	Seguridad de la Información - Matriz
	ACTA DE REVISIÓN DE SEGURIDAD DE LA INFORMACIÓN

## 1.- REVISOR

<b>NOMBRES Y APELLIDOS</b>	Efrain Chamba
<b>CARGO</b>	Jefe de Seguridad de la Información
<b>FECHA DE REVISIÓN</b>	21/02/2020

## 2.- DETALLE

<b>NOMBRE DEL SERVIDOR:</b>	biometrico01.bancodesarrollo.fin.ec
<b>DIRECCION IP:</b>	172.16.192.3
<b>ROL:</b>	Servidor Web
<b>SISTEMA OPERATIVO:</b>	CENTOS 7
<b>SOFTWARE BASE:</b>	APACHE TOMCAT, MYSQL, POSTGRES, PHP, JBOS
<b>PROYECTO:</b>	Sistema de registro Biométrico (FullTime)

### 2.1.- REVISIÓN DEL SERVIDOR WEB

En la presente revisión de han identificados las siguientes vulnerabilidades.

	Vulnerabilidad	Severidad	Afectación	Remediación
1	Versión de Apache Tomcat insegura	Alta	Denegación del servicio web	Actualizar Apache Tomcat a la última versión estable
2	Contraseñas visibles en la integración del servidor de aplicaciones JBOS con la Base de datos y aplicativos de terceros	Alta	Acceso no autorizado de atacantes o usuarios maliciosos internos a las bases de datos que utiliza el sistema FullTime.	Implementar métodos de integración segura del servidor de aplicaciones JBOS con las bases de datos y aplicativos, en donde se encripten sus credenciales de la conexión.
3	Versión de Java Server Faces insegura	Media	Atacantes remotos realizar ataques de scripting entre sitios (XSS) a través de vectores que implican modificar el objeto de vista serializada.	Actualizar Java Server Faces a la última versión estable.
4	Existencia del protocolo SSL Versión 2 y 3.	Media	El trafico web encriptado utiliza protocolos inseguros. Un atacante puede explotar estos defectos para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.	Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0. Utilice TLS 1.1 (con conjuntos de cifrados aprobados) o superior en su lugar.

### 2.2.- REVISION DE LA APLICACION

El aplicativo FullTime presenta varias vulnerabilidades en su sistema de autenticación.

	Vulnerabilidad	Severidad	Afectación	Remediación
5	El sistema de autenticación actual permite la enumeración de usuarios.	Alta	Un atacante o un usuario interno con altos conocimientos tecnológicos puede intentar obtener un	Implementar en el sistema los controles necesarios para que no permita obtener información de los usuarios.

			listado de los usuarios del sistema para fines maliciosos.	
	El sistema de autenticación no permite administrar de manera adecuada las contraseñas: <ul style="list-style-type: none"> <li>- bloqueo de usuarios al ingresar un número máximo de intentos.</li> <li>- Periodicidad para renovación de contraseña.</li> <li>- Recuperación de contraseña olvidada.</li> </ul>	Media	Un atacante o un usuario interno con altos conocimientos tecnológicos puede intentar obtener mediante ingeniería social las credenciales de los usuarios del sistema para fines maliciosos.	Integrar el sistema de autenticación con el servicio de directorio activo.


### 2.3.- MITIGANTES


Para mitigar las posibles afectaciones que se puedan dar con la permanencia del aplicativo FullTime en la infraestructura tecnológica del Banco, se han llevado a cabo las siguientes acciones.

- El aplicativo web FullTime, los servidores en los cuales reside y los componentes que utiliza se encuentran aislados en un segmento de red protegido y sin acceso a los servicios de internet.
- El acceso al sistema FullTime por parte del personal es exclusivamente dentro de la red interna y través del protocolo HTTPS con certificado digital.
- La administración de las contraseñas para ingresar al portal será de forma manual, y deberán estar a cargo del área de Talento Humano, la cual obligará a cambiar a los usuarios su contraseña cada cierta periodicidad de tiempo, se recomienda 30 días.
- Adicionalmente, existe una carta de compromiso por parte del proveedor en la cual se comprometen a solventar las vulnerabilidades expuestas en los componentes de la aplicación con la publicación de una segunda versión del sistema FULLTIME. Se anexa Carta de Compromiso.

### 3.- CONCLUSIONES Y RECOMENDACIONES

- La aplicación FullTime y sus componentes, a la fecha, no cumplen con las especificaciones de seguridad de infraestructura tecnológica sin embargo debido a las mitigantes establecidas, es factible que dicho aplicativo pueda coexistir de manera controlada y temporal en el ambiente de producción, siempre y cuando se cumpla el compromiso por parte del proveedor para el cierre de las vulnerabilidades reportadas.
- En necesario que se califique el riesgo de dichas vulnerabilidades y que sea asumido formalmente por el área correspondiente hasta que sean solventadas, o de ser el caso, hasta que se cumpla el tiempo de permanencia del sistema en el ambiente de producción.
- Previa salida producción se debe cumplir con la política de cambio contraseña robusta para el usuario administrador del servidor y el administrador del aplicativo FullTime.
- Una vez solventadas las vulnerabilidades reportadas se debe cumplir con el proceso periódico de actualización y parchado integral del servidor tanto del sistema operativo, el software base, esto con el fin de minimizar la aparición de nuevas vulnerabilidades que puedan atentar contra la confidencialidad, integridad, y disponibilidad de la información que alberga el sitio web.

<b>Revisado por:</b>
 <b>Efraín Chamba</b> <b>Jefe de Seguridad de la Información</b>





# CASA PAZMIÑO S.A.

Import & Export

Oficio N° 2019-DS-0003  
Quito, 27 de junio del 2019

Señores,

**BANCODESARROLLO**

Atención:

Ing. Néstor Arajundi Morales  
Gerente de Operaciones y Tecnología

Ing. Héctor Sanipatín  
Coordinador de Producción  
Presente-

De mis consideraciones:

Reciba usted un cordial saludo de nuestra empresa **CASA LUIS PAZMIÑO IMPORT & EXPORT S.A.**, empresa dedicada al desarrollo de software y a la comercialización de equipos de oficina desde el año 1985.

En respuesta a sus atentos correos enviados el día 26 de Junio de 2019, manifestamos lo siguiente:

- No soporta Protocolo seguro de transporte HTTPS cifrado con certificado de autenticación y TLS Transport Layer Security, para acceso de los usuarios internos del banco. Esto también incluya a componentes de acceso al servidor de correo electrónico.

**Respuesta:** Para solventar este punto nuestra empresa realizara un proxy inverso, en un plazo de 15 días hábiles.

- Componentes de versiones obsoletas de software base (Jboss 5.1, JDK 6.75, PostgreSQL 9.3), poseen vulnerabilidades que se constituyen en un alto riesgo de ataques.

**Respuesta:** Para solventar este punto nuestra empresa esta trabajando en la actualización de nuestro sistema Fulltime Web versión 3.0, la misma que tiene como fecha tentativa de lanzamiento en el año 2020. Esta actualización tendrá la última versión en plataforma WildFly más estable y con lenguaje de programación Java compatible para sistemas operativos Windows y Linux, con motor de base de datos MS SQL Server y PostgreSQL.

Es importante señalar que nuevos requerimientos por parte de nuestros clientes, para esta nueva versión lo estamos recibiendo hasta octubre de este año.

Por la fina y positiva atención que se sirva dar a la presente, procederemos como es su sentir con la inmediata terminación del proyecto del sistema de control de asistencia.

Anticipo mis debidos agradecimientos.

Atentamente,

Jose Luis Pazmiño  
Gerente Nacional de Ventas  
**CASA PAZMIÑO IMPORT & EXPORT**

CC: Jose Vargas  
Director Administrativo

Matriz  
Av. Concha F25-17 (1123) y Colón (esq.)  
(593-2) 2 504675 - 2557512 - 2503398  
2557514 - 2503401  
Quito - Ecuador

**Sucursales**

Ambato: 04 2523114 / 04 2525511  
Guayaquil: 04 2523774 / 04 2523776



**echamba@bancodesarrollo.fin.ec**

---

**De:** Michelle Castañeda <mcastaneda@bancodesarrollo.fin.ec>  
**Enviado el:** miércoles, 5 de febrero de 2020 8:16  
**Para:** echamba@bancodesarrollo.fin.ec  
**CC:** 'Yolanda Espejo'  
**Asunto:** RV: Compromiso Casa Pazmino

Buen día Efraín,

Sobre el compromiso de Casa Pazmiño para solucionar el tema de los correos electrónicos, aunque en la carta emitida por ellos no está escrito explícitamente el tema de los correos, en el mail anterior podrá observar que ya nos emitieron una respuesta favorable a nuestro pedido.

Para el conocimiento de todos,

Cordialmente,

Michelle Castañeda  
ASISTENTE DE TALENTO HUMANO



**Dir:** Calle Ladrón de Guevara E13-408 y Barcelona esq. (Oficina Matriz)

**Telf:** 2900-109 Ext: 517

**Web:** [www.bancodesarrollo.fin.ec](http://www.bancodesarrollo.fin.ec)

 NO IMPRIMA ESTE CORREO INNECESARIAMENTE

**De:** fcuichan@casapazmino.com.ec <fcuichan@casapazmino.com.ec>  
**Enviado el:** martes, 04 de febrero de 2020 18:06  
**Para:** 'Michelle Castañeda' <mcastaneda@bancodesarrollo.fin.ec>  
**Asunto:** RE: Compromiso Casa Pazmino

Estimada Michelle,

Para informarle que la nueva versión de Full Time Web versión 3.0 se encuentra en la fase de análisis por lo que llegado este requerimiento se procederá al realizar la socialización sobre las vulnerabilidades de los aplicativos de los correos electrónicos para que sea tomando muy en cuenta.

Quedo atento a sus comentarios

Saludos cordiales,



**Fernando Cuichan**  
Coordinador Área de Sistemas  
Oficina Matriz  
Telf: (593) 2 2557 514 ext 112  
Cel: (593) 9 5882 5265  
E-mail: fcuichan@casapazmino.com.ec



[www.casapazmino.com.ec](http://www.casapazmino.com.ec)

Quito - Ecuador

Av. Coruña E25-32 y 12 de Octubre.



COMPACTADORAS  
DE DISCOS



TERMINALES  
TODO ECUANO



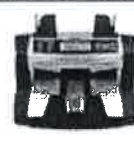
CONTROL DE ASISTENCIA  
CONTROL DE ACCESOS



CONTROL DE TURNOS Y FILAS



DESTRUCTORA  
DE DOCUMENTOS



CONTADORAS DE BILETES  
CONTADORAS DE MONEDAS

Por favor imprimir solamente lo que sea necesario. Piense en el medio ambiente.

**From:** Michelle Castañeda <mcastaneda@bancodesarrollo.fin.ec>

**Sent:** Wednesday, January 29, 2020 5:37:55 PM

**To:** [ilp1155@hotmail.com](mailto:ilp1155@hotmail.com) <[ilp1155@hotmail.com](mailto:ilp1155@hotmail.com)>

**Subject:** RV: Compromiso Casa Pazmino

Estimado Jose Luis,

Un gusto saludarle desde Banco CODESARROLLO - Talento Humano,

De acuerdo con la instalación del sistema FULLTIME, se nos emitió una carta compromiso para solucionar las vulnerabilidades encontradas en dicho sistema que no permitían el uso de todas las características del sistema adquirido. (Esto fue en Junio del 2019)

Sin embargo, nuestro Jefe de Seguridad de la Información, Ing. Efraín Chamba, para poder autorizar el uso de la ventana a nivel nacional requiere que los aplicativos del sistema operativo soporten los protocolos de seguridad de correo electrónico, para poder usar el mismo. Pero en la carta emitida en Junio del 2019, no se menciona dicho cambio para el sistema 3.0.

De esa forma solicitarle su respuesta que avale que en la próxima actualización de FullTime se trabajará sobre las vulnerabilidades de los aplicativos de los correos electrónicos; y así finalmente cumplir con lo acordado en el contrato de compra.

En espera de su gentil respuesta, me despido y le agradezco.

Cualquier novedad nos encontramos a las órdenes,

Atte.

Michelle Castañeda  
ASISTENTE DE TALENTO HUMANO



**Dir:** Calle Ladrón de Guevara E13-408 y Barcelona esq. (Oficina Matriz)

**Telf:** 2900-109 Ext: 517

**Web:** [www.bancodesarrollo.fin.ec](http://www.bancodesarrollo.fin.ec)

**NO IMPRIMA ESTE CORREO INNECESARIAMENTE**