ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE CONTROLES EN LAS INTERFACES DE SOFTWARE DE FACTURACIÓN ELECTRÓNICA"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JAIRON HUMBERTO RAMIREZ GUTIERREZ

GUAYAQUIL – ECUADOR

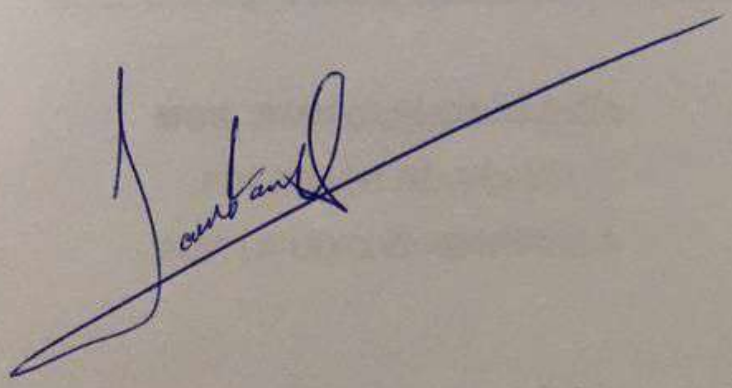
AÑO: 2016

AGRADECIMIENTO

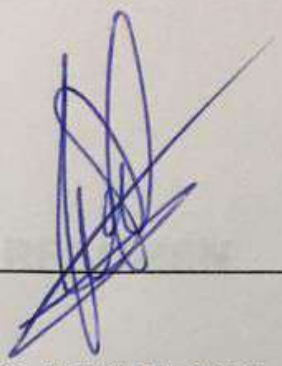
Agradezco a Dios ya que sin sus bendiciones no hubiese tenido la salud ni la fuerza para cumplir mis metas propuestas y en especial a mi madre y padre (+) que con su dedicación, ejemplo y sacrificio lograron que en cada etapa de mi vida cumpliera con mis metas.

DEDICATORIA

Dedico éste proyecto a mi esposa Verónica Preciado e hijos Doménica, Gabriel, Briana y Suri por su inmensa paciencia, compresión y sacrificio que tuvieron mientras curse mis estudios, hoy se ve el resultado mis amores para seguir adelante. Familia los AMO.

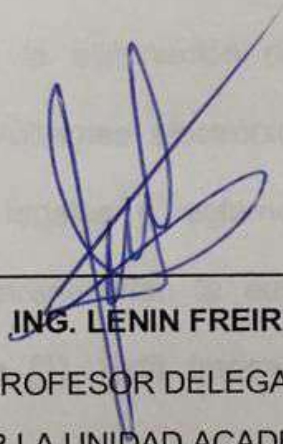


TRIBUNAL DE SUSTENTACIÓN



ING. LENIN FREIRE

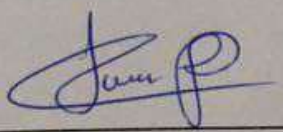
DIRECTOR MSIA



ING. LENIN FREIRE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



MGS. JUAN CARLOS GARCÍA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESÚMEN

El modelo de facturación electrónica, está ya implementado en algunos países de América y ECUADOR no ha sido la excepción, ha comenzado y con éxito la carrera hacia la eliminación de Documentos Pre-Impresos reemplazándolos por comprobantes electrónicos que son documento que cumple con los requisitos legales y reglamentarios exigibles para todos comprobantes de venta, garantizando la autenticidad de su origen y la integridad de su contenido [1]. Esta transacción electrónica es una de las operaciones que se realiza al final de un proceso de Business to Business (B2B) en donde se intercambia documentos electrónicos en formatos como EDI (Electronic Data Interchange) , XML (eXtensible Marckup Languaje).

En la actualidad, existe varias formar de poder contar con la implementación de este servicio:

- Software Local, la compañía cuenta con desarrollo propio para todo el proceso de envío y recepción de documentos electrónicos.

- Software de Servicio Externos, el proveedor recibe información del cliente para realizar todo el proceso de Recepción / Autorización / Almacenamiento de documentos electrónicos.

Frente a estos escenarios las PYMES hoy optan por tercer izar este servicio a través de proveedores de las diferentes ofertas de cada uno. Pero como el proveedor garantiza que la información que ha llegado a sus servidores es Integra desde su emisión de sus clientes, por esto y más las exigencias hacia los Software Externos deben tener claro las mejores prácticas de seguridad para salvaguardar la información que reciben de sus clientes.

La solución es incorporar mejoras a la cadena del proceso de autorización en los Servidores Externos, y esto consiste en implantar controles en las interfaces de Envío / Recepción de documentos electrónicos, haciendo uso de los Servicios Web que reconozcan si la información ha sido alterada y que se tomen correctivos necesarios para analizar los casos de mayor incidencia.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

B2B	Bussines to Bussiness
ERP	Enterprise Resource Planning
EDI	Electronic Data Interchange
HASH	Función Resumen que devuelve un conjunto De Caracteres
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
MD5	Familia de Funciones de Hash de cifrado
PYMES	Grupo de Empresas Pequeñas y medianas
SHA-1	Familia de Funciones de Hash de cifrado
SHA-256	Familia de Funciones de Hash de cifrado
SHA-512	Familia de Funciones de Hash de cifrado
XML	Lenguaje de Marcas Extensible

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En Latinoamérica y el mundo, el modelo de facturación de electrónica se está volviendo cada vez más común y ahora este concepto es transcendental por el impacto que ya ha provocado en las actividades comerciales y tributarias de nuestro país, sin duda sus inicios desde el 2011 los cambios se han notado con todos los cambios incorporados por el ente regulador hacia sus contribuyentes.

Como concepto facturación electrónica de define como un documento tributario generado por medios informáticos en formato electrónico, que reemplaza al documento físico en papel, pero que conserva su mismo valor legal con unas condiciones de integridad, autenticidad y seguridad no observadas, de manera que la facturación electrónica consiste en la transmisión de las facturas o documentos similares entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

Las grandes empresas tales como Bancos , Emisores de Tarjetas de Crédito, Bananeros y Contribuyentes Especiales, han cumplido con todas las obligaciones para emisión de sus documentos con todas las medidas de seguridad para garantizar la integridad y confiabilidad de sus documentos hacia sus clientes.

Ahora es el turno de las empresas PYMES que se van incorporando a través de los beneficios de proveedores externos que dan el servicio de Software de Facturación Electrónica para que puedan cumplir con los reglamentos, pero ahora la pregunta es como ellos garantizan que los documentos que reciben y procesan no han sufrido cambios desde la recepción en sus servidores externos y devolución de documentos autorizados, surge entonces la necesidad de implementar controles en las interfaces que ejecutan el proceso desde la recepción y envió de los documentos electrónicos autorizados.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

En el ecuador los primeros en iniciar con el proceso de Facturación Electrónica han sido los contribuyentes especiales, los cuales por su capacidad técnica cuenta con una infraestructura tecnológica que les permiten garantizar que la información generada es integra y confiable.

Ahora las empresas PYMES están también siguiendo el mismo ejemplo y por ellos se han visto en la necesidad de comenzar a gozar de los réditos de los documentos electrónicos., hoy en día existen muchas ofertas como vemos en la siguiente grafica

Figura 1.1 Ejemplo de Servicios de Proveedores Externos

Muchos de los software que actualmente están en el mercado, han ido evolucionando y siendo claramente responsables con la información que se maneja de los clientes, pero es importante destacar que se tiene que mantener controles en el CORE del proceso de recepción y envío de documentos autorizados, por la experiencia en los mayorías de los software a los cuales he realizado integraciones ninguno ha manejado controles para los documentos.

En la capa tradicional que se tiene casi todos tienen el mismo esquema, pero en la selección con color rojo, podemos apreciar que es aquí donde radica el problema descrito puesto que no se cuenta con las verificaciones respectivas para validar Integridad de los datos que se recibe desde los datos del ERP del cliente

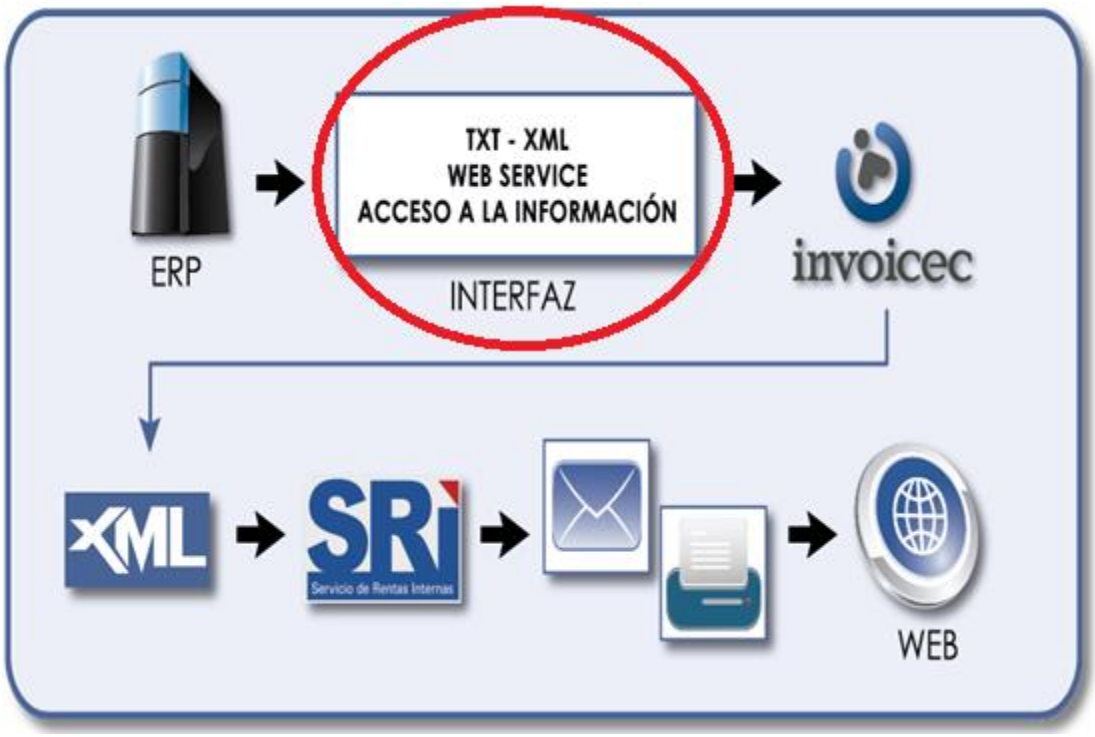


Figura 1.2 Modelo de Servicio Web con Facturación Electrónica

1.2 SOLUCIÓN PROPUESTA

Las limitaciones en la infraestructura de las PYMES obligan en muchos casos a que se tengan que usar servidores externos capaces de procesar y almacenar información en la nube. Normalmente hacen uso de Servicios Web (Web Services) para recibir los XML desde sus clientes, procesarlos, almacenarlos. Aquí es nace la necesidad de implementar los Controles en las Interfaces permitiendo asegurar el Envío / Recepción de la información en los servidores Externos.

Los cambios a implementar se realizaran dentro del **Core** del Proceso de Recepción de Documentos entre el cliente y el Servicio Web de los proveedores externos.es aquí donde radica la alta posibilidad de que la información sea alterada porque existe integración con software externo del lado del cliente.

Figura 1.3 Capa donde se implantaran los cambios

Todo control a implementar tiene su beneficio y los que obtendremos dentro del modelo planteado serán los siguientes:

- Garantizar la Integridad de la información que viene del lado del clientes, a través de la obtención del HASH de cada archivo que se envía a los Servidores Externos

- Validar que los Documentos recibidos en los servidores externos son auténticos y no han sufrido ningún cambio

- Posterior a la autorización de los documentos que se han recibido, hay que también la necesidad de enviar la información hacia el cliente que está a la espera del número de autorización y del XML

autorizado, de la misma forma también obtendremos el HASH de la información que nos llega y validaremos para verificar su integridad.

La clave éxito para esta implementación será usar las funciones (método) HASH que nos garantizan la integridad de cualquier tipo de información cuando esta va de un lugar a otro; y a los proveedores externos que integren en sus Servicio de autorización de documento les permitirá garantizar la confiabilidad de toda la información que procesan en sus servidores.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS PREVIO A IMPLEMENTACIÓN

2.1.1. SITUACIÓN ACTUAL

La evolución de los sistemas de facturación electrónica ha tenido un repunte en el último y se espera un crecimiento mayor, los contribuyentes de las PYMES están en la actualidad ya viendo la posibilidad iniciar el proceso de facturación electrónica, pero aunque no cuentan con una infraestructura tecnológica de alto nivel de procesamiento y almacenamiento, entonces buscan proveedores

externos que puedan cubrir su necesidad en el menor tiempo y costo.

Frente a ellos las soluciones de Software en el mercado hay una gran variedad con diferentes ofertas por volumen de documentos es la que más prima en los medios actuales, esto hace que el cliente no tenga la necesidad de invertir en equipos que puedan realizar dichas tareas.

Pero ¿Cómo operan las compañías que actualmente ofrecen este servicio? Es muy sencillo tiene habilitado un Servicio Web (Web Services) para la recepción de información que viene del lado del cliente. Con esta aplicación se recibe, procesa y envía al cliente la información de los documentos de los documentos electrónicos autorizados.

2.1.2. ESTUDIO DE SOLUCIONES EXISTENTES

En el mercado actual por la experiencia que he visto pocos son los proveedores que manejan este tipo de controles en las interfaces de recepción de documentos, entre ellos puedo mencionar a Es-Dinámico, Security-Data.

Figura 2.1 Ejemplo de Software de Facturación Electrónica

Figura 2.2 Ejemplo de Software de Facturación Electrónica

Es probable que otros proveedores por desconocimiento no hayan tenido la precaución de validar la información que se recibe, pero como todos conocemos los Softwares no siempre pasan primero por los controles de seguridad sino por controles solamente de funcionabilidad, y he allí donde radica el problema de las aplicaciones en el mercado.

2.1.3. SOLUCIÓN DEFINITIVA

El uso de herramientas tales como la obtención del **HASH** del XML, nos permiten validar si los documentos son íntegros desde él envió del documento electrónico y nos garantizan que la información a procesar es la correcta [6], para ello entonces es necesario la creación de un Servicio Web (Web Service) [2] para recibir los HASH de cada documento que se procesa y la forma de cómo lo relacionaremos con el XML recibido será a través de la CLAVE DE ACCESO la misma que es única por cada documento que se recibe.

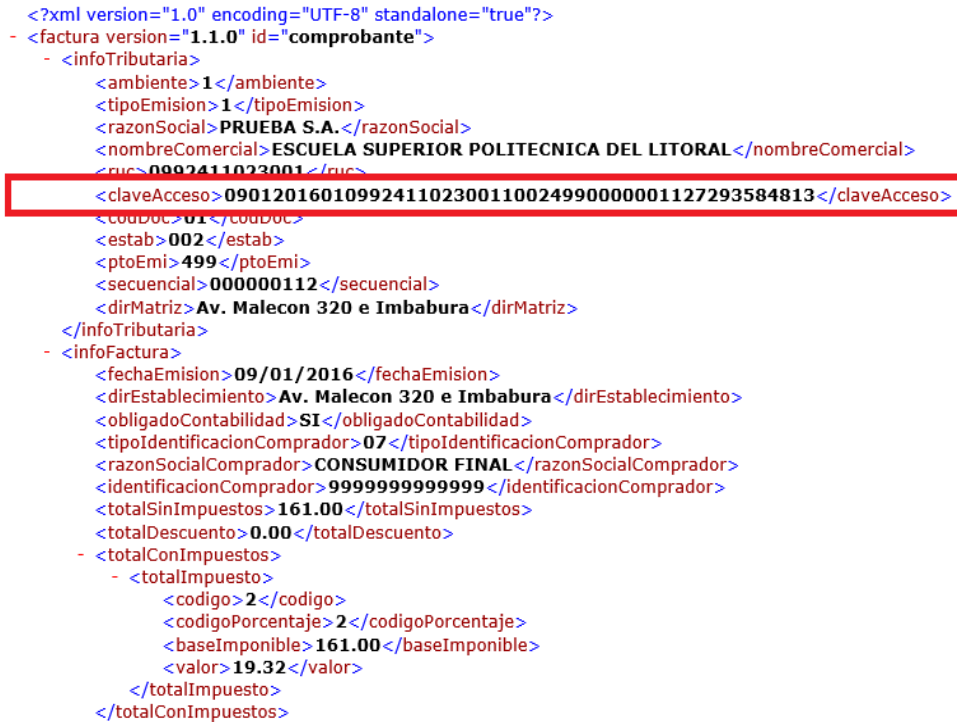


Figura 2.3 Ejemplo de un XML donde consta la CLAVE DE ACCESO

Entonces antes de recibir un XML de la factura, se recibirá un XML donde consta el HASH y la clave de acceso la misma que permitirá validar para saber si no tenido problemas de integridad y rechazar en caso de que así sea para grabar en LOGS de auditoria y tomar los correctivos necesarios para superar la novedad.

2.2 DISEÑO

Para la elaboración del diseño hemos utilizado una herramienta de programación llamada Visual Studio 2012 by Microsoft

Figura 2.4 Software de Programación

Para empezar realizaremos la creación de un Servicio Web cuyo nombre será < **RecepcionHasDoc** > el cual nos permita receptar un XML con la estructura de los siguientes datos

- Hash del documento

- Clave de acceso

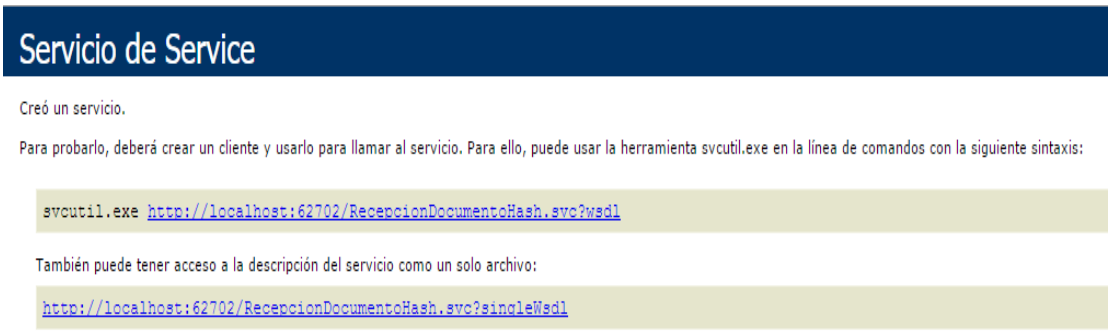


Figura 2.5 Diseño servicio web RecepcionHasDoc

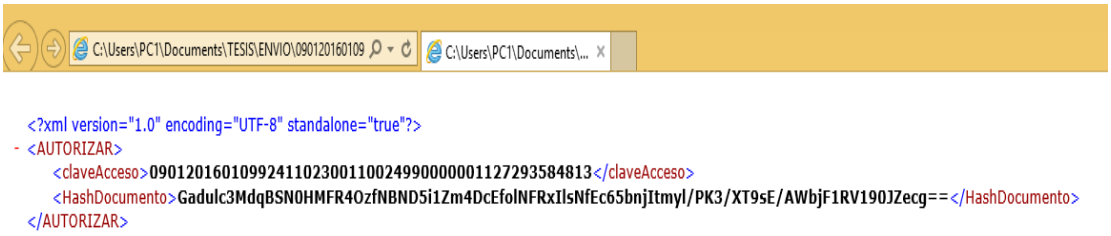


Figura 2.6 XML de ejemplo donde consta HASH y la CLAVE DE ACCESO.

La grafica a continuación ilustra cómo se realizan los envíos del lado del cliente hacia los servidores externos de facturación electrónica y estos a su vez posteriormente validarán la información que se ha recibido.

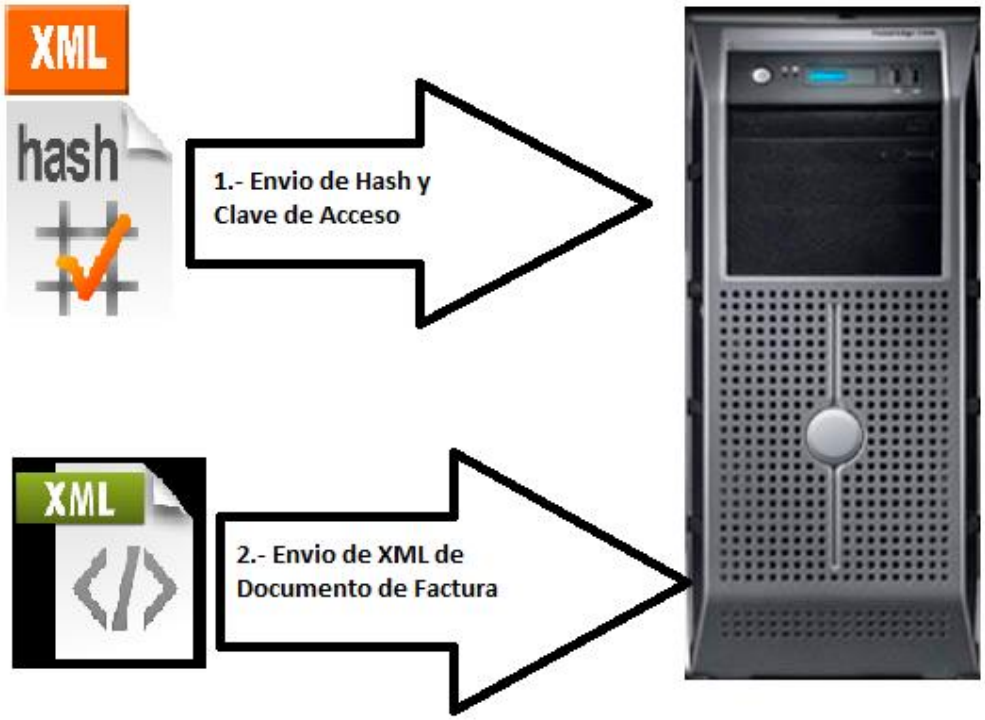


Figura 2.7 Ejemplo de la ejecución de Envío desde el cliente hacia los servidores externos.

En conjunto estos dos elementos serán implementados en las siguientes capas dentro del CORE del Servidor Externo:

1. En el cliente, previo al envío del XML de la factura autorizar el sistema generará un HASH y en conjunto con la clave de acceso se generar un XML que permitirá enviar esta estructura a los servidores Externos [4]

Figura 2.8 Ejemplo de Recepción de XML y HashDoc

2. En los Servidores Externos, estarán habilitados dos servicios para procesar un documento electrónico

a. Servicio Recepción de Hash del documento para validar contra el Servicio de Recepción de XML, este se encargará de almacenar la Clave de Acceso y el Hash.

b. Servicio de Recepción de XML del documento electrónico autorizar. [4]

Figura 2.9 Ejemplo de Recepción de XML de factura

Al fusionar la recepción de ambos XML en el CORE en los servidores externos estarán preparados para validar si la información recibida es íntegramente valida o no, caso contrario rechazar y proceder a notificar a través de alertas de control para este tipo de incidentes.

INSTALACIÓN Y CONFIGURACIÓN

DESDE EL CLIENTE

Desde el cliente donde se genera la información del ERP se enviará hacia los servidores externos a través del consumo de los Servicios Web, cabe mencionar la importancia del orden de envío de cada uno de ellos.

Figura 2.10 Ejemplo de envío desde el ERP del cliente al CLOUD

1. RecepcionDocumentoHash.svc?wsdl, servicio web para recibir XML con el hash y la clave de acceso [3]

http://localhost:62702/RecepcionDocumentoHash.svc?singleWsdl

Figura 2.11 Ejemplo de Servicio Web para recibir el XML con HASH

2. RecepcionDocumentoXML.svc?wsdl , servicio web a consumir para recibir XML con datos de factura [3]

http://localhost:62702/RecepcionDocumentoXML.svc?singleWsdl

Figura 2.12 Ejemplo del Servicio Web para recibir XML de factura

El único Servicio nuevo en los proveedores externos es la inclusión del servicio web para recibir el Hash del documento que como ya hemos mencionado nos garantizará la integridad del archivo XML con los datos de la factura que contiene.

DESDE LOS SERVIDORES EXTERNOS

En los servidores externos están activos los servicios mencionados anteriormente a la espera de poder procesar toda la información que va llegando, ahora el orden en que se ejecuta es vital para implementar de una forma correcta las validaciones en las interfaces.

Figura 2.13 Servidor Externo donde están disponibles los Servicios Web

1. Almacenar el Hash y la clave de acceso de cada documento recibido.

2. Obtener el Hash del XML de la factura que se ha recibido y compararlo con el HASH que se calcula mientras se procesa los archivos, esto garantizará si el archivo no ha sufrido alguna modificación.

    a. En caso de ser exitoso la validación, se procederá a seguir con el proceso normal de autorización.

    b. Caso contrario, se deberá guardar LOGS de auditoria y enviar mails a los encargados de monitorear dichos procesos con el fin de notificar al cliente y aplicar las medidas correctivas.

PRUEBAS

Los documentos electrónicos cuando son recibidos son procesados (autorizados) automáticamente y para saber cuáles son los documentos autorizados y sus diferentes estatus existen diferentes tipos de Consola de Auditoría que permitan auditar la capacidad de procesamiento y los posibles errores de los servicios web disponibles.

Ahora con la nueva implementación que hemos integrado, tenemos en las consolas de auditoria una nueva columna que indica si el HASH del documento fue validado, garantizándo la integridad y confiabilidad de la información que se recibe y se envía desde los clientes.

Como se puede apreciar en la gráfica cuando exista un documento que no pasó la validación del HASH entonces en la consola de auditoria este tendrá un color ROJO especial para poder identificar cuáles son los documentos rechazados.

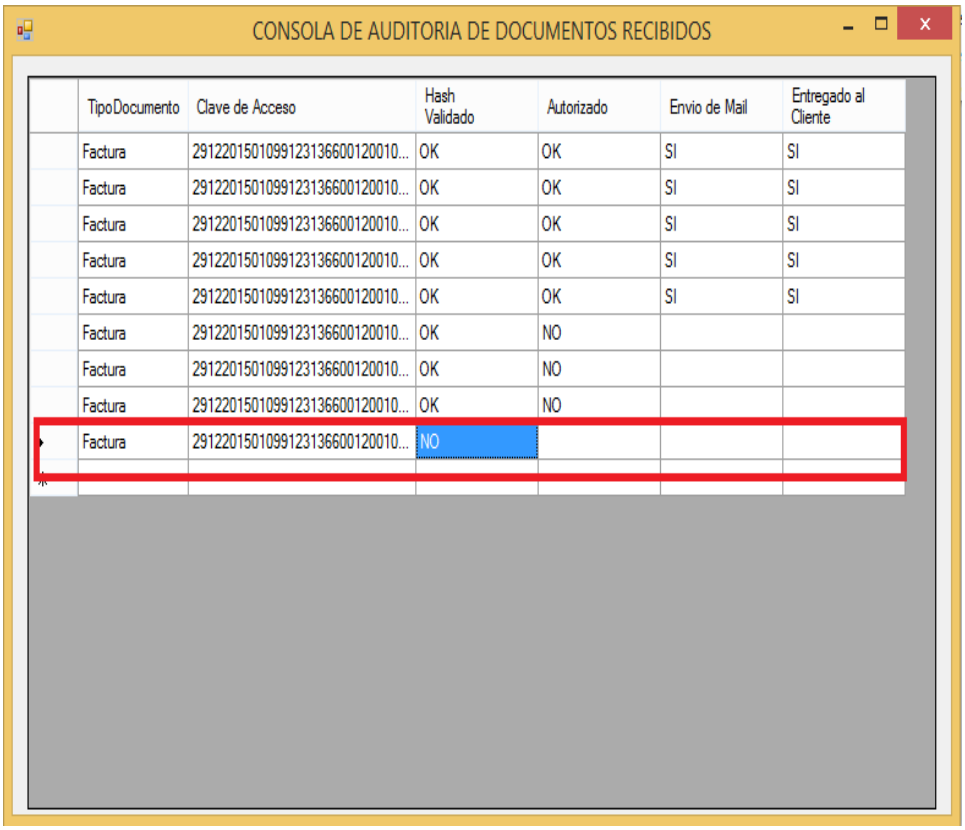


Figura 2.14 Consola de Auditoría de Documentos Recibidos

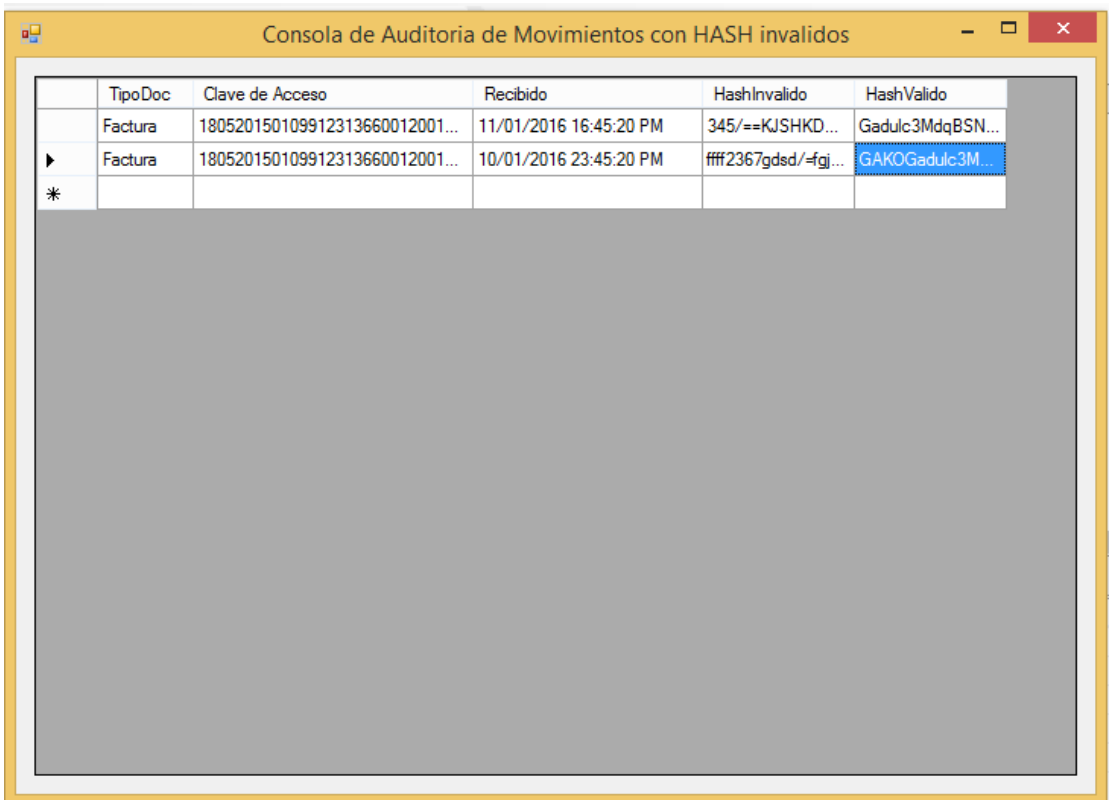


Figura 2.15 Consola de Auditoría de Documentos que no pasaron las pruebas

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 MEJORAS OBTENIDAS

Los resultados obtenidos con la implementación de estos controles son garantizar el correcto funcionamiento de las aplicaciones externas que ofrecen soluciones de facturación electrónica en general. De esta forma pueden incluir dentro de sus expectativas comerciales hacia sus clientes que cuentan con procesos de seguridad que certifican que los datos recibidos y enviados hacia sus clientes son válidos.

En la experiencia que tengo por las integraciones con diferentes ERP puedo recomendar que las mejoras obtenidas a través de estos controles

garanticen un Plus-Comercial a las empresas que ofrecen este servicio hoy en día en el país.

FECHA	DOC. RECIBIDOS	HASH NO VALIDO	AUTORIZADOS
01/01/2016	4500	10	4490
02/01/2016	4700	0	4700
03/01/2016	4000	0	4000
04/01/2016	2500	0	2500
05/01/2016	5000	0	5000
06/01/2016	5000	0	5000
07/01/2016	6000	5	5995

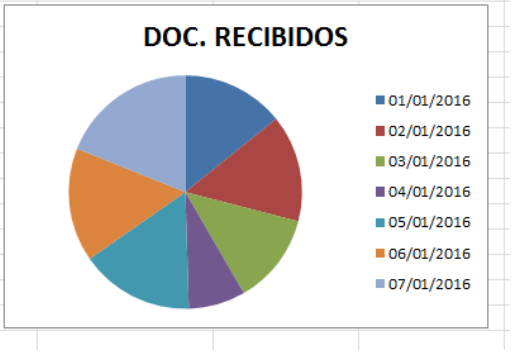


Figura 3.1 Estadísticas de monitoreo de información procesada

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIÓN

1. Frente a tantos ataques a la integridad de la información que se procesa desde y hacia la NUBE, enfrentamos entonces la necesidad implementar o mejorar controles que nos garanticen que la información recibida es válida.

2. Las consolas de auditoría en los Servidores Externos sirven para verificar los documentos que no cumplieron los controles de aceptación de documentos, esto se convierte en un semáforo para toma de medidas correctivas o preventivas para que los sistemas sean fiables desde el cliente hacia los servidores externos y viceversa.

3. La implantación de controles en las interfaces no aseguran totalmente que no pueda existir alguna inconsistencia en la información que se recibe, debido a que no existe un mecanismo totalmente seguro, lo que si ayuda es en la mitigación de las probabilidades de que estos escenarios no se repitan.

RECOMENDACIONES

- Una recomendación en un tiempo prudente es cambiar la forma de calcular los HASH de los archivos, para ellos existen varias opciones tales como las que se detallan:

    a. MD5

    b. SHA-3, según NIST en AGOSTO/2015 lo declara como una herramienta de última generación para asegurar la integridad de la información electrónica [5].

  Sería recomendable cambiar anualmente cambiar el método para el cálculo del hash.

- Es importante también validar que los canales de transmisión (HTTP / HTTPS) o medios por los cuales llega la información hacia los servidores

solo correspondan a equipos que pertenecen a clientes válidos. Es decir implementar una lista blanca de los todos clientes que cuentan con sus servicios activos

- Implementación de LOGS de auditoria para control de alertas frente a casos de documentos que no hayan pasado por las validaciones de HASH exitosamente.

- Implementar controles correctivos para tratar casos de incidencias de documentos electrónicos con estados de hash no válidos.

BIBLIOGRAFÍA

[1] Servicio de Rentas Internas, Comprobantes Electrónicos, http://www.sri.gob.ec/de/10109, fecha de consulta Agosto 2015

[2] Nicolas Change, Comprender los Servicios Web (parte 2), http://www.ibm.com/developerworks/ssa/webservices/tutorials/ws-understand-web-services2/, fecha de consulta Julio 2011

[3] Microsoft Corporation, Crear y probar un Servicio Web, https://support.microsoft.com/es-es/kb/309013, fecha de consulta Diciembre 2015

[4] Microsoft Corporation, Como crear nuevos archivos XML, https://msdn.microsoft.com/es-ec/library/cc438002(v=vs.71).aspx, fecha de consulta Diciembre 2015

[5] National Institute of Standars and tecnology NIST, Crytografia Hash Estándar, http://www.nist.gov/itl/csd/201508_sha3.cfm, fecha de consulta Agosto 2015

[6] National Institute of Standars and tecnology, Secure Hashing, http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html, fecha de consulta Agosto 2015