de la empresa, colores o características similares a los canales oficiales y mediante la petición de realizar alguna actualización en sus datos o con el engaño de que la cuenta puede ser bloqueada si no se realiza algún procedimiento, se puede obtener información personal, casi siempre son datos bancarios, con esta información la persona o personas involucradas pueden hacer uso de esta información y obtener el beneficio deseado.

Este reporte hecho por el FBI es global, pero solo tiene 600 quejas registradas de México. En ese sentido, cabe mencionar que, en México para poder procesar pagos en línea se debe cumplir con una certificación por el manejo de datos bancarios, esta certificación se debe renovar cada año y se llama PCI DSS (Payment Card Industry, Data Security Standard).

Esta certificación consta de cumplir lineamientos de seguridad en el manejo de datos, cifrado de datos sensibles que se obtienen en los procesos de pagos, servidores seguros con las últimas actualizaciones de software y cumplir con estándares de seguridad de accesos y arquitectura segura. También se valida el código que se tiene en la aplicación, así como el cifrado de los equipos de cómputo del personal, entre otras especificaciones.

Acerca de PCI Security Sanders Council: Es una organización destinada a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas.

En la Figura 1.1 se muestran lo que esta empresa nombra como hitos, que son de forma muy general los aspectos que deben seguir las empresas que realicen operaciones que involucren datos bancarios. En negritas se muestra el objetivo principal y después una breve explicación de cada uno de estos hitos.

Hitos	Objetivos
1	**Eliminar los datos confidenciales de autenticación y limitar la retención de los datos.** Este hito se dirige a un área clave de riesgo para las entidades que han estado en riesgo. Recuerde - si no se almacenan los datos confidenciales de autenticación y otros datos del titular de la tarjeta, se reducirán considerablemente los efectos del riesgo. Si no los necesita, no los almacene
2	**Proteja los sistemas y las redes, y esté preparado para responder a una falla en el sistema.** Este hito se dirige a los controles de los puntos de acceso para la mayoría de riesgos, y los procesos para responder.
3	**Aplicaciones seguras de tarjetas de pago.** Este hito se dirige a los controles de las aplicaciones, los procesos de la aplicación y los servidores de la aplicación. Las deficiencias en estas áreas ofrecen una presa fácil para poner en riesgo a los sistemas y obtener acceso a los datos del titular de la tarjeta.
4	**Supervisar y controlar el acceso a sus sistemas.** Los controles para este hito le permiten detectar quién, qué, cuándo y cómo con respecto a quién accede a su entorno de red y de datos del titular de la tarjeta.
5	**Proteja los datos del titular de la tarjeta que fueron almacenados.** Para aquellas organizaciones que han analizado sus procesos comerciales y que determinaron que deben almacenar los Números de Cuenta Primarios, el Hito Cinco se dirige a los mecanismos de protección clave para esos datos almacenados.
6	**Finalice los esfuerzos de cumplimiento restantes, y asegúrese de que todos los controles están implementados.** La intención del Hito Seis es completar los requisitos de la PCI DSS, y finalizar todas las políticas relacionadas restantes, los procedimientos y los procesos necesarios para proteger el entorno de los datos del titular de la tarjeta.

Figura 1.1. Hitos de seguridad a seguir dentro de cualquier empresa.

La seguridad informática se ha convertido en un tema de suma importancia hoy en día por la cantidad de información que se procesa en cada uno de los sistemas existentes. Con la cantidad de información que manejan las aplicaciones financieras, es de suma importancia mantener protegido el sistema con las mejores herramientas o tecnologías con el objetivo de evitar fuga de información y posibles fallas del sistema causados por ataques cibernéticos.

La seguridad informática es un tema crucial para la protección y gestión de la información de cualquier organización, por lo que es de suma importancia reconocer las categorías que existen para determinar las acciones en cada una de ellas.

La seguridad informática contempla cuatro áreas principales:

● **Confidencialidad**: Solo usuarios autorizados pueden acceder a recursos, datos e información.

● **Integridad**: Solo los usuarios, sistemas o procesos autorizados deben ser capaces de modificar los datos cuando sea requerido.

● **Disponibilidad**: Los datos deben estar disponibles para los usuarios, sistemas o procesos autorizados cuando sea necesario.

● **Autenticación**: Verificar que realmente se está en comunicación con el usuario, sistema o proceso legítimo.

De acuerdo con los elementos de objeto de protección, clasificamos estos tipos de seguridad informática:

1. Seguridad de hardware
2. Seguridad de software
3. Seguridad de red

1. Seguridad de hardware

Se aplica a la protección de elementos físicos para evitar amenazas e intromisiones. La seguridad de hardware se encarga de encontrar las vulnerabilidades existentes en los equipos desde su fabricación, hasta los dispositivos de entrada y salida que están conectados.

Las herramientas utilizadas para la **seguridad de hardware** controlan de forma exhaustiva el tráfico que se produce en la red, brindando una seguridad más potente. Este tipo de seguridad es de las más robustas. Fortalece a los sistemas más importantes como filtro adicional de seguridad.

Los ejemplos más típicos son los cortafuegos o servidores intermedios (proxy). Los menos comunes son los módulos de seguridad de hardware (HSM) que suministran claves criptográficas para el cifrado, el descifrado y la autenticación.

2. Seguridad software

Los errores en el software generan vulnerabilidades y esto constituye uno de los mayores riesgos de seguridad. Existen diferentes tipos de errores que se generan en el software, por ejemplo, errores de implementación, desbordamientos de buffer, defectos de diseño o un mal manejo de estos.

La seguridad de software protege las aplicaciones y el software de amenazas externas como virus o ataques maliciosos. El antivirus es una de las herramientas más utilizadas para este tipo de seguridad, que dispone de una actualización automática y ayuda a encontrar virus nuevos. Otros ejemplos son los cortafuegos, filtros antispam, software para filtrar contenidos y publicidad no deseada.

3. Seguridad en la red

Se refiere a las actividades encaminadas a la protección de datos en red, es decir, su función principal es proteger el uso, fiabilidad, integridad y seguridad de la red para evitar que la información sea modificada o robada.

Las amenazas más comunes en la red son:

● Virus, gusanos y caballos de troya

● Software espía y publicitario

● Ataques de día cero, también llamados ataques de hora cero

● Ataques de hackers

● Ataques de denegación de servicio

● Intercepción o robo de datos

● Robo de identidad

Los componentes de seguridad de red incluyen antivirus y antispyware, cortafuegos, sistemas de prevención de intrusiones y redes privadas virtuales.

Entre las potenciales consecuencias de no tener un sistema seguro están las siguientes:

- Perder la confianza de los clientes y que utilicen otra empresa para el procesamiento de pagos
- Perder ventas
- Costo de los nuevos plásticos en caso de clonaciones
- Pérdidas económicas por fraudes
- Asumir costos legales por demandas y juicios
- Multas o penalizaciones
- Que se deshabilite el procesamiento de pagos con tarjetas de crédito
- Pérdida de trabajos desde personal técnico hasta altos niveles Directivos

1.1 Acerca de Pagos.mx

Pagos.mx tiene sus orígenes en España y se funda el 1ero de marzo de 2000 en México, su principal objetivo fue tener un enlace que llevara el control de las compras hechas por sus empresas fundadoras, esto primordialmente con el uso de un sistema de subastas, donde los proveedores revisaban los artículos que las empresas fundadoras requerían y con base en ello colocar su oferta con la finalidad de vender sus productos. Este sistema servía también para el cobro de derechos para subir ofertas y el pago de los artículos comprados, además de un *canal* de comunicación entre los proveedores y la empresa.

Actualmente la empresa es filial de uno de los Bancos más importantes en México y de una empresa de Telecomunicaciones.

Se ha distinguido por poner al alcance de sus clientes una plataforma de cobranza electrónica la cual es utilizada por el 100% de los gobiernos estatales para la recaudación de impuestos y por numerosas empresas privadas.

Entre las principales características de esta plataforma se encuentran:

- La recepción de pagos a través de múltiples medios: tarjetas, cheque electrónico, transferencia interbancaria.
- Identifica y concilia todos y cada uno de los pagos recibidos y genera reportes personalizados.
- Se ajusta a los estándares de seguridad de la industria, cumpliendo con la certificación **PCI DSS (Payment Card Industry Data Security Standard).**

En el año 2012 recibió el premio por parte de Information Week México como el ranking número 29 bajo el título de “Las 50 empresas más innovadoras”, debido a que se adoptó una nueva forma de trabajo no presencial, a través del uso de la plataforma en línea, mejor conocida como Nube, la adopción de nuevas tecnologías y una mejor organización laboral

Visión

Ser referentes en soluciones que generen sinergia entre los sectores financiero-telecomunicaciones en México y Latinoamérica.

Contar con empleados, clientes y socios de negocios altamente satisfechos.

Misión:

Proveer a nuestros clientes soluciones innovadoras con base tecnológica, que incrementen su eficiencia y generan confianza.

Pagos.mx ha abierto nuevas oportunidades de negocio mediante soluciones innovadoras a sus clientes que pertenecen a diversos sectores como son:

- Agricultura
- Alimentos y bebidas
- Construcción
- Consultoría
- Maquinaria
- Medio ambiente
- Minorista
- Municipios

- e-commerce
- Editorial
- Educación
- Electrónica
- Energía
- Entidades Federativas
- Entretenimiento
- Exportadora
- Finanzas
- Gobierno
- Ingeniería
- Manufactura
- Organismo de Agua
- Organismos Paraestatales
- Industria Química
- Hospitales
- Seguros
- Servicios
- Tecnología
- Telecomunicaciones
- Transportes
- Turismo
- Ventas por Catálogo
- Telemarketing

Pagos.mx se divide en 6 áreas, todas dirigidas por una Dirección General.

1. Área Estrategia: Esta área es la más nueva y su objetivo es la administración de todos los proyectos, en esta área se decide qué requerimientos solicitados por el cliente son viables en su desarrollo y si va a tener algún costo extra para el cliente, igualmente con proyectos nuevos, esta área tiene la facultad de dar su consentimiento para realizarlos.

2. Área Operaciones: Es el área encargada del manejo diario del dinero correspondiente a los pagos recibidos en días anteriores y que el banco deposita a las cuentas de la empresa, sus responsabilidades son; conciliar estos montos con los datos que se guardan en el sistema, la dispersión del dinero recibido a las cuentas de los clientes, realizar devoluciones cuando exista una reclamación de parte del tarjetahabiente y son el primer contacto con el cliente si se presenta algún requerimiento nuevo en la plataforma.

3. Área Comercial: En esta área se centran todos los recursos dirigidos a las ventas de los productos, realiza el levantamiento de los proyectos y el seguimiento de

peticiones de cada uno de los clientes. Da atención personalizada a cada uno de los clientes, dando explicación de la plataforma y los beneficios que ofrece la empresa en caso de contratar alguno de los productos, hace demostraciones de la plataforma para motivar la contratación del producto.

4. Área Finanzas: Es la encargada de todos los recursos tanto monetarios como de personal de la empresa. Lleva la administración del presupuesto dado por el banco y el control de los gastos que tienen todas las áreas de la empresa, en esta área también se encuentra el tema de la organización de los recursos humanos, contrataciones, permisos de viajes y organización de eventos que involucren toda la empresa.

5. Área de Tecnología: Engloba las áreas encargadas de desarrollar y dar mantenimiento a todos los proyectos, entre las responsabilidades son la administración de Bases de Datos, de los servidores físicos, de las cuentas de AWS y sus servicios de la nube, así como el desarrollo de sistemas nuevos o hacer ajustes en el software ya sean nuevos requerimientos o de mantenimiento a los desarrollos ya existentes.

6. Área Seguridad: Es el área encargada de cumplir con los lineamientos de PCI y dar seguimiento a los posibles intentos de fraude o hackeo del sistema. Es la responsable de organizar a las otras áreas en las tareas para cumplir normas de lavado de dinero, de seguridad de los datos personales de los tarjetahabientes, así como tener el control de software con licencias.

En la figura 1.1.1 se observa una ilustración de la estructura de Pagos.mx la cual es información que se comparte con los clientes.

Figura 1.1.1. Estructura organizativa de Pagos.mx

El área de Tecnología se divide en 2 subáreas, Producción y Desarrollo.

Subárea Producción, es la encargada de la administración de servidores físicos, donde se encuentra el Websphere, las Bases de Datos, así como la administración de la plataforma de AWS donde se encuentra la última versión de las aplicaciones. Además, se encarga de la correcta funcionalidad de los equipos de cómputo de los empleados.

Subárea Desarrollo, es la encargada de los proyectos a nivel código y con apoyo de Producción tener las aplicaciones funcionando correctamente.

Entre las aplicaciones que debe revisar la subárea de Desarrollo, se encuentran las que se hospedan en los servidores físicos que son las que han servido de base en la operación de toda la empresa. Primero, es la plataforma de pagos que ha existido por más de 10 años y se ha mantenido con base en actualizaciones, en segundo sitio se encuentra la reportería o lo que se nombra dentro de la empresa como BackOffice que es donde se puede obtener la información de cada uno de los pagos de los comercios asociados, además de otras operaciones bancarias, finalmente se encuentra el módulo de configuración de los clientes que es una plataforma donde se muestra cada uno de los clientes, así como sus medios de pago, sus contratos, y sus tasas de comisiones entre otras características.

También se ha creado una versión nueva del motor de pagos, esta versión nace con la finalidad de reducir costos e incluir nuevas tecnologías, cabe mencionar que esta plataforma reside en la nube de Amazon (AWS), también involucra todo lo que tenga que ver con el motor de pagos y la página administradora de los reportes de pagos del cliente.

Por último, existen los proyectos especiales, uno de los cuales fue desarrollado para clientes que no contaban con sistemas propios, en estos casos, se cuenta con un portal con acceso restringido y en donde el cliente decide quién puede acceder a él, y donde una vez permitido el acceso se muestra el historial de los pagos realizados por el usuario, y desde ahí puede elegir los adeudos que tenga para poder efectuar el pago correspondiente.

Otro de los proyectos especiales es desarrollado para clientes que cuentan con una plataforma donde se tiene permitido el uso de información bancaria y donde se comunican con el motor de Pagos.mx que es el motor de pagos mediante servicios Web y a través del cual se obtiene una respuesta de autorización o de rechazo según la información enviada.

Como se observa en el organigrama de la Figura 1.1.2. todas las áreas que pertenecen a la empresa son dirigidas por una Dirección General, estas áreas se encuentran al mismo nivel y cada una tiene su organización interna, también se puede observar que el área de Tecnología se divide en dos subáreas de las cuales yo colaboro directamente en la subárea de Desarrollo.

Figura 1.1.2. Organigrama de Pagos.mx

2

Descripción de proyectos

Aquí se describen algunos de los proyectos y áreas en las que he participado dentro de la empresa.

Mi experiencia dentro de ésta incluye la participación principalmente dentro del proyecto que ha sido un importante soporte por más de una década realizando el cobro en línea de diversos clientes, principalmente de todos los gobiernos estatales y una gran cantidad de gobiernos municipales de todo el país con la recaudación de impuestos.

Entre las otras actividades en la empresa se mencionarán varios proyectos especiales como el cobro de tiempo aire para una empresa de telefonía celular, migración de datos y configuraciones a la plataforma de la nube del portal de pagos.

Las actividades que se enlistan a continuación describen tres puntos importantes cada una; el objetivo, breve descripción de lo que se debería hacer en esta actividad, las actividades donde se detalla qué acciones o tareas se realizaron y por último los resultados donde se explica si se logró el objetivo y qué aportó la actividad en mi carrera profesional.

2.1. Front portal de pagos.

El portal de pagos es un sistema creado para que el cliente desde su página web tenga la opción de pago en línea de sus servicios, productos, entre otros. Su principal característica es que el portal de pagos tiene la imagen lo más parecida al portal del cliente para que a simple vista no se pudiera observar que se redirigió al cliente a otro portal para procesar su pago.

El portal de pagos maneja varios tipos de pago o medios de pago para que el cliente eligiera la mejor opción según sus necesidades, entre estos medios de pagos existen el pago con tarjeta de crédito, en sus diferentes modalidades, un solo pago, meses sin intereses, pago con puntos recompensa (el banco ofrece un porcentaje de recompensa en cada compra), compra ahora y paga meses después, pagos fijos, con Cheque en Línea, pago con cuenta

de otros bancos o interbancaria, impresión de una ficha para realizar el pago en sucursal y Pay Pal.

El flujo del pago es recibir los datos del cliente mediante un envío de parámetros POST, dependiendo de las opciones contratadas por el cliente se muestran los medios de pago a elegir, una vez ingresados los datos necesarios se procesa el pago y al ser aceptado el pago, se proporciona un comprobante al usuario y mediante un envío post se hace la confirmación al sistema del cliente cuando el pago fue exitoso.

En esta área se utilizan conocimientos de java, manejo de html, servlets, jsp's, CSS, javascript, Ajax, jasperreports o ireports para los reportes, WebServices.

A continuación, se describen las funciones en el proyecto Front. Estas funciones las realicé entre noviembre del 2008 y octubre de 2013.

- **Atención requerimientos de clientes.**

Objetivo: Dar apoyo a nuestro Servicio de Atención al Cliente para resolver dudas, comentarios o fallas en el sistema reportadas por el cliente.

Actividades: Descubrir el origen del error, establecer medidas adecuadas para que no se repita, proporcionar una explicación clara del problema y solución a nuestra área de Servicio de Atención al Cliente para exponérsela al cliente.

Resultados: Se obtuvo un conocimiento sólido en cuanto a la lógica del negocio y al código utilizado en el sistema de pagos, por lo que se tenía un óptimo nivel de respuesta en cuanto a los problemas reportados a nuestra área de Servicio de Atención al cliente.

- **Pruebas de conectividad entre la plataforma del cliente y el Pagos.mx.**

Objetivo: Ofrecer a nuevos clientes soporte para que su plataforma se conecte a la plataforma de Pagos.mx de manera correcta.

Actividades: Mediante una conferencia se realizan pruebas con el cliente, estas pruebas consisten en que se envíe un pago de prueba desde la aplicación del cliente a nuestra plataforma de pruebas para validar que la comunicación y la integridad de la información sea la correcta.

Revisión de Look & Feel, Pagos.mx maneja el concepto de que la plataforma debe parecerse lo más cercano posible al sistema del cliente, esto implica tener las mismas imágenes, colores, botones, entre otros, esto le da al usuario final la seguridad de que está pagando por el sitio del cliente y no que está cambiando a una tercera empresa que no conoce.
Validación de comprobantes de pago, se comprueba que el comprobante contuviera toda la información correcta del pagador, así como el envío de este por medio de email.

Resultados: Se cumplieron con normas de calidad en el proceso de atención al cliente y se valida que la plataforma del cliente cumplía con los estándares de seguridad, cuidando la integridad de la información enviada mediante algoritmos de cifrado.

- **Agregar nuevos medios de pago.**

Objetivo: Implementar en el sistema nuevas opciones de pago al cliente, entre los que sobresalen PayPal, American Express y Cie Interbancario.

Actividades: Agregar funcionalidad correspondiente a cada medio de pago nuevo, cumpliendo las características de cada uno de ellos.

Resultados: Se analizaba la documentación de cada medio de pago y se incorporaba a nuestra plataforma de pagos de manera que cumpliera con los requerimientos de la documentación, se probaba el flujo del nuevo medio de pago realizando pruebas en un ambiente de preproducción si el medio de pago lo permitía o mediante simuladores creados dentro de la empresa.

Antes de liberar el producto se realizaban pruebas integrales que era probar todo el flujo tanto en la navegación web como el cobro y depósito del dinero utilizado en la transacción, tiempos de respuesta, casos de éxito y de rechazo.

- **Configuraciones de los portales**

Objetivo: Agregar configuración en la BD para que nuevos clientes pudieran utilizar el portal de pagos, también incluían nuevas peticiones de clientes ya configurados.

Actividades: Mediante *querys* se insertaban los datos de cada uno de los clientes y se tenía que validar la funcionalidad del portal mediante una página de prueba para simular el envío POST del cliente hacia el portal del pago y hacer la transacción del pago para confirmar que todo trabajaba normal.

Resultados: Después de las validaciones pertinentes se podía migrar al cliente de plataforma sin la necesidad de que el cliente hiciera cambios en su sistema, esto era de mucha utilidad ya que algunos clientes no tenían la posibilidad de realizar cambios de código o simplemente el tiempo en que estos cambios se podían realizar aumentaría considerablemente la migración a la nueva plataforma.

- **Administración de balanceadores.**

Objetivo: Los balanceadores son componentes los cuales reciben parámetros desde protocolos GET o FORM y hacen transformaciones para obtener un switcheo entre las dos plataformas que tiene el portal de pagos, esto es decir que clientes que operaban en la antigua plataforma pudieran hacer uso de la nueva sin necesidad de aplicar un cambio en sus aplicativos.

Actividades: Crear las transformaciones necesarias para poder cambiar un cliente a la nueva plataforma de la nube del portal de pagos, mediante un análisis de cada uno de los parámetros recibidos, se valida y se realizan las acciones adecuadas para cumplir con el

layout y enviar todos los valores que la nueva plataforma necesita para su correcto funcionamiento.
En la mayoría de los casos solo se hacía un cambio de nombre del parámetro, en otros casos solo se aplicaban condicionantes para poder establecer los valores correctos y en el resto de los casos se creaban funciones de javascript para cumplir con el objetivo.

Resultados: La migración entre plataformas se realizaba de manera rápida y transparente para el cliente, se cumplían con pruebas integrales para validar el correcto funcionamiento entre su sistema y del portal de pagos, pero se ahorró mucho trabajo al no tener que solicitar un cambio de aplicativo del lado del cliente y en cuestión de minutos se podía hacer un cambio entre plataformas sin afectar la operación del cliente.

- **Conectividad a WebServices de los clientes para el envío de la confirmación del pago.**

Objetivo: Establecer la conexión y enviar los parámetros utilizados por el sistema del cliente para que pudiera conciliar los pagos en línea y tener total control de su contabilidad.

Actividades: Solicitar liberación de las reglas de firewall, crear una aplicación cliente[1], se manejan los componentes que debe cumplir el envío de la información, esto es llenar objetos con la información adecuada y por último se consumían los servicios que el WebServices establecía.

Resultados: Se obtuvieron conocimientos de SOAP y REST para poder consumir los WebServices de los clientes dependiendo que protocolo habían implementado en su sistema, se cumple con los objetivos de tener una comunicación directa y rápida al sistema del cliente y que pueda tener toda la información disponible en tiempo real.

[1] Código encapsulado en una librería donde esta toda la lógica para invocar el WebServices del cliente.

Las actividades descritas anteriormente las pude llevar a cabo gracias a los fundamentos obtenidos en la Facultad, materias como Computadoras y Programación, Estructuras de Datos y una optativa de Temas Especiales donde aprendí el lenguaje Java, esto por mencionar algunas, ya que todas las materias ayudan de manera directa o indirectamente, al tener los fundamentos de programación pude aprender a utilizar software y herramientas más especializadas con el propósito de resolver los problemas o requerimientos solicitados. Haber aprendido a programar en bloc de notas, el saber los fundamentos para compilar y ejecutar los programas, con ese conocimiento el aprender a usar un IDE fue cosa sencilla, ya que te ahorra muchos pasos.

2.2 Plataforma de pagos para el centro de atención telefónica de una agencia de viajes.

Objetivo: Tener una plataforma para la aceptación de pagos de un portal de viajes, los medios de pagos a utilizar son mensualidades sin intereses en plazos de 3,6,9,12,13,18, pago con puntos del banco, skip and payment[2], pago en una sola exhibición, la aplicación no estará abierta al público, se utilizará en las oficinas del cliente y el contacto con el tarjetahabiente será por medio de un Centro De Atención Telefónica.
Tener una plataforma de reportes, donde se puedan consultar cada uno de los pagos recibidos por el cliente, devoluciones realizadas por el cliente, consolidado de pagos entre otra información.

Actividades: En la primera planeación se me asignó el módulo del procesamiento de pagos, una vez entregado se me asignó ayudar en el módulo de reportes de los pagos, pero como el proveedor asignado no tuvo avance significativo y al tener la fecha de entrega próxima, se tomó la decisión de realizar este módulo desde el comienzo.

En las siguientes páginas se describen cada una de las opciones que tiene esta plataforma.

[2] Compre ahora y empiece a pagar ciertos meses después, pueden incluir meses sin intereses.

Descripción de la plataforma

Módulo de Acceso al Sistema: Se compone de una pantalla donde se solicita el usuario y contraseña para poder ingresar al sistema, las validaciones se basan en las configuraciones ya utilizadas anteriormente en los demás proyectos de Pagos.mx.

En la Figura 2.2.1 se muestra la página web que utiliza el cliente para entrar al sistema mediante un usuario y una contraseña.

Figura 2.2.1. Acceso a la plataforma de pagos de la agencia de viajes

Una vez ingresado un usuario y contraseña de forma correcta se tienen dos opciones de direccionamiento dependiendo el perfil del usuario, Usuario Administrador que es la parte de los reportes de pagos del cliente y Usuario CallCenter que es la parte donde se ejecuta el cobro al cliente que llama por teléfono para hacer la reservación de su viaje.

Usuario Administrador.

Se tiene una pantalla de inicio que sirve como un pivote para la navegación de todas las opciones que ofrece el sistema.

En este caso se revisará el usuario administrador que es la sección del sistema donde se encuentran los reportes de pagos en sus diferentes modalidades y el control de los usuarios que pueden hacer uso del sistema.

Dentro de esta sección se encuentran diferentes opciones que puede acceder el usuario, puede hacer alta, actualización y baja de usuarios, obtener los reportes de los pagos de un periodo determinado de tiempo, entre otras opciones.

En la figura 2.2.2 se muestran las opciones que se tienen en el menú del usuario administrador, cada renglón es una opción y al dar clic se redirige la navegación a la opción elegida.

Figura 2.2.2. Menú de opciones para el usuario administrador.

Módulo de Administración de Usuarios: Su función es la de dar de alta, baja o modificar usuarios, entre los datos que se manejan son el nombre, el usuario, contraseña, email.

En la Figura 2.2.3 se muestra el módulo de administración de usuario, que está conformado por el formulario que se debe llenar para dar de alta un usuario y las opciones para buscar un usuario existente en el sistema.

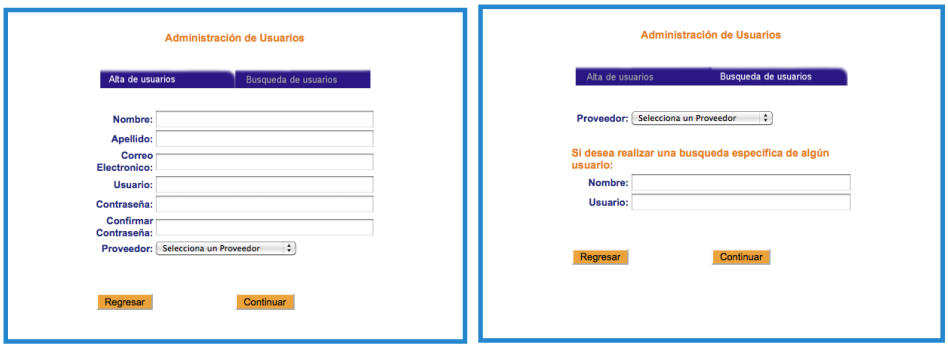


Figura 2.2.3. Módulo de administración de usuarios.

En la siguiente figura se muestra el formulario que es necesario llenar para ejecutar una actualización en la información del usuario.

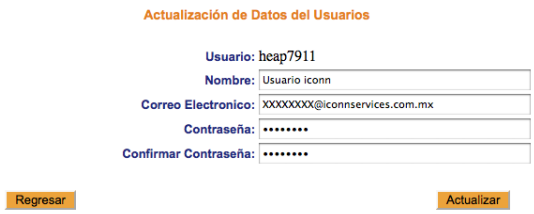


Figura 2.2.4. Módulo de actualización de información de usuarios.

Módulo de Reportes de Pagos

En esta parte tenemos una página inicial donde se muestran diferentes tipos de la búsqueda de pagos, se pueden buscar pagos de todo un mes, de un día, de un servicio[3], se puede hacer una búsqueda especifica de un folio de pago, además los resultados se pueden mostrar de diferente forma, ya sea un listado de pago por pago o un resumen de los montos totales de las ventas.

En la figura 2.2.5 se muestra un ejemplo de una búsqueda de pagos que puede utilizar el cliente, en este caso se busca un reporte Analítico, de todo el mes de marzo de 2013, de todos los servicios y todas las formas de pago y que el resultado este ordenado por medio de pago.

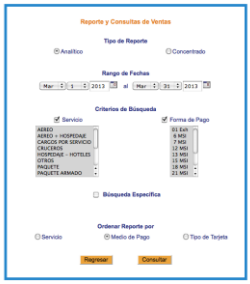


Figura 2.2.5. Módulo de Reportes de Pagos.

En la siguiente figura se ve un ejemplo de un resultado de una búsqueda de pagos de un reporte analítico, en este tipo de reporte aparece la información detallada de cada uno de los pagos, entre los datos destacados son la referencia que es un identificador del pago y el importe que se le cobro al tarjetahabiente.

[3] Servicio en el sistema corresponde a una clasificación que se hace para que el cliente lleve una mejor administración de los recursos obtenidos en sus ventas, en este caso tenemos servicios que se refieren a ventas de Vuelos, Hoteles, Renta de Autos, etc.

Fecha de Pago	Forma de Pago	Servicio	Cajero	Folio de Pago	Referencia	Número de TDC	Tipo de tarjeta	Importe Cobrado	Cargo Financiero	IVA	Total Cargo Financiero	Importe a Disp. al Prov.
01 de marzo de 2013												
	EXH	AEREO	Gdelgado	5855	4301-432-13	4101	PLATINUM	4,046.00	60.69	9.71	70.40	3,975.60
		VISAS	Gdelgado	62	4302-007-13	4772	BANCOMER	2,297.00	34.46	5.51	39.97	2,257.03
							Total EXH	6,343.00	95.15	15.22	110.37	6,232.63
	PUNTOS	AEREO	Gdelgado	5856	4301-432-13	4101	PLATINUM	1,000.00	15.00	2.40	17.40	982.60
		AEREO	Gdelgado	5857	4301-431-13	4101	PLATINUM	10,142.00	152.13	24.34	176.47	9,965.53
							Total PUNTOS	11,142.00	167.13	26.74	193.87	10,948.13
	12 MSI	HOSPEDAJE - HOTELES	Gdelgado	1768	4301-433-13	4555	V. ORO	13,423.00	201.35	32.22	233.57	13,189.43
							Total 12 MSI	13,423.00	201.35	32.22	233.57	13,189.43
							Total 01-03-2013	30,908.00	463.63	74.18	537.81	30,370.19
04 de marzo de 2013												
	EXH	HOSPEDAJE - HOTELES	Gdelgado	1770	4301-445-13	4101	PLATINUM	425.10	6.38	1.02	7.40	417.70
		PAQUETE	Gdelgado	1806	4301-443-13	4555	V. CLASICA	37,210.00	558.15	89.30	647.45	36,562.55
		AEREO	Gdelgado	5872	4301-442-13	4931	V. CLASICA	136.00	2.04	0.33	2.37	133.63
		AEREO	Gdelgado	5875	4301-442-13	4931	V. CLASICA	30.00	0.45	0.07	0.52	29.48
							Total EXH	37,801.10	567.02	90.72	657.74	37,143.36
	PUNTOS	HOSPEDAJE - HOTELES	Gdelgado	1769	4301-438-13	4555	INFINITE	3,579.10	53.69	8.59	62.28	3,516.82
		HOSPEDAJE - HOTELES	Gdelgado	1771	4301-445-13	4101	PLATINUM	6,008.90	90.13	14.42	104.55	5,904.35
		AEREO	Gdelgado	5863	4301-436-13	4931	V. ORO	2,370.60	35.56	5.69	41.25	2,329.35
		AEREO	Gdelgado	5865	4301-434-13	4555	INFINITE	6,838.00	99.57	15.93	115.50	6,522.50
		AEREO	Gdelgado	5866	4301-437-13	4931	V. ORO	4,765.00	71.48	11.44	82.92	4,682.08
		AEREO	Gdelgado	5868	4301-440-13	4101	PLATINUM	14,642.00	219.63	35.14	254.77	14,387.23
		AEREO	Gdelgado	5869	4301-442-13	4101	EDUCACIÓN	1,426.00	21.39	3.42	24.81	1,401.19
		AEREO	Gdelgado	5870	4301-442-13	4931	V. ORO	739.00	11.09	1.77	12.86	726.14
		AEREO	Gdelgado	5871	4301-442-13	4931	V. ORO	226.00	3.39	0.54	3.93	222.07
		AEREO	Gdelgado	5873	4301-442-13	4931	V. CLASICA	408.00	6.12	0.98	7.10	400.90
							Total PUNTOS	40,802.60	612.05	97.92	709.97	40,092.63
	SKIP	CRUCEROS	Gdelgado	546	4301-435-13	4555	V. CLASICA	37,356.44	560.35	89.66	650.01	36,706.43
		AEREO	Gdelgado	5874	4301-444-13	4101	PLATINUM	16,755.48	251.33	40.21	291.54	16,463.94
							Total SKIP	54,111.92	811.68	129.87	941.55	53,170.37
	6 MSI	PAQUETE	Gdelgado	1805	4301-443-13	4931	V. CLASICA	40,000.00	600.00	96.00	696.00	39,304.00
		PAQUETE	Gdelgado	1807	4301-443-13	4555	V. CLASICA	40,000.00	600.00	96.00	696.00	39,304.00
							Total 6 MSI	80,000.00	1,200.00	192.00	1,392.00	78,608.00

Figura 2.2.6. Listado de información de los pagos recibidos en la plataforma.

En la siguiente figura se muestra el resultado de una consulta de pagos con un reporte concentrado, que es un resumen de los montos totales de los pagos, en este caso están agrupados por medio de pago, al final del reporte se muestra la suma de cada rubro (IVA, comisiones, entre otros) para todos los medios de pago.

Concentrado de Ingresos
Periodo: 01-03-2013 al 31-03-2013

	Importe Cobrado	Cargo Financiero	IVA	Total Cargo Financiero	Importe a Dispersar al Proveedor
Financiamiento					
1 EXH	603356.72	9194.98	1471.21	10666.19	592690.53
Puntos	1443729.90	22559.38	3609.48	26168.86	1417561.04
3 Skip 13 MSI	474197.55	7112.99	1138.09	8251.08	465946.47
6 MSI	274195.36	7767.20	1242.75	9009.95	265185.41
7 MSI	61358.35	920.38	147.26	1067.64	60290.71
12 MSI	220775.00	3569.14	571.08	4140.22	216634.78
13 MSI	235877.26	3538.16	566.10	4104.26	231773.00
15 MSI	26324.00	394.86	63.18	458.04	25865.96
18 MSI	120254.00	1803.82	288.61	2092.43	118161.57
21 MSI	471158.00	7516.28	1202.61	8718.89	462439.11
24 MSI	2264801.73	81807.51	13089.23	94896.74	2169904.99
Total Ingresos 01-03-2013 al 31-03-2013	6196027.87	146184.70	23389.60	169574.30	6026453.57

Figura 2.2.7. Concentrado de los pagos agrupados por medio de pago.

Módulo de Consolidado de pagos

Este módulo es otro tipo de reporte para mostrar los montos totales de pagos por cada uno de los proveedores[4], en este caso se muestra el monto total de cada uno de los días del periodo elegido en la página de inicio del módulo.

En la figura 2.2.8 se muestra el formulario con las opciones que se tienen para hacer la búsqueda de pagos con este tipo de reporte, se puede buscar un proveedor en específico o todos juntos, al igual que buscar por un servicio o todos los existentes y al final se debe elegir el periodo de tiempo requerido.

Figura 2.2.8. Módulo de consolidado de pagos.

En la figura 2.2.9 se muestra un ejemplo de un resultado de una búsqueda en este módulo, como se observa existen columnas como Importe Cobrado, el Cargo Financiero y el IVA, entre otros, en cada columna se despliega la información por día y al final el total acumulado en cada rubro en el periodo de tiempo seleccionado.

	Importe Cobrado	Cargo Financiero	IVA	Total Cargo Financiero	Importe a Dispersar al Proveedor
01-octubre-2012	25.00	0.35	0.06	0.82	24.59
09-octubre-2012	1400.00	19.60	3.13	45.46	1377.27
03-enero-2013	200.00	2.80	0.44	6.48	196.76
18-enero-2013	234.00	3.28	0.52	7.60	230.20
Totales	**1859.00**	**26.03**	**4.15**	**60.36**	**1828.82**

Figura 2.2.9. Listado de consolidado de pagos agrupados por día.

[4] Proveedores es un término que en el sistema se refiere a las diferentes empresas que en algún momento se pensó que iban a asociarse con el cliente e iban a utilizar la plataforma para realizar sus ventas por Internet. Hasta el momento no existe algún proveedor asociado.

Usuario CallCenter.

La segunda parte de esta sección es el módulo donde se procesan los pagos, como se explicó anteriormente la empresa tenía una dinámica especial para hacer la venta de sus paquetes de viaje. El cliente cuenta con una página web en donde se le muestran sus paquetes de viaje, todo lo que incluía cada uno, así como su precio, si un usuario está interesado en realizar una reservación debe marcar a un callcenter, el personal que atiende al usuario tiene el acceso a esta plataforma de Pagos.mx donde una vez iniciada la sesión debe llenar un pequeño formulario donde se indica qué servicio está contratando el usuario, así como el folio de reservación que es el número de contrato, el monto total a cobrar por el paquete de viaje y por último el nombre de quien está haciendo la venta.

En la siguiente figura 2.2.10 se muestra el formulario llenado con datos de prueba para ilustrar el proceso, como se puede ver es muy sencillo y rápido de llenar.

Figura 2.2.10. Formulario para iniciar el cobro.

Una vez llenado el formulario el siguiente paso es la pantalla que se ilustra en la figura 2.2.11, en ella podemos ver los medios de pagos disponibles para realizar el pago, se pueden elegir varias opciones indicando el monto correspondiente a cada una de ellas, en este paso se deben llenar los datos de la tarjeta de crédito o débito, las tarjetas de débito solo pueden hacer cobro en una sola exhibición mientras que las tarjetas de crédito si pueden tener las opciones de pagar a mensualidades sin intereses, cobro con puntos de

recompensa bancaria y el medio de pago de compre ahora y pague a partir del siguiente mes.

También se cuenta con una opción de consulta de puntos, que se utiliza en caso de que el usuario requiera saber la cantidad de puntos que tiene en su cuenta para poder hacer el pago con ese método.

Figura 2.2.11. Medios de pago disponibles para el cobro.

Una vez elegidos los medios de pago se enviaban para su autorización, en ella el banco indicaba si los pagos fueron aceptados o rechazados.

En la siguiente figura se muestra como ejemplo el resultado de enviar el cobro a tres medios de pago diferente, en este caso el medio de pago de puntos si tuvo una respuesta positiva de parte del banco, mientras los pagos de una sola exhibición y de meses sin intereses fueron rechazados por el banco, se muestran los montos que fueron cobrados y los que faltan por cobrar, en caso de que existan pagos rechazados.

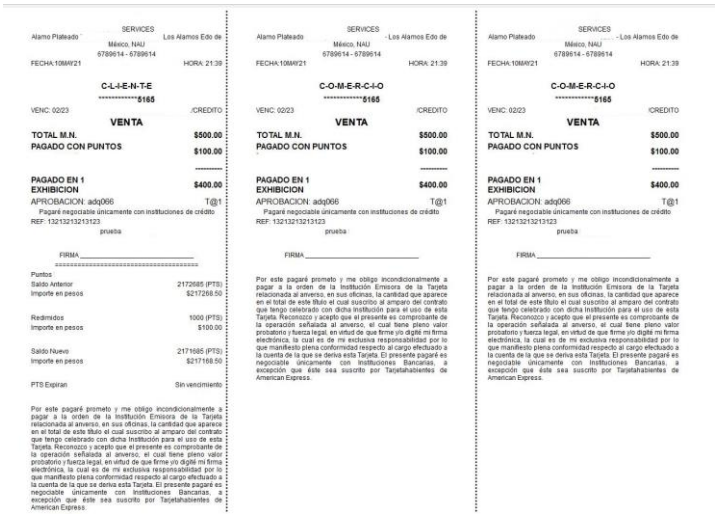
Figura 2.2.12. Resultado de la autorización bancario.

La última pantalla es la que se muestra en la figura 2.2.13, en ella se presenta un resumen de los pagos que tiene el usuario con datos importantes para identificarlos, como el medio de pago, el número de tarjeta, la autorización y el estatus del pago, además por cada pago se tiene la opción de reimprimir el comprobante de pago, enviar dicho comprobante al usuario vía correo electrónico y la posibilidad de realizar la cancelación del pago.

Figura 2.2.13. Información de cada pago realizado por el usuario.

Para finalizar este módulo de cobro se muestra en la figura 2.2.14 un ejemplo del comprobante de pago, en este caso está un poco editado por un tema de marcas registradas, pero se muestra información del banco, de la empresa que está haciendo el cobro, montos de la transacción, datos importantes como la aprobación bancaria, los últimos dígitos de la tarjeta, fecha de cobro entre otros.

Para este comercio se realizó un formato de comprobante de pago especial, ya que en una hoja de papel deseaban imprimir tres comprobantes de pago, uno para el usuario y dos para el comercio con el objetivo de llevar el control y contabilidad de sus ventas.



SERVICES

Alamo Plateado Los Alamos Edo de México, NAU

6789614 - 6789614

FECHA:10M/Y21 HORA: 21:39

C-L-I-E-N-T-E

**********5165

VENC: 02/23 /CREDITO

VENTA

TOTAL M.N.	$500.00
PAGADO CON PUNTOS	$100.00
PAGADO EN 1 EXHIBICION	$400.00

APROBACION: adq066 T@1

Pagaré negociable únicamente con instituciones de crédito

REF: 13213213213123

prueba

FIRMA _____

Puntos	
Saldo Anterior	2172685 (PTS)
Importe en pesos	$217268.50
Redimidos	1000 (PTS)
Importe en pesos	$100.00
Saldo Nuevo	2171685 (PTS)
Importe en pesos	$217168.50
PTS Expiran	Sin vencimiento

Por este pagaré prometo y me obligo incondicionalmente a pagar a la orden de la Institución Emisora de la Tarjeta relacionada al anverso, en sus oficinas, la cantidad que aparece en el total de este título el cual suscribo al amparo del contrato que tengo celebrado con dicha Institución para el uso de esta Tarjeta. Reconozco y acepto que el presente es comprobante de la operación señalada al anverso, el cual tiene pleno valor probatorio y fuerza legal, en virtud de que firmo y/o digité mi firma electrónica, la cual es de mi exclusiva responsabilidad por lo que manifiesto plena conformidad respecto al cargo efectuado a la cuenta de la que se deriva esta Tarjeta. El presente pagaré es negociable únicamente con Instituciones Bancarias, a excepción que éste sea suscrito por Tarjetahabientes de American Express.

SERVICES

Alamo Plateado Los Alamos Edo de México, NAU

6789614 - 6789614

FECHA:10M/Y21 HORA: 21:39

C-O-M-E-R-C-I-O

**********5165

VENC: 02/23 /CREDITO

VENTA

TOTAL M.N.	$500.00
PAGADO CON PUNTOS	$100.00
PAGADO EN 1 EXHIBICION	$400.00

APROBACION: adq066 T@1

Pagaré negociable únicamente con instituciones de crédito

REF: 13213213213123

prueba

FIRMA _____

Por este pagaré prometo y me obligo incondicionalmente a pagar a la orden de la Institución Emisora de la Tarjeta relacionada al anverso, en sus oficinas, la cantidad que aparece en el total de este título el cual suscribo al amparo del contrato que tengo celebrado con dicha Institución para el uso de esta Tarjeta. Reconozco y acepto que el presente es comprobante de la operación señalada al anverso, el cual tiene pleno valor probatorio y fuerza legal, en virtud de que firmo y/o digité mi firma electrónica, la cual es de mi exclusiva responsabilidad por lo que manifiesto plena conformidad respecto al cargo efectuado a la cuenta de la que se deriva esta Tarjeta. El presente pagaré es negociable únicamente con Instituciones Bancarias, a excepción que éste sea suscrito por Tarjetahabientes de American Express.

SERVICES

Alamo Plateado Los Alamos Edo de México, NAU

6789614 - 6789614

FECHA:10M/Y21 HORA: 21:39

C-O-M-E-R-C-I-O

**********5165

VENC: 02/23 /CREDITO

VENTA

TOTAL M.N.	$500.00
PAGADO CON PUNTOS	$100.00
PAGADO EN 1 EXHIBICION	$400.00

APROBACION: adq066 T@1

Pagaré negociable únicamente con instituciones de crédito

REF: 13213213213123

prueba

FIRMA _____

Por este pagaré prometo y me obligo incondicionalmente a pagar a la orden de la Institución Emisora de la Tarjeta relacionada al anverso, en sus oficinas, la cantidad que aparece en el total de este título el cual suscribo al amparo del contrato que tengo celebrado con dicha Institución para el uso de esta Tarjeta. Reconozco y acepto que el presente es comprobante de la operación señalada al anverso, el cual tiene pleno valor probatorio y fuerza legal, en virtud de que firmo y/o digité mi firma electrónica, la cual es de mi exclusiva responsabilidad por lo que manifiesto plena conformidad respecto al cargo efectuado a la cuenta de la que se deriva esta Tarjeta. El presente pagaré es negociable únicamente con Instituciones Bancarias, a excepción que éste sea suscrito por Tarjetahabientes de American Express.

Figura 2.2.14. Comprobante de pago.

Resultados: El proyecto principal se liberó con éxito no sin antes tener que pasar por varias dificultades como es la rotación de personal y trabajar en horas fuera del horario laboral para cumplir los tiempos establecidos con el cliente. Una vez liberado, se realizaron cambios mínimos en leyendas, en ubicación de datos dentro de los reportes y cuestiones que el cliente identificó una vez haciendo uso de la aplicación en su operación diaria.

El proyecto se llevó a cabo de octubre de 2010 a enero de 2011 y desde entonces la aplicación ha funcionado correctamente cumpliendo con el objetivo de hacer los cobros del cliente y tener una serie de reportes con todos los pagos realizados en tiempo real, esto es, sin esperar que el banco emita estados de cuentas.

Este proyecto lo pude llevar acabo con la experiencia adquirida en el tiempo que llevaba en la empresa, pero hago hincapié que sin los fundamentos obtenidos en la facultad no hubiera podido desarrollar las habilidades obtenidas, en esta caso me gustaría mencionar la materia de Base de Datos, ya que con ayuda del conocimiento adquirido en esa asignatura diseñe un esquema de tablas que ayudaron a guardar los datos de los usuarios, el normalizarlas, el saber que dato era la llave primaria o si debía crear llaves foráneas. La explotación de estos datos en los reportes, en la parte de la administración de usuarios, que son inserciones, consultas y actualizaciones a la Base de Datos.

2.3 Migración a nueva plataforma.

Objetivos. Hacer el volcado de información de una estructura de Base de Datos creada hace unos 15 años a una nueva, así como homologar funcionalidades especiales que tenía cada uno de los clientes para que su migración a la nueva plataforma fuera lo más transparente posible.

Actividades. Análisis de la Base de Datos de la plataforma de pagos antigua, obtener la correspondencia entre las columnas de la nueva Base de Datos, migrar configuraciones de los clientes, así como todo el historial de sus pagos.
En base al análisis se crean consultas o procesos de Base de Datos para automatizar el volcado de la información entre la BD de DB2 de la plataforma de pagos antigua y la BD de Oracle de la nueva plataforma.
El ejemplo principal de esta actividad es la tabla de configuraciones en la BD antigua, la cual tenía toda la información de cada uno de los clientes, contratos, servicios y la cual solo estaba ligada a 3 catálogos.
En la nueva estructura esta configuración se extiende alrededor de 15 tablas para poder obtener la misma información de cada cliente.
Se realizan diferentes actividades para homologar las plataformas, como por ejemplo la creación de balanceadores que fueron la solución para que el cliente no tuviera que hacer cambios en sus sistemas ya que los parámetros requeridos para procesar un pago cambiaron radicalmente. En estos balanceadores se configuraban los parámetros que se recibían anteriormente y a cuál parámetro nuevo equivaldría.

Resultados. Se migró al 100% las configuraciones de los clientes, así como los pagos que se tenían en el historial del cliente.

La fecha aproximada de estas tareas fue de octubre del 2013 a agosto 2015.

3

BackOffice en Plataforma de Cobranza Electrónica.

Hace más de quince años Pagos.mx incursiona en el área de pagos en línea con la intención de resolver el problema de agilizar el proceso del cobro a los proveedores que tenían el objetivo de vender productos en la plataforma de subastas de una empresa de telefonía. Con el respaldo de otra de las compañías subsidiarías de Pagos.mx, se empieza a comercializar la nueva plataforma como producto a grandes clientes del banco, así fue creciendo la plataforma de cobranza captando los impuestos de todos los estados de la República Mexicana y con grandes y pequeños comercios interesados en tener una herramienta de cobro en línea y que el dinero captado en esta plataforma se depositara en sus cuentas de forma rápida y sin gastos de cobranza.

El BackOffice nace en la necesidad de administrar los pagos de todos los clientes y cumplir en tiempo y forma el depósito del dinero de cada una de las transacciones recibidas por los usuarios, además de mostrar de forma confiable y transparente la información de los pagos al cliente.

Como definición general el BackOffice es un portal en línea en el cual se muestra en tiempo real cada uno de los pagos realizados en el sistema, con el detalle de qué tarjeta habiente realizó el pago, qué concepto, producto o servicio corresponde a éste, así como el monto total de la transacción, además de indicar si el pago ya se depositó en la cuenta del cliente o en qué estatus se encuentra.
Es la principal ventaja que se ofrece al cliente ya que se le da una herramienta útil para que tenga su contabilidad y sus reportes de pagos en un par de clics.

Pero el BackOffice no solo es la plataforma de reportes, este proyecto se divide en diferentes procesos para cumplir con el cobro de los pagos al tarjetahabiente y tener correcta la información para hacer los depósitos correspondientes a los clientes, pero al tener diversos medios de pagos, se requiere cumplir con diferentes tareas dedicadas a la comunicación en diferentes canales para el cobro de las transacciones.

Para ejemplificar lo que se comenta anteriormente se pueden mencionar los medios de pagos que ofrece la plataforma de pagos, con un crecimiento de transacciones y con la finalidad de tener diversas opciones para que el cliente final pueda hacer los pagos por el

sistema, se han implementado pagos con plataformas ajenas al banco como serían American Express, PayPal, además de los pagos con Tarjeta de Crédito Visa y MasterCard, pagos con Cheque en Línea, SPEI, cuentas interbancarias e impresión de fichas para el pago en Sucursales bancarias.

La figura 3.1 que se muestra a continuación, presenta los logos de los diferentes medios de pago que al mismo tiempo son empresas que tienen un reconocimiento mundial.

Figura 3.1. Medios de pagos

A lo largo de la vida de la plataforma se han usado diferentes tecnologías para la administración del código, repositorios, cada desarrollador utiliza el ide y los *frameworks* que mejor cumplan con las funcionalidades que va a implementar, y cabe mencionar que todo está desarrollado en el lenguaje java, complementando la base está en javascript con HTML y CSS.

Como se ha mencionado anteriormente, la plataforma tiene más de 15 años en funcionamiento por lo que la base de todo el sistema se realizó con tecnología de ese entonces, se usó para la navegación web unos componentes llamados Servlets, que son clases de java con comunicación web, en los cuales se pueden enviar y recibir peticiones desde un HTML y mostrar información creando código HTML, en muchos procesos se utilizaban este tipo de método para mostrar la información en una página web, hasta que

se empezaron a usar JSP's (Java Server Pages), por ser dinámicos y se puede insertar código Java en el caso de necesitarlo.
Siguiendo con la evolución del sistema, se han utilizado en diferentes partes de la plataforma tecnologías recientes y compatibles, por ser más fáciles de administrar, por ser más seguras y por supuesto de mayor facilidad en su desarrollo.

Los procesos y sistemas del portal están instalados en servidores físicos y administrados con Websphere[5] de IBM.
Se cuenta con procesos que están afuera del Websphere y que están desarrollados para que se ejecuten de manera rápida sin depender de otros proyectos.

Dichos desarrollos están hechos mediante *shells* de Linux para poder controlar los horarios de ejecución, y los parámetros que se van a mandar a cada una de las clases java que se van a ejecutar.

Acerca del portal del BackOffice

El sistema BackOffice consta de diferentes reportes y estos se muestran según el perfil que se asigne al usuario, por lo general el cliente tiene acceso a los reportes más básicos como son el Informativo Genérico, que es un desglose de cada uno de los pagos, otro reporte es el Envío Genérico el cual es utilizado para conciliar los pagos en el sistema del cliente.

Dentro de las opciones que se tienen en el Back Office se encuentran los procesos para que el área de Operaciones haga sus tareas de conciliar, dispersar, cobrar de comisiones, así como la ejecución de devoluciones.

Existen opciones especializadas, estos son reportes que tuvieron un requerimiento especial de parte del cliente, entre los ejemplos son reportes que contienen pagos de un medio de pago que denominamos solo sucursal, los cuales son pagos que se hacen en la sucursal

[5] Nombre de la consola de administración de los servidores de IBM

bancaria, es decir que no utilizan la plataforma de pagos, para tener la información, el banco nos proporciona los registros de estos pagos diariamente. Otro ejemplo puntual son los reportes que se mandan en un formato Excel, en el cual están los pagos mensuales del cliente y se separan en varias páginas por filtros, como pagos con tarjeta de crédito, pagos de tarjeta de débito, así como separados por el concepto que se cobró.

En la siguiente figura 3.2 se muestran las opciones que se tienen en el BackOffice, estas opciones son para un usuario con todos los permisos, la opción de Reportes nuevo gel, es donde está la mayoría de las opciones.

Figura 3.2. Menú de opciones del BackOffice

El reporte más utilizado es el Informativo Genérico ya que en él se encuentran los datos principales de todos los pagos, los cuales son el concepto de pago, el medio de pago

utilizado por el tarjetahabiente, el monto pagado, un dato llamado referencia el cual es uno de los identificadores del pago, el estatus en el que se encuentra esa transacción, el cual puede ser; pagado, conciliado, dispersado (que el dinero ya se depositó a la cuenta del comercio) o si el pago fue devuelto.

En la siguiente figura 3.3 se muestra una parte del Informativo Genérico, se puede observar columnas que nos indican los datos principales del pago, estos son el folio de pago, que es un numero consecutivo o id en la Base de Datos, se observa el folio empresa y referencia empresa los cuales son datos que envía el sistema del cliente y sirven como identificadores para evitar pagos duplicados, el nombre del usuario y el monto que se pagó en cada transacción.

INFORMATIVO GENERICO

N	FOLIO DE PAGO	FOLIO EMPRESA	REFERENCIA EMPRESA	FECHA DE DISPERSION	NOMBRE	RFC	TOTAL COBRADO [PESOS]	TOTAL IMPORTE [PESOS]
	9061996	169	2170118000301AR70835		Tarjeta Prueba UNAM		202.52	202.52
	9062005	170	2170118000302AR60829		Tarjeta Prueba UNAM		272.52	272.52
	9062008	171	2170118000303AR00835		Tarjeta Prueba UNAM		522.52	522.52
	9062018	172	2170118000304AR20880		Tarjeta Prueba UNAM		252.52	252.52
	9062019	173	2170118000305AR50845		Tarjeta Prueba UNAM		352.52	352.52
	9062023	174	2170118000306AR60873		Tarjeta Prueba UNAM		272.52	272.52
	9062025	175	2170118000307AR60884		Tarjeta Prueba UNAM		272.52	272.52
	9062030	177	2170118000309AR70826		Tarjeta Prueba UNAM		202.52	202.52
							2350.16	**2350.16**
							2350.16	**2350.16**
							2350.16	**2350.16**
	9062233	154	4420118000254AT30804		FXVXCVXV		511.00	511.00
	9062248	178	2170118000310AU60877		Tarjeta Prueba IIJ		272.52	272.52
	9062250	179	2170118000311AU10800		Tarjeta Prueba IIJ		222.52	222.52
	9062256	180	2170118000312AU70816		Tarjeta Prueba IIJ		202.52	202.52
	9062266	184	2170118000313AU50893		Tarjeta Prueba IIJ		352.52	352.52
	9062267	185	2170118000314AU40887		Tarjeta Prueba IIJ		212.52	212.52

Figura 3.3. Informativo Genérico pagos de prueba de la UNAM

Como se puede ver en la imagen anterior en este reporte se muestra la información de cada uno de los pagos, teniendo subtotales, los cuales se muestran en letras negritas, y se obtienen ya sea por día, por servicio de pago y por sucursal donde se realizó el pago. Así como el gran total de todos los pagos contenidos en este reporte.

El otro reporte mencionado anteriormente y que se utiliza diariamente para que el comercio pueda ingresarlo a su sistema y poder identificar los pagos que se depositaron a su cuenta al cual se le llama Envío Genérico, los datos que contienen así como la ubicación dentro del archivo depende de los requerimientos de cada cliente, pero la mayoría contienen datos como la referencia de pago, la autorización que asigno el banco una vez aceptada la transacción, monto pagado, el identificador que nuestra plataforma le asigna. Este reporte además de poder obtenerlo desde el portal del BackOffice también existe la opción de enviarlo directamente y en automático al servidor del comercio con un envío FTP o SFTP.

En la siguiente figura 3.4 se muestra un ejemplo de un archivo que se envía a uno de los principales clientes, este cliente tiene un layout específico para que su sistema pueda obtener la información y actualizarla, entre los datos se encuentran la autorización bancaria, la fecha y la referencia para cada uno de los pagos.

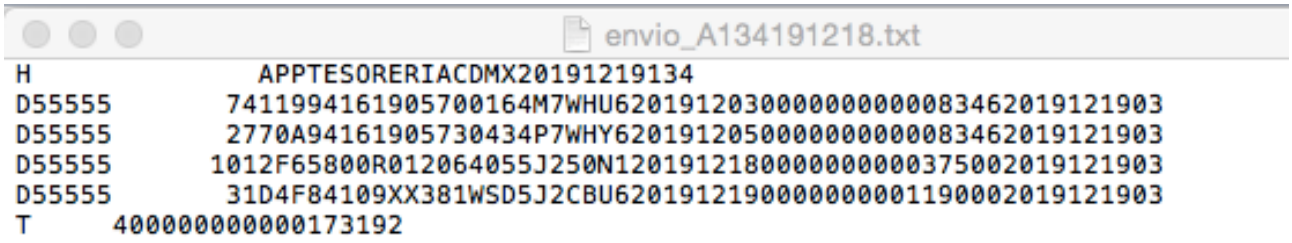


Figura 3.4. Ejemplo de un archivo de conciliación.

En la siguiente parte se describen cada una de las tareas realizadas en este proyecto.

- **Soporte al área de Operación Central.**

Objetivo. Que la funcionalidad del portal este totalmente disponible para que el área de OPC pudiera realizar sus operaciones diarias, entre lo que destaca, la conciliación de los pagos diarios de todos los clientes y la dispersión del dinero de estos pagos a las cuentas de los clientes.

Funciones. Recibir reportes de algún problema y buscar la solución del mismo, en este tipo de actividad se podían dar muchas peticiones posibles y las cuales podían ser causadas por la degradación del servidor ya fuera por memoria o por alguna falla en las consultas a

la Base de Datos, errores en código, esto es que no se estuviera tomando en cuenta alguna condición o algún tipo de dato y esto hiciera que el sistema hiciera acciones que no correspondiera a lo que se deseaba hacer, también se dan casos que la información no era la misma entre los sistemas del banco y del BackOffice, en cada uno de los casos el área de OPC reportaba la falla a nuestra área.

Resultados. El tiempo de respuesta en dar solución a los problemas tenía que ser casi inmediata ya que los procesos que realiza el área de OPC tienen tiempo límite para realizarlos, con esto se adquirió un gran conocimiento de la plataforma y los procesos ejecutados por el BackOffice ya que era necesario saber por dónde empezar a buscar la falla y de ahí seguir el proceso y encontrar la solución, en la parte técnica además del conocimiento de programación de java, javascript se adquirió conocimientos de Unix, ya que algunos procesos eran directos al servidor sin tener un administrador de servidores como WebSphere para el monitoreo de aplicaciones.
Estos conocimientos se utilizaban también para la creación y mejora de shell's que eran generados para la ejecución de tareas programadas.
Otro aspecto importante es la de pedir información de la BD, en algunos casos no se tenía información del problema que nos facilitara la tarea y se tenía que crear consultas SQL con la poca información y de ahí obtener algo que nos sirviera para solucionar el problema.

- **Correcciones de bugs.**

Objetivo. Mantener la plataforma libre de errores y trabajar en soluciones si es que se reportaba algún error.

Funciones. Buscar errores en la plataforma ocasionados por algún código realizado mucho tiempo atrás y que, por motivos de nuevos procesos, la utilización de nuevas plataformas o parámetros se pudiera crear un bug en el sistema, así como la corrección para que la plataforma o algún proceso trabajara correctamente.

Resultado.

La mayor parte de código de este proyecto tenía mucho tiempo funcionando y funcionaba bien, cumpliendo con los objetivos de cuando fue generado, pero como los clientes van cambiando y van necesitando diferentes funcionalidades y las existentes se vuelven obsoletas o simplemente no funcionaban para nuevos casos, se presentaban fallas ya que no se analizaban todos los procesos, la mayor parte por desconocimiento de dicho proceso o por pensar que el proceso actualizado no era utilizado en otra parte del sistema.

Hay muchos ejemplos que se presentaron en esta parte, y es la que absorbía más tiempo laboral, ya que eran casos extremadamente raros, código que no fallaba un día antes, al darse un alta de algún cliente, de plataforma, algún cambio en la configuración, esto era suficiente para que se presentara el fallo en el portal.
En este caso como el anterior el conocimiento de los procesos era esencial, así como el manejo de Java para encontrar el error y poder corregirlo, no sin antes validar casos que no teníamos considerados anteriormente.

- **Mejoras de los procesos de conciliación.**

Objetivo. Mejorar un proceso de conciliación para una nueva plataforma de pagos.

Funciones. Una tarea realizada en este punto fue la de mejorar una funcionalidad que conciliaba los pagos de una plataforma llamada interred, versión 3.4, el sistema trabajaba correctamente cuando los pagos que se procesaban diario eran menos de 5 mil, pero se dio de alta un cliente que tenía la cantidad de pagos de casi 10 veces esta cifra, el proceso tardaba 2 horas en terminar con todas las tareas que ejecutaba, esto no daba margen de error por temas de que el principal resultado del proceso era un archivo que se enviaba al banco para el cobro de las transacciones teniendo un tiempo límite y algún error no se podía procesar nuevamente la conciliación y ocasionar que no se cobraran las transacciones del día anterior teniendo como consecuencias sanciones económicas y hasta legales con los clientes.

Las funciones en este punto fue interpretar el código que se tenía y mejorarlo, se optimizó la consulta a la BD, de tal forma que se eliminaron funciones en código que hacían que el

proceso aumentara su tiempo de ejecución, se utilizaron librerías recientes para aumentar la eficacia en las funcionalidades, una de estas funcionalidades es la de realizar actualizaciones en bloques, esto es, actualizar muchos pagos a la vez y no uno por uno como se venía haciendo. Después de los cambios en código se realizaron pruebas exhaustivas en el ambiente de pruebas ya que era un tema delicado si en algún momento fallaba.

Resultados. Se obtuvo nuevo conocimiento técnico, ya que con el manejo de nuevas tecnologías para hacer procesos que se hacían anteriormente, el entender la lógica del proceso y todas sus vertientes fue clave en este ajuste, ya que se pudo realizar una nueva arquitectura del proceso.

Con todos los cambios realizados se logró que un proceso que duraba 2 horas en su ejecución en la actualidad utiliza solamente 15 minutos en terminar de procesar la misma cantidad de transacciones y tener listo el archivo a enviar al proveedor para el cobro.

Este ajuste dio tiempo de sobra para tener una reacción en caso de error y poder actuar en una solución en caso de que se presentara alguna contingencia en los servidores o Base de Datos.

En la siguiente figura 3.5 se muestra uno de los ajustes que se hicieron en el código, en la parte de la izquierda se muestra en la segunda línea el llamado a un método el cual hacía la consulta de todos los pagos y en unas líneas después comienza una iteración, cuyo objetivo era ordenar pago por pago dependiendo de la moneda con la que se había realizado la transacción. En la parte de la derecha es el código nuevo o mejorado y como se muestra ya no existe la iteración, los pagos se separaron haciendo dos llamados a un método donde se realiza la consulta en la Base de Datos.

Figura 3.5. Muestra de cambio de código de una versión a otra.

En la siguiente figura 3.6 se puede observar otro de los cambios significativos entre versiones, en la parte de la izquierda se puede observar que se hacía de nuevo la consulta global y posteriormente se actualizaba mediante una iteración del resultado de esa consulta pago por pago. En la parte de la derecha, la mejora fue eliminar la consulta ya que los datos ya se habían obtenido desde el principio y las actualizaciones se hacen por bloques para que las actualizaciones fueran más rápidas.

Figura 3.6. Diferencia en las actualizaciones entre versiones.

- **Adaptación de aplicación para el envío de archivos.**

Objetivo. Hacer que el proceso de envío de archivos obtenidos de un aplicativo del Banco y que solo se podían obtener desde una computadora localizada en la oficina de la empresa se ejecutara automáticamente sin la necesidad de que personal del área de Operaciones estuviera presente en la oficina.

Funciones. Adaptar una aplicación realizada anteriormente para que trabajará sin la necesidad de tener que darle clic para iniciar el proceso, se realizaron ajustes en código mediante Swing[6] y con la ayuda de Tareas[7] se hizo el manejo para que la ejecución del proceso principal se hiciera en determinado tiempo sin la ayuda del personal. Este aplicativo se instaló en tres máquinas diferentes con condiciones especiales cada una, pero con el mismo propósito general para todas.
Adicionalmente se realizó una nueva versión de este aplicativo, una función en java sin la imagen que nos daba Swing, con esto eliminamos funciones que solo se utilizaban para la estética de la aplicación y se generó algo simple y rápido para cumplir este proceso.

Resultado. Fue difícil trabajar con código realizado por otras personas y del cual no se contaba con documentación técnica para saber porque se realizaban diversas funcionalidades. Al principio solo adecué lo mejor posible el código existente y al final hice a un lado la cuestión estética y solo tener una pantalla del código del sistema de Windows y un log para el monitoreo de la aplicación.
Entre las mejoras que resultaron de este ajuste fue que el personal del área de Operaciones que anteriormente iba a la oficina diariamente se pudo organizar y solo estar presente una persona al día para el monitoreo de estos procesos, con esto el resto del equipo de esa área pudo trabajar vía remota.

[6] Librería de java para crear interfaces gráficas

[7] Librería de java para el manejo de procesos dentro de una aplicación.

- **Convergencia entre plataformas**

Objetivo. Que la plataforma de pagos aquí mencionada tuviera comunicación con la nueva versión de la misma plataforma de pagos, pero realizada en la nube de Amazon.

Funciones. Mediante el consumo de WebServices, se debía mandar información de pagos a la nueva plataforma, para poder realizar reportes de pagos solicitados por el banco.

Resultados. Al tener muchas limitaciones en usar nuevas tecnologías en el sistema se tenía que usar librerías no tan recientes para que esta comunicación se diera correctamente, al final se pudo cumplir con los objetivos planteados y se podía explotar este proceso para obtener correctamente los reportes necesarios para enviarlos al banco.

- **Ajustes de archivos Envío Genérico.**

Objetivo. Proporcionar al cliente un archivo con los pagos realizados y cobrados el día anterior para que pudieran actualizar los estatus en su sistema.

Funciones. Cumplir mediante un layout, el cual podía ser a petición del cliente, la generación de un archivo, conteniendo la información necesaria para los procesos del cliente, este archivo se genera mediante la explotación de la información contenida en la Base de Datos y que cumplía con las características que el cliente utilizaba en sus sistemas para reconocer los pagos y poder entregar el comprobante correspondiente a sus usuarios.
Resultados. Se cumplió con los requerimientos que solicitaba el cliente, layout y horarios de envío del archivo. Se implementaron diferentes tipos de envío para depositar el archivo al servidor del cliente, cumpliendo con las normas de seguridad ya que en algunos casos los datos contenidos en el archivo era información sensible. Se utilizaba Unix para la conexión a los servidores de los clientes, ya fueran transferencias SFTP, FTP o SCP, además de en algunos casos utilizar clientes de conexión como SSH Client, WinSCP o Filezilla.

- **Cumplir con los requerimientos de PCI en el portal del BackOffice.**

Objetivo: Cada año se ejecuta una auditoria para obtener la certificación de PCI y poder seguir operando pagos con tarjetas de crédito, con lo cual el portal del BackOffice tenía que cumplir los aspectos de dicha auditoria.

Funciones. Antes de la auditoria se hacía un escaneo del portal mediante herramientas en busca de vulnerabilidades y de ese escaneo se debía trabajar en solucionar cada una de las vulnerabilidades, las acciones que se hacían podían ser cambiar alguna librería, modificar código del portal o agregar código, así como configuraciones en el servidor.

Resultados. Cada año pudimos cumplir los requisitos para obtener la certificación de PCI Secure y así poder seguir operando operaciones con tarjetas de crédito, el portal al cumplir con estos requisitos era difícil de hackear y en general no teníamos sorpresas de ataques.

En la siguiente figura 3.7 se muestran ejemplos de vulnerabilidades obtenidas en un escaneo al BackOffice, se indica el nombre de la vulnerabilidad y una solución a ejecutar.

Análisis de vulnerabilidades	Solución indicada
1. Encabezado X-Frame-Options no establecido (4) El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.	**1. SOLUCIÓN** Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
2. X-Frame-Options definidas mediante META (no-obediente con especificaciones) (5) Se encontró una etiqueta META X-Frame-Options (XFO), definiendo XFO mediante una etiqueta TAG es explícitamente no compatible con la especificación (RFC 7034).	**2. SOLUCIÓN** Asegúreque de que X-Frame-Options es configurado mediante un campo de encabezado de respuesta.
3. Absence of Anti-CSRF Tokens No Anti-CSRF tokens were found in a HTML submission form. Una solicutud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un	**3.SOLUCIÓN** Frase: Arquitectura y Diseño Utilice una biblioteca o marco comprobado que no acepte que ocura esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.

Figura 3.7 Resultado de un escaneo de vulnerabilidades en el BackOffice.

En este capítulo me gustaría mencionar las asignaturas de Redes y nuevamente a Base de datos, esta última igual al tratarse de explotar la información obtenida en la Base de Datos de la empresa, todo el conocimiento adquirido me sirvió para ejecutar mi trabajo de forma correcta y con los fundamentos de la asignatura pude obtener la habilidad de manejar diferentes Bases de Datos.

La asignatura de Redes por los problemas que salían al querer tener comunicación entre servidores, el poder diagnosticar de qué lado era el problema y de que tipo, con la finalidad de implementar la comunicación de forma correcta.

4

Resultados

La experiencia obtenida dentro de la empresa ha sido extensa, al pasar por varias áreas he tenido que desarrollar diferentes habilidades como son el manejo de base de datos, administración de servidores AIX utilizando Unix, análisis y desarrollo de sistemas, dentro de éste utilizar diferentes frameworks, sistemas de control de versiones, software de gestión de proyectos, plugins y diferentes tipos de programación todos basados en tecnología java.

He dado atención especializada y personalizada a personas de diferentes niveles de conocimiento en sistemas, desde ingenieros en sistemas como a personal administrativo.

Esta atención es una parte importante para que la implementación en la conexión entre aplicaciones se hiciera en forma correcta y ágil, con esto se proyectaba una buena imagen de la empresa, la cual siempre brinda seguridad y confianza al cliente para que haga uso de la plataforma.

Dentro de la empresa he desarrollado varios puestos todos enfocados en el desarrollo de software y en cada uno de ellos he adquirido conocimientos técnicos diferentes como se ha descrito anteriormente, cumpliendo en cada puesto con las tareas asignadas.

Un aspecto que considero importante es que debido a la diversidad de clientes que me ha tocado atender, he tenido la oportunidad de trabajar tanto con clientes que no sabían ni hacer una página web y explicarles paso a paso el proceso a seguir, como con clientes que son expertos en la materia y me tocaba aprender de su experiencia, tuve la oportunidad de interactuar con clientes y proveedores de clientes de diferentes nacionalidades como son australianos, hindús, argentinos y españoles.

Otro tema importante es que la mayor parte del tiempo que he trabajado en la empresa ha sido vía home Office o de forma remota, lo cual tiene muchos pros y contras, como beneficios están evitar tiempos en los traslados a la oficina, no batallar con alguna manifestación o la delincuencia que ha crecido en la ciudad, el poder comer con la familia casi todos los días y en mi caso vivir tan cerca el crecimiento de mis hijos, irlos a dejar a su escuela, y pasar por ellos en la tarde.

Los inconvenientes que veo son que por ejemplo es importante hacerle ver a la familia que al estar utilizando mi equipo de cómputo estoy trabajando y que reconozca que no estoy de vacaciones, además de que por la naturaleza de mi trabajo mis actividades no las desarrollo en un horario especifico, de manera que los compañeros de trabajo o clientes me pueden buscar a altas horas de la madrugada y debo estar disponible para trabajar. Y en cierto punto reconozco ser un ermitaño trabajando sólo e interactuar con otro ser humano únicamente mediante el teléfono o video llamadas.

La productividad en este caso es variable ya que existen muchos distractores estando fuera de la oficina, es más fácil poder ver alguna serie en la TV o que la familia este tratando de que realices actividades que no tengan que ver con el trabajo, pero entre las mayores ventajas es que estoy disponible en cualquier momento sin necesidad de traslados, siendo una arma de doble filo porque pueden ser las 3 de la mañana y debo estar trabajando o atendiendo alguna emergencia y claramente esto no es compensado.

Con base en mejoras o creación de nuevos procesos, se ayuda a áreas internas para facilitar sus tareas, ya sea con la automatización o simplificando acciones que anteriormente funcionaban, pero con el tiempo fueron cambiando los requerimientos y quedaban tareas tediosas para los compañeros. En este punto no se cuantificó todo lo que se ayudó a las otras áreas, pero sí fue considerable el tiempo que se ahorró para que pudieran tener una mejor productividad en su día a día.

Como aporte adicional es que en el área existe una gran oportunidad para mejorar en cuanto a organización, no hay un objetivo claro en el equipo, cada uno hace lo que sabe y debe hacer, esto ha funcionado por mucho tiempo debido a la poca rotación de personal, la mayoría de los miembros de los equipos tenemos entre 6 y 10 años trabajando en la empresa.

Una de estas mejoras sería hacer una guía de errores comunes para que nuestra área de SAC sea más efectiva y que no requiera que el equipo de desarrollo ocupe tiempo en búsqueda de información que se podría obtener en algún nuevo reporte.

En cuanto al organigrama en el área se puede mejorar, hay muchos niveles intermedios que podrían recaer en menos personas, tenemos al director, subdirector, al Project manager y al líder de proyecto, estos puestos se podrían agrupar en dos y agregar manos en la parte de QA, y de desarrollo, ya que por el momento QA no existe y desarrollo recae en una sola persona con apoyo de una empresa externa para diferentes proyectos.

También se ha intentado implementar Scrum dentro de la empresa, pero por diferentes motivos no se afianzó esa idea, considero que sería importante implementar una cultura de desarrollo ágil dentro de la empresa, pero se necesita trabajar en la estructura del equipo y en eliminar vicios que se tienen de mucho tiempo atrás, así como tener una mejor comunicación todos los integrantes del área de Tecnología.

Respecto a la formación adquirida en la Facultad de Ingeniería puedo decir que gracias a ella tengo un pensamiento analítico, después de resolver cientos tal vez miles de problemas académicos tengo la facilidad de analizar problemas que se han presentado en mi vida profesional, tener una visión completa de la información y datos que se tienen y con base en esto diseñar una solución óptima.

Todas las asignaturas que cursé en la Facultad me fueron de gran ayuda, unas con aplicación de manera directa en mi vida profesional, pero todas me ayudaron en mi formación como ingeniero, me gustaría hacer mención particular en una asignatura optativa, Telemedicina, en este curso aprendí lo relacionado a establecer un sitio donde se tuvieran dispositivos tecnológicos para dar apoyo médico a zonas rurales o zonas alejadas a ciudades grandes, lugares donde no se contaba con acceso a médicos especializados, con la tecnología se podía dar una consulta remota en temas que requerían el conocimiento de médicos especializados en algún ramo particular, menciono esto porque estos temas los he aplicado dentro de mi vida profesional, guardando las distancias de la comparación, todo el tiempo con el home office se necesita el apoyo de personas especializadas o que tienen el conocimiento requerido para resolver algún problema y mediante la tecnología se podía tener acceso a este apoyo y así he resuelto problemas o he ayudado a resolverlos.

Glosario

3DSecure: Es una firma electrónica o código él cual solo lo conoce el tarjetahabiente, sirve como validación extra en el cobro con TDC, su finalidad es evitar fraudes y transacciones no reconocidas.

API: (Application Progamming Interface) (Interfaz de Programación de Aplicaciones) Funciones externas que se encuentran compiladas y almacenadas en librerías DLL.

Ajax; (Asynchronous JavaScript and Xml) (JavaScript y XML Asíncronos) Es una tecnología de desarrollo web para crear aplicaciones mediante la combinación de HTML, XML y/o CSS como método de representar la información.

AWS (Amazon Web Services) (Servicios Web de Amazon) Es una plataforma de servicios en la nube de la empresa Amazon, puedes tener tus aplicaciones en AWS.

Bcrypt: Es una función de hashing de contraseñas diseñado por Niels Provos y David Maxieres, basado en el cifrado de Blowfish.

DLL: (Dynamic Link Library) (Librería de Vínculos Dinámicos). Archivo donde se guardan rutinas ejecutables.

DTD (Document Type Definitiion) (Definición de Tipo de Documento) Define la estructura, los elementos y los atributos que contiene un documento XML.

Framework: Grupo de objetos muy depurados que ofrecen una funcionalidad optimizada y prefabricada. Su objetivo es facilitar el desarrollo rápido de soluciones.

JavaScript: Lenguaje de programación de tipo interpretado para escribir scripts o conjunto de órdenes, el navegador de Internet es el encargado de interpretar, verificar y ejecutar de forma adecuada tales órdenes.

JSON: (JavaScript Object Notation) (Notación de Objetos JavaScript) Es un formato sencillo para el intercambio de información.
OPC: Área dedicada a la operación de los pagos de los clientes, esto incluye la conciliación de pagos en caso de no hacerse automática y ejecutar los procesos de dispersión del dinero a las cuentas de los clientes.

Phishing: Algunos atacantes realizan páginas web con la imagen corporativa de alguna empresa, con la finalidad de obtener información de sus clientes, estos pueden ser desde el nombre, dirección, como números de tarjetas de crédito y hasta montos de sueldos y números de seguro social.

POST: Método de envío de información de un formulario web de manera “oculta”, no se muestra la información en la URL.

Prepared Statements: Se traduciría como sentencia preparada, sirve para no utilizar los parámetros directos en una consulta a Base de Datos, con este método los parámetros se aplica un hash antes de utilizarlos evitando la inyección de datos no permitidos.

REST: (Representational State Transfer) (Transferencia de Estado Representacional) Filosofía de diseño y arquitectura web que se apoya en el intercambio de información mediante XML.

SAST: (Static Application Security Testing) (Análisis de Código Fuente de Aplicaciones) Servicio que analiza el código fuente de aplicativos de software para encontrar vulnerabilidades.

SOAP: (Simple Object Access Protocol) (Protocolo Simple de Acceso a Objetos) Protocolo ligero basado en XML para intercambiar información entre aplicaciones.

SQL: (Structured Query Language) (Lenguaje estructurado de consulta) Es un lenguaje común de programación de bases de datos.

TPV: (Terminal Punto de Venta) Es el equipo físico que se utiliza para cobrar, emitir ticket de compra y comunicarse a un sistema de gestión de ventas.

URL: (Universal/Uniform Resource Locator) (Localizador de Recursos Universal/Uniforme) Dirección que identifica de forma única una ubicación de Internet.

WebService: Conjunto de especificaciones que posibilitan la comunicación y provisión de servicios entre diferentes aplicaciones vía web.

XML: (eXtensible Markup Language) (Lenguaje de Marcado Extensible) Lenguaje de meta marcado que proporciona un formato para describir datos estructurados en forma de texto simple, y además es autodescriptivo. Esto facilita declaraciones más precisas del contenido y resultados de la búsqueda más significativos en múltiples plataformas.

XSD: (XML Schema Definition) (Esquema de Definición del XML) Es la validación para comprobar que la estructura del XML sea correcta; su estructura, los tipos de datos, atributos, orden, etc.

XXE (XML External Entity) (Entidad Externa del XML) Es un tipo de ataque donde se inyecta un XML corrupto, pero la aplicación no tiene las validaciones necesarias para detectarlo, el atacante puede tener acceso a archivos o servicios del sistema

Referencias

ADQUIRA México - La mejor solución para realizar, recibir y controlar pagos por Internet [en línea] <http://www.adquira.com.mx/> [Consultado 5 agosto 2011]

Aprende Hacking explotando los 10 riesgos más críticos, Gerardo Eliasib, <https://hackingprofessional.github.io/Security/El-riesgo-de-las-Configuraciones-Incorrectas-de-Seguridad-OWAPS-V/> [consultado 14 febrero de 2020].

Flap México. <https://www.flap.com.mx> [Consultado 9 de marzo de 2019]

Glosario IT, <https://www.glosarioit.com> [consultado 6 de marzo de 2020]

History of Java Technology, <https://www.oracle.com/technetwork/java/javase/overview/javahistory-index-198355.html> [consultado 22 de febrero de 2020].

Owasp - <https://www.owasp.org/index.php> [Consultado 28 de julio de 2018]

PCI Security Standars Council, <https://es.pcisecuritystandards.org/minisite/env2/> [consultado 20 de abril de 2019].

Security Node Applications, Chetan Karande <https://www.oreilly.com/library/view/securing-node-applications/9781491982426/> [Consultado 9 de marzo de 2019]

ANEXO A

Seguridad de Aplicaciones mediante OWASP.

Dentro del desarrollo de aplicaciones se debe cumplir con la seguridad y protección de la información en todo momento y para eso se toma en cuenta el listado que publica OWASP (Open Web Application Security Project) acerca de las principales vulnerabilidades a los cuales están expuestas las aplicaciones web, esto en base a un estadísticas de los ataques informáticos sufridos por diversas compañías o sistemas y con esta lista también provee recomendaciones para evitar que tu aplicación no tenga alguna de estas vulnerabilidades.

OWASP, traducido al español como Proyecto abierto de seguridad en aplicaciones web sale en Internet en el año 2001, es una comunidad sin fines de lucro en la que cualquier persona puede participar y está dedicada a apoyar a cualquiera que desee implementar aplicaciones confiables en Internet, así como mejorar la seguridad de las ya existentes. Las herramientas, documentación y publicaciones son gratuitas.

A continuación, se da una explicación breve de cada vulnerabilidad y se ahonda más en las que tienen que ver con el desarrollo de software, así como las principales recomendaciones para prevenir que personas no autorizadas puedan acceder a la aplicación explotando estas vulnerabilidades.

- Injection.

Muchas aplicaciones utilizan interpretes SQL, comandos de sistema operativo, envío de correo, LDAP, entre otros. Estos interpretes toman los datos ingresados en el sistema por el usuario para completar comandos y ejecutar instrucciones, la inyección es cuando esta entrada ingresada por el usuario se interpone entre los datos y el código del sistema, ocasionando que el usuario en este caso puede ser un usuario malicioso ejecute comandos en la aplicación, entre los riesgos que se pueden suceder por no tomar acciones para prevenir esta inyección es la posible pérdida o corrupción de datos, accesos no autorizados, accesos correctos que sean denegados y se puede perder el control total del sistema.

Para describir esta vulnerabilidad se usará un ejemplo, en la siguiente figura se muestra una página de inicio de sesión de un sistema, en donde se solicita ingresar un usuario y una contraseña para poder tener acceso al sistema.

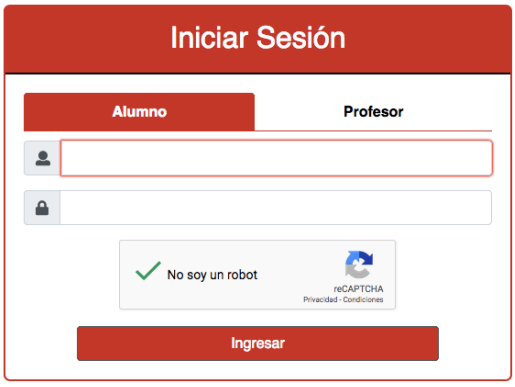


Figura A.1. Ejemplo de Inicio de sesión en una página web

Al no tener ninguna validación sobre los datos que ingresan en el acceso y suponiendo que se use lo más sencillo en la consulta para validar el usuario se obtiene el siguiente escenario en la consulta:

```
String query = "SELECT * FROM accounts WHERE
custID= ' "+request.getParameter("id") +" '  AND
password = '"+request.getParameter("password") +'";
```

Donde la consulta hecha a la Base de Datos se realiza con los datos obtenidos tal cual los captura el usuario.

En la siguiente figura se muestra el mismo acceso al sistema, pero con datos capturados por el usuario malicioso.

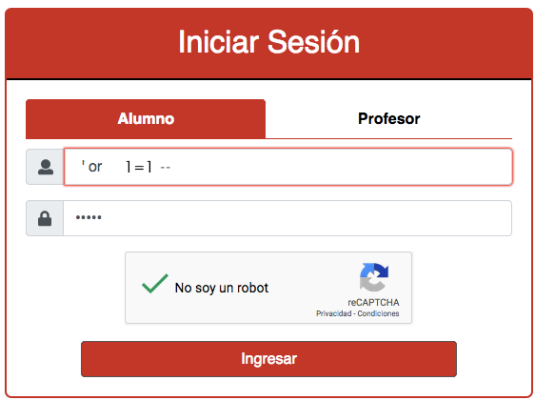


Figura A.2 Ejemplo de información capturada por el usuario malicioso.

Con este simple dato que se tiene en el ejemplo como lo que ingresa el usuario malicioso al sistema, la consulta a la Base de Datos cambiaría de la siguiente forma:

```
Query = “SELECT * FROM accounts WHERE custID=’’ or 1=1
- -  AND password = ‘valor’ '';
```

El resultado de esta consulta es que se busca un valor vacío en la columna de custID y con el 1=1 nos mostraría todos los registros de la tabla *accounts* no importando el valor buscado en custID y como se colocan dos guiones los cuales en SQL significan que después de ellos se acaba la sentencia y empiezan comentarios, de manera que el usuario malicioso además de obtener información, podría ingresar otra sentencia con la cual puede haber modificaciones en los datos o ejecutar procesos almacenados de la Base de Datos.

Entre las recomendaciones que provee OWASP es realizar las siguientes acciones para prevenir este tipo de vulnerabilidad:

- Utilizar frameworks o librerías revisadas.
- Utilizar un api el cual sirva de interprete o parametrizador.
- Correr la aplicación con privilegios mínimos.
- Utilizar intérpretes para procesar todos los caracteres especiales.
- Utilizar listas blancas para validar los parámetros que se reciben de peticiones.
- Utilizar consultas a la Base de Datos parametrizadas.

❖ Broken Authentication.

Se podría traducir como robo de autentificación, aunque no necesariamente es un robo, se produce cuando un usuario malicioso obtiene acceso al sistema, lo puede hacer de diferentes formas, combinando nombres de usuarios y contraseñas comúnmente usados, puede utilizar ataques de fuerza bruta o usando herramientas de ataques.

El usuario malicioso puede ganar acceso a unas pocas cuentas o solo con la cuenta administrador y con eso tener oportunidad de comprometer la seguridad del sistema. Dependiendo del tipo de sistema puede tener acceso a información sensible, acceso a cuentas bancarias, robo de identidad, entre otros.

Para ejemplificar este tipo de vulnerabilidad se presenta el siguiente escenario:
Los tiempos de espera de la aplicación no están configurados correctamente. El usuario usa una computadora en un café internet para acceder al sistema. En lugar de seleccionar "cerrar sesión", el usuario simplemente cierra la pestaña del navegador y se aleja. El atacante usa el mismo navegador una hora más tarde, y ese navegador aún está autenticado, teniendo todo el acceso a la cuenta del usuario.

Acciones para prevenir este tipo de ataques:

- Implementar una autentificación multifactor, el cada vez más utilizado captcha, para prevenir ataques de fuerza bruta, robos de credenciales.
- No dejar credenciales o contraseñas con los valores default.
- Implementar validaciones para impedir el uso de contraseñas débiles, estos deben incluir letras, números, caracteres especiales, una longitud mínima, así como no usar palabras completas.
- Limitar o usar un tiempo de espera al momento de tener un error en el acceso al sistema, así como tener alertas a los administradores de sistema al momento de identificar ataques de fuerza bruta u otros ataques.
- Manejar valores en el identificador de sesión que sean nuevos en cada sesión y se generen de forma aleatoria. No mostrar el identificador de sesión en la URL ni en el envío de parámetros, así como invalidar los identificadores de sesión en cada término de sesión y en determinado tiempo de inactividad.
- Que la recuperación de contraseña no sea un proceso de fácil acceso, en algunos casos se envían las contraseñas por email o mensaje de texto donde pueden verse en la alerta de los smartphones.
- Utilizar al menos dos de tres opciones de acceso que cumplan con el lema: algo que sabes (contraseña), algo que eres (FaceID) y algo que tienes (dispositivos de token)

❖ Sensitive Data Exposure.

Exposición de datos sensibles se refiere cuando un sistema o aplicación muestra datos sensibles sin cifrarlos, ya sea en pantalla, en la URL o en los registros de la aplicación. Al hacer esta acción se permite que un atacante pueda obtener información de los usuarios, como lo serían, nombre, dirección, número de tarjeta.

El robo de información sensible puede dar lugar al robo de identidad, fraudes con tarjetas de crédito u otros delitos.

Con el siguiente ejemplo se muestra de forma sencilla lo que sería un ataque que aproveche esta vulnerabilidad:

En la siguiente imagen se muestra una URL que se forma después de un acceso al sistema, en este caso los parámetros utilizados se mandan vía GET y se muestran en la navegación sin cifrar, esto puede ser leído en el historial de navegación o puede ser leído mediante software especial para capturar datos en redes compartidas.

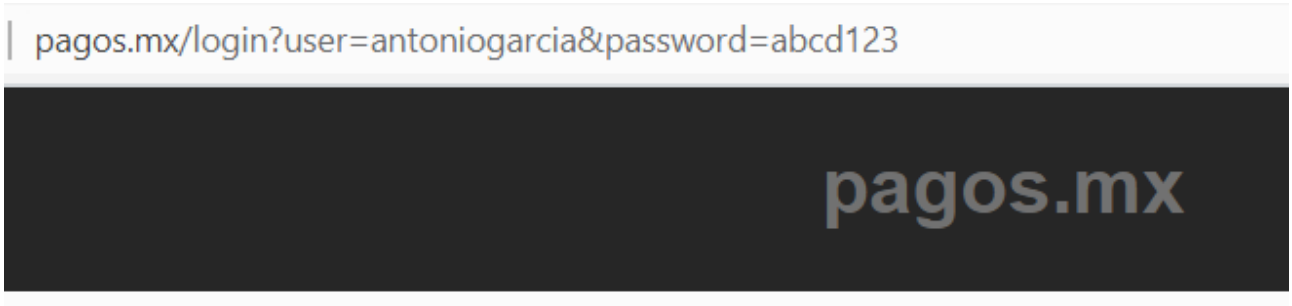


Figura A.3. Ejemplo de URL que expone datos sensibles.

Acciones para prevenir estos tipos de ataques.

- Clasificar los datos sensibles dependiendo de las leyes del país o países en las cuales se utilice el sistema.
- No guardar datos sensibles que no sean necesarios en el sistema.
- Hacer un cifrado seguro de los datos sensibles.
- Estar al día en los estándares de seguridad de cifrado, nuevos algoritmos, protocolos y llaves.

- Cifrar todos los datos que se transmiten en la red mediante los últimos estándares de seguridad del http.
- Inhabilitar el autocompletar en los formularios donde se colocan datos sensibles.
- Verificar independientemente la efectividad de la configuración del sistema.
- Almacenar contraseñas con un algoritmo especial, existen varios ejemplos los cuales se pueden utilizar bcrypt, PBKDF2, entre otros.

❖ Broken Access Control

Acceso de Control Roto se refiere a una mala práctica que puede ser tanto de configuración de los servidores como de programación, la cual deja expuestas algunas partes del sistema, lo que provoca que un usuario sin permisos obtenga acceso a ellas o ejecute acciones que no debería.
Dentro de la programación este tipo de vulnerabilidad sucede cuando después de ingresar al sistema el usuario intenta realizar una función no válida para su perfil y si el sistema no revisa si el usuario tiene permisos para ejecutar esa acción, el usuario malicioso puede obtener información sensible como contraseñas, cuentas bancarias, entre otras, dependiendo el tipo de sistema podría obtener el control total.

Las debilidades del control de acceso son comunes dado que no existen métodos automatizados para detectarlas, y si no se comienza por establecer, desde un principio, con claridad, qué usuarios tendrán qué permisos, es fácil caer en error o no detectar éstos.
Esta vulnerabilidad según OWASP es común encontrarla en los sistemas y además es fácil de explotar.

Para ejemplificar este caso en la siguiente imagen se muestran ejemplos de varias URL donde se muestra un dato nombrado Id y su valor sin cifrar, haciendo saber al atacante que la aplicación necesita ese dato para su ejecución. Con lo cual podría poner números al azar y obtener en este caso acceso a la cuenta de otro cliente del banco.

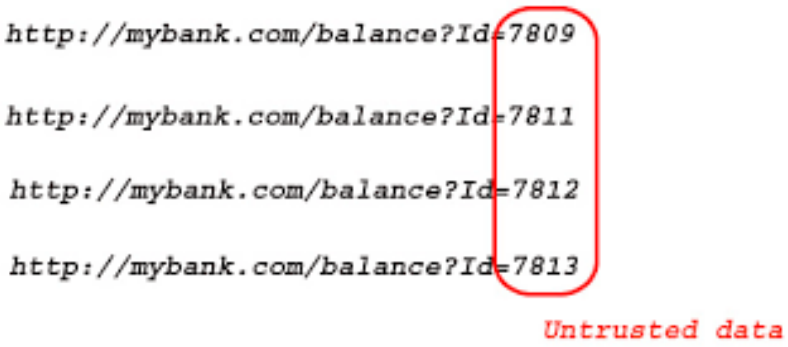


Figura A.4. Ejemplo de URL's con datos sensibles en claro.

La revisión del código de la aplicación puede verificar rápidamente si cualquiera de los enfoques se implementa de forma segura. Las pruebas también son efectivas para identificar referencias directas de objetos y si son seguros. Las herramientas automatizadas generalmente no buscan tales defectos porque no pueden reconocer lo que requiere protección o lo que es seguro o inseguro.

Acciones para prevenir este tipo de ataques:

- Cambiar nombres predeterminadas a las páginas web.
- Usar referencias a las páginas web, esto es con un controlador invocar las páginas destino mediante una clave y no el nombre real.
- Usar roles y permisos para los usuarios que utilizaran el sistema.
- Verificar acceso a cada uno de los recursos para asegurar que el usuario tiene permiso para acceder a él.

❖ Cross Site Scripting (XSS)

Ejecución de comandos en sitios cruzados es una mala práctica de programación, la cual surge por aceptar datos sin hacerles una validación del tipo de dato que esperamos (listas blancas) o por no realizar un cifrado a los datos, esto es, leer los caracteres especiales que usan los comandos de código HTML, JavaScript o SQL y reemplazarlos por un código universal de caracteres, como ASCII o una versión de Unicode, esto para que los traductores de código los reconozcan como un carácter y no como parte de una sentencia.

Este tipo de ataques tratan de usar sesiones de otros usuarios, redireccionar la navegación a sitios maliciosos y pueden llegar a modificar las páginas web insertando imágenes y textos que den mala imagen a la empresa a la que pertenece.
Para identificar este tipo de vulnerabilidad se requiere que se haga una revisión manual de código y como pruebas de penetración, además de enfoques automatizados.

Es llamado XSS, aunque sus siglas son CSS ya que estas últimas se refieren a las hojas de estilos utilizadas para las páginas web.

Ejemplo de escenarios de ataque:
En la siguiente figura se muestra un usuario malicioso que aprovecha que el campo de texto Message no utiliza el cifrado correctamente e inserta un script para obtener información del siguiente usuario, en este caso un archivo que puede contener información como usuario, contraseña, id de la sesión o algún dato sensible.

Figura A.5. Ejemplo de inserción de ataque XSS

En la figura A.6 se observa el resultado del script malicioso insertado anteriormente en la aplicación web, en este caso se muestra el ID de sesión, con el cual se puede entrar a la aplicación con el perfil de esta persona. El usuario malicioso puede hacer algo más que

mostrar esta información en pantalla, la podría enviar a otro sitio donde la pueda almacenar y ocuparla para otras acciones.

Figura A.6. Resultado de un ataque XSS

Acciones para prevenir este tipo de ataques:

- La principal recomendación es que a todos los inputs o campos donde se permita al usuario ingresar información hacia el sistema se cifren adecuadamente, ya que el sistema puede tratar la información del usuario malicioso como un contenido activo en el navegador.
- También se recomienda el uso de listas blancas, que es validar el tipo de dato que se esté esperando en el envío de información del usuario, se valida igualmente la longitud y el formato del dato antes de aceptar la entrada al sistema.

Existen librerías para validar el XSS, entre las que destaca la de OWASP llamada AntiSamy.

- Using Components with Known Vulnerabilities.

Uso de componentes con vulnerabilidades conocidas, es muy común utilizar librerías o aplicaciones de terceros al momento de desarrollar una aplicación, a su vez esta librería o aplicación depende de otra de otro desarrollador.

En esta cadena de dependencias cualquiera de las librerías o aplicaciones puede ser que tengan problemas de seguridad ya sea porque no está correctamente desarrollada o porque no es la versión actualizada.

Para validar tu aplicación se debe conocer que aplicaciones hace referencia, nombres y versiones de cada una para poder investigarlos, para esto existen listas donde se encuentran las vulnerabilidades que se han ido descubriendo.

En la siguiente figura se muestra un ejemplo de estas listas, en este caso es la Base de Datos Nacional de Vulnerabilidad, NVD por sus siglas en inglés, una página de Estados Unidos donde podemos observar el nombre de la librería, la versión, el problema que se encontró, así como la fecha en que se reportó.

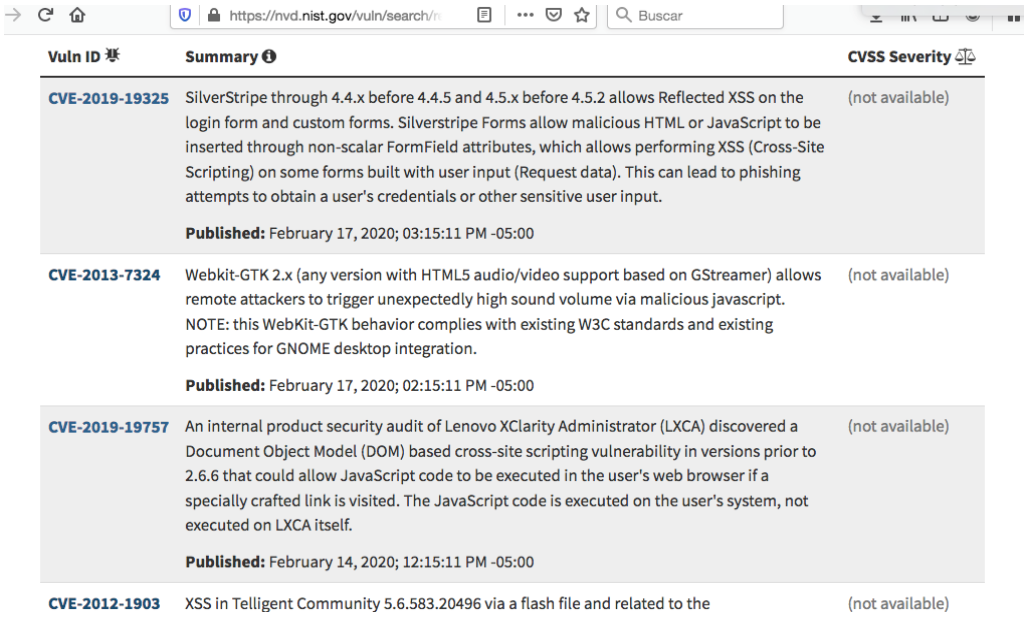


Figura A.7. Ejemplo del listado de la NVD (National Vulnerability Database).

Acciones para prevenir este tipo de ataque:

- Remover dependencias, componentes o funcionalidades no utilizadas.
- Tener un inventario de versiones de las librerías.
- Monitoreo frecuente de las listas de vulnerabilidades.
- Utilizar alguna herramienta de análisis automatizado, así como estar suscrito a las alertas de seguridad de los componentes utilizados.

❖ Insufficient Logging and Monitoring

Monitoreo y registros de aplicación insuficientes, cada aplicación genera errores ya sean del servidor, de la Base de Datos, de memoria o en validaciones de datos de entrada o salida del sistema, de seguridad, todos si no son manejados correctamente pueden afectar la operación del sistema, o si no se toman en cuenta para corrección del error cualquier usuario malicioso puede encontrarlos y explotar las vulnerabilidades del sistema.

Cabe mencionar que, si el sistema no genera alertas en caso de detectar algún ataque, así como los tiempos de respuesta en caso de tener las alertas no es la adecuada también es tiempo que el usuario malicioso puede ocupar para encontrar vulnerabilidad

Acciones para tomar en cuenta:

- Tener un registro de los errores en los inicios de sesión, validación de entradas de datos para poder identificar cuentas sospechosas,
- En caso de tener errores de cualquier tipo el registro deberá tener tipo de evento, fecha y hora, nombre de usuario, direcciones IP, URL solicitado entre otra información.
- Los errores mostrados a los usuarios no deben contener información detallada del error en el sistema, con un mensaje genérico o un mensaje especifico dependiendo el error será suficiente.
- Tener un monitoreo con alertas para que las actividades sospechosas sean identificadas y atendidas en tiempos aceptables.
- Tener políticas de acción y recuperación de incidentes.

“Por mi Raza Hablará el Espíritu”

Facultad de Ingeniería

Ciudad Universitaria, Cd. Mx., 2021

José Antonio García Rojo