AAI-04-2017

21 DE NOVIEMBRE DE 2017

INGENIERO
HORACIO ALVARADO BOGANTES
ALCALDE

ASUNTO: AUDITORÍA SOBRE SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD (INFORME DE VULNERABILIDADES INTERNAS Y EXTERNAS REALIZADA POR DELOITTE)

Estimado señor:

Esta Auditoría contrató algunos servicios en el campo de la Auditoría Informática, mediante la Licitación Abreviada número 2015LA-000020-0002600001, denominada *"Contratación de Servicios de auditoría a la Unidad de Tecnología de Información basado en las Normas de aplicación general (N-2-2007-CO-DFOE), de la Municipalidad de Belén"*, la cual estuvo a cargo de la empresa la empresa Deloitte & Touche, S.A.

La contratación fue dividida en varias etapas, las cuales pueden clasificarse, en una primera fase relacionada con un estudio inicial en la que se obtuvieron las vulnerabilidades del sitio web y una segunda etapa fase, respecto de la cual se brindó un seguimiento de las acciones implementadas por la Administración (Staff Informática), con el fin de atender dichas situaciones de vulnerabilidad.

Actualmente la citada contratación se encuentra en esta segunda etapa de seguimiento, sobre la cual la empresa contratista ya ha emitido los informes correspondientes.

De conformidad con el Plan de Pruebas llevado a cabo, el primer informe de auditoría (sobre la determinación de vulnerabilidades) detalla una serie de oportunidades de mejora que, en caso de ser consideradas y atendidas en cuanto a la vulnerabilidad que describen, podrían permitir a la Municipalidad remediar debilidades de seguridad existentes en la infraestructura tecnológica actual, y en las actividades de seguridad informática aplicadas por los responsables de las tecnologías de información, al igual que establecer y mantener un esquema de operación más seguro y controlado.

Por otra parte, es importante tener presente que en el citado primer informe resultante del estudio realizado, se utilizaron leyendas para describir los atributos de las observaciones o vulnerabilidades enumeradas en el mismo.

En el siguiente cuadro se describen dichos conceptos aplicados:

	FACTORES INCLUIDOS EN LOS HALLAZGOS		
NIVEL	**Riesgo**	**Esfuerzo de Resolución**	**Complejidad del ataque**
Alto (A)	Se refiere a vulnerabilidades en las cuales su explotación puede derivar en un compromiso total de la confidencialidad, integridad y/o disponibilidad del dispositivo en sí y eventualmente de otros componentes conectados; generalmente afecta a recursos críticos de la infraestructura, como servidores de bases de datos, o accesos a sistemas aplicativos y/o a dispositivos de control de tráfico de red.	Requiere modificación de código de aplicaciones o rediseños de infraestructura, pruebas, análisis de calidad y soporte en la puesta en producción. Se deberá incurrir en varios días de esfuerzo para su resolución.	Cuando la probabilidad del ataque es muy baja, o bien se requieran recursos tecnológicos y humanos complejos para poder concretar el ataque.
Medio (M)	Se refiere a vulnerabilidades cuya explotación puede derivar en el compromiso de algún atributo de seguridad, pudiendo afectar tanto a recursos críticos como no críticos de la infraestructura.	Su solución puede requerir desde algunas horas hasta algunos días de esfuerzo.	Cuando la probabilidad del ataque es media, o bien se requieran recursos tecnológicos y humanos relativamente sencillos para poder concretar el ataque.
Bajo (B)	Se refiere a vulnerabilidades menores, por ej. Divulgación de información no sensitiva como versiones de software.	Se deberán realizar cambios menores a la configuración de los recursos afectados. Su resolución requiere solamente algunas horas de esfuerzo.	Cuando la probabilidad del ataque es alta, existe información de dominio público sobre cómo explotar la vulnerabilidad, y no se requieren recursos tecnológicos y humanos complejos para poder concretar el ataque.

En virtud de que el estudio en referencia, se enfocó en analizar separadamente las vulnerabilidades externas e internas de la Municipalidad, a continuación, se describirá en capítulos aparte, los principales de los informes correspondientes emitidos por la empresa contratista Deloitte.

I. VULNERABILIDADES EXTERNAS

Con respecto a las vulnerabilidades externas (página web institucional) la primera etapa de la Auditoría, resulta importante resaltar los siguientes aspectos:

A. **Los objetivos** de la Auditoría se relacionan con la identificación de las posibles debilidades en las configuraciones de seguridad de la plataforma tecnológica expuesta a Internet, mediante la simulación de un ataque malicioso contra los sitios web oficiales de la compañía y sus componentes, así detectar vulnerabilidades en la captura y procesamiento de los datos en la aplicación.

   Sobre el particular, el principal objetivo fue verificar si es posible la obtención de datos valiosos, confidenciales para un atacante que pueda afectar la confidencialidad, integridad y disponibilidad de la información del sitio oficial de la Municipalidad de Belén.

B. **El alcance** del estudio, se puede ubicar en los siguientes aspectos:

   Las tareas de investigación consistieron en:

   Identificar posibles vulnerabilidades en el sitio web definido.

   Evaluar si dichas vulnerabilidades podrían llegar a ser explotadas por un intruso o usuario malicioso para obtener control de cuentas o modificar transacciones, estableciendo diferentes escenarios para la simulación de ataques a través de las técnicas implementadas por la empresa de evaluación o intrusión contra plataformas web.

   Además se informa que el desarrollo de las pruebas se focalizó en comprender si los atributos de confidencialidad, integridad y disponibilidad de la información del sitio podrían en el futuro estar comprometidos, en los escenarios de ataque planteados.

C. En el siguiente cuadro, se resumen las vulnerabilidades externas determinadas:

ID.	Vulnerabilidad	Riesgo	Ataque	Resolución
Web-01	Sitio vulnerable a SQL Injection	Alto	Medio	Alto
Web-02	El sitio es vulnerable a ataques Cross Site Scripting	Alto	Medio	Medio
Web-03	Software desactualizado	Alto	Medio	Alto
Web-04	Divulgación de información sensible en pantalla de error	Medio	Medio	Bajo
Web-05	Vulnerabilidad en los certificados SSLv3	Medio	Medio	Medio
Web-06	Acceso a ficheros del servidor web	Medio	Medio	Bajo
Web-07	Métodos no seguros de autenticación	Medio	Medio	Medio
Web-08	No están configuradas las características HTTP X-Frame-Options dentro del código fuente de la aplicación.	Medio	Medio	Bajo
Web-09	Autocomplete no declarado en el código fuente.	Medio	Medio	Bajo

De lo descrito en el cuadro anterior, se evidencia que un total de tres vulnerabilidades se encontraban dentro de la categoría de riesgo **"alto"** y seis en riesgo **"medio".**

G. Sobre el mencionado estudio en materia de Seguridad Informática, es importante tomar en consideración que, el Concejo, en la Sesión Ordinaria Nº 05-2017, celebrada el 31 de enero del año en curso, conoció la respuesta de la Coordinadora de Gestión Informática referente a las vulnerabilidades detectadas en el estudio citado. Al respecto, dicho Órgano colegiado, tomó el Acuerdo que se transcribe a continuación, en lo de relevancia:

***Artículo 7**. Se conoce el oficio AMB-MC-024-2017 del Alcalde Horacio Alvarado. Trasladamos el oficio INFO-004-2017, suscrito por Alina Sánchez, coordinadora de la Unidad de Informática, donde remite el informe solicitado sobre las acciones tomadas en torno a la Auditoría realizada a dicha unidad. Al respecto, y en cumplimiento del acuerdo tomado en la Sesión Ordinaria Nº 75-2016, adjunto enviamos el documento mencionado para su conocimiento.*

INFO-004-2017
Se detalla, En respuesta al memorando AMB-MA-004-2017, fechado 18 de enero 2017,

según acuerdo tomado por el Concejo Municipal durante la sesión ordinaria número 75-2016, se adjunta el informe solicitado acerca de las acciones tomadas por la Unidad de Informática para dar solución a los riesgos de vulnerabilidad señalados en el informe de Auditoría Interna ante el Concejo Municipal.
(…)
CONCLUSIÓN SOBRE VULNERABILIDADES Y MEJORAS REALIZADAS
Según revisión a todas las vulnerabilidades encontradas en el informe, se detectó que la gran mayoría corresponden a situaciones ligadas a equipos con Sistemas Operativos antiguos u obsoletos (Windows XP, Windows 2003, Fox Pro y VPRO5), los cuales eran utilizados para los sistemas municipales antiguos (Financieros y Base de Datos). Dichos equipos fueron reemplazados con la puesta en marcha del nuevo sistema de gestión municipal (SIGMB), con lo cual dichas vulnerabilidades fueron solventadas. En lo referente al sitio web, con los trabajos de mejora que se han venido realizando desde finales del año 2016 a la fecha, todas las vulnerabilidades serán mitigadas y se ampliará la seguridad y versatilidad de los servicios brindados a través del sitio web municipal.

SE ACUERDA CON CUATRO VOTOS A FAVOR DE LOS REGIDORES Eddie Méndez, Lorena González, María Antonia Castro, Gaspar Rodríguez Y UNO EN CONTRA DEL REGIDOR Jose Luis Venegas: PRIMERO: Dar por recibido el oficio INFO-004-2017. (...)"

D. No obstante lo anterior, en una segunda etapa de la Auditoría, la empresa contratista realizó el análisis correspondiente al seguimiento de las medidas tomadas por la Administración (Staff Informática) en atención a las vulnerabilidades evidenciadas.

Dicha revisión tuvo como **objetivo:** *"Evaluar el proceso de mitigación* de los riesgos determinados, por el personal técnico de la Municipalidad de Belén, en lo que respecta a la resolución de vulnerabilidades asociadas a la plataforma tecnológica."

El **alcance** de la citada revisión se orientó en: *"Identificar posibles vulnerabilidades en el sitio web definido, evaluar si dichas vulnerabilidades podrían llegar a ser explotadas por un intruso o usuario malicioso para obtener control de cuentas o modificar transacciones, estableciendo diferentes escenarios para la simulación de ataques a través de nuestras técnicas de evaluación e intrusión contra plataformas web."*

Esta fase de la Auditoría fue ejecutada entre el 18 y el 22 de setiembre de 2017, con el fin de encontrar oportunidades de mejora en la página web.

La revisión permitió la ubicación de cada una de las vulnerabilidades determinadas, de acuerdo con la siguiente clasificación, según su atención por la Administración:

Solucionada: Se refiere a que la vulnerabilidad ha sido mitigada en la totalidad de los recursos reportados como afectados durante el proceso de pruebas original.
Parcialmente solucionada: Se refiere a que la vulnerabilidad ha sido mitigada en parte de los recursos afectados; no obstante, todavía se encuentra en alguno o varios de los equipos.

No solucionada: Se refiere a que la vulnerabilidad no ha sido mitigada en ninguno de los equipos reportados como afectados por la misma.

Justificada: Se refiere a que la vulnerabilidad aún existe pero fue justificada por parte de la Municipalidad.

E. En el siguiente cuadro, se resumen los resultados obtenidos en el la etapa de seguimiento descrita:

ID.	Vulnerabilidad	Solucionada	No Solucionada
Web-01	Sitio vulnerable a SQL Injection	SI	
Web-02	El sitio es vulnerable a ataques Cross Site Scripting		NO
Web-03	Software desactualizado		NO
Web-04	Divulgación de información sensible en pantalla de error	SI	
Web-05	Vulnerabilidad en los certificados SSLv3		NO
Web-06	Acceso a ficheros del servidor web	SI	
Web-07	Métodos no seguros de autenticación	SI	
Web-08	No están configuradas las características HTTP X-Frame-Options dentro del código fuente de la aplicación.	SI	
Web-09	Autocomplete no declarado en el código fuente.		NO

De lo consignado en el cuadro anterior, se evidencia que un total de 5 vulnerabilidades (56 %) fueron atendidas y solucionadas, mientras que un total de 4 (44 %) de ellas, aún no han sido atendidas por lo que permanecen dichas vulnerabilidades.

II. VULNERABILIDADES INTERNAS

Con respecto a las vulnerabilidades en la infraestructura informática internas web institucional) la primera etapa de la Auditoría, resulta importante resaltar los siguientes aspectos:

A. **El objetivo** del estudio en esta parte, fue el de identificar posibles vulnerabilidades existentes en la Infraestructura de la Red Interna de la Municipalidad, haciendo uso de 1 rango de IP. La fase consistió en evaluar si dichas vulnerabilidades que podrían llegar a ser explotadas por un intruso o usuario malicioso para obtener control de los equipos, modificar las transacciones o poner en riesgo la estabilidad de la red y sus servicios pudiendo ocasionar eventuales pérdidas económicas.

B. **El alcance** del estudio se puede ubicar en los siguientes aspectos:

   Las tareas de investigación consistieron en identificar posibles vulnerabilidades en la red interna, servidores y servicios asociados, en un rango de red seleccionado por el personal de la Municipalidad de Belén. Evaluar si dichas vulnerabilidades podrían llegar a ser explotadas por un intruso o usuario malicioso para obtener control de cuentas o modificar transacciones, estableciendo diferentes escenarios para la simulación de ataques a través de las técnicas implementadas por la empresa de evaluación e intrusión contra infraestructuras de red internas.

   Además se establece que, el desarrollo de las pruebas se focalizó en comprender si los atributos de confidencialidad, integridad y disponibilidad de la información del sitio podrían llegar a ser comprometidos. Por lo anterior las pruebas se orientaron en un total de 256 direcciones de IP de la institución.

C. El estudio permitió determinar un total de **41 vulnerabilidades** en la infraestructura tecnológica interna; de las cuales **21** (51 %) de ellas se encuentran dentro de la categoría de riesgo **"alto**." Adicionalmente **20** vulnerabilidades, es decir un 49 % se ubican en un nivel de riesgo "**medio"**.

   En el siguiente cuadro, se transcriben y resumen las vulnerabilidades internas determinadas, que poseen un riesgo alto:

ID.	Vulnerabilidad	Riesgo	Ataque	Resolución
Int-01	Servicio de DameWare mini remote de control vulnerable a desbordamiento de búfer	Alto	Medio	Bajo

ID.	Vulnerabilidad	Riesgo	Ataque	Resolución
Int-02	La versión de Windows XP ya no cuenta con soporte	Alto	Medio	Alto
Int-03	MS15-034: vulnerabilidad en el HTTP.sys podría permitir ejecución de código remoto.	Alto	Medio	Bajo
Int-04	MS08-067: Vulnerabilidad en el servicio de SERVER con solicitudes RPC podría permitir la ejecución remota de código malicioso (958644)	Alto	Medio	Bajo
Int-05	El equipo presenta múltiples vulnerabilidades Microsoft SMB con las cuales se puede tomar el control sobre el equipo.	Alto	Medio	Bajo
Int-06	MS14-066: Vulnerabilidad en Schannel podría permitir la ejecución de código malicioso.	Alto	Medio	Bajo
Int-07	El nombre de la comunidad de SNMP está por defecto.	Alto	Medio	Bajo
Int-08	El demonio “telnetd” de FreeBSD es vulnerable a desbordamiento de buffer.	Alto	Medio	Bajo
Int-09	La version de windows server 2003 ya no cuenta con soporte.	Alto	Bajo	Alto
Int-10	Multiples vulnerabilidades en HP System Management Homepage 7.5.0.	Alto	Medio	Bajo
Int-11	Open NMS vulnerable a ejecución remota de código.	Alto	Medio	Medio
Int-12	Usuario y contraseña por defecto en el servidor de almacenamiento HP.	Alto	Bajo	Bajo
Int-13	MS112-020: Vulnerabilidad en Microsoft Windows podría permitir la ejecución de código malicioso.	Alto	Bajo	Bajo
Int-14	Divulgación de información por la vulnerabilidad Heartbleed que afecta Open SSL.	Alto	Medio	Bajo
Int-15	Vulnerabilidad en versión de OpenSSH.	Alto	Medio	Bajo
Int-	Acceso a recursos compartidos	Alto	Bajo	Bajo

ID.	Vulnerabilidad	Riesgo	Ataque	Resolución
16	sin requerir autenticación.			
Int-17	Acceso no autorizado al servidor VNC	Alto	Bajo	Bajo
Int-18	Versión de web server sin soporte.	Alto	Bajo	Alto
Int-19	El servidor Apache HTTP es vulnerable a ataques de DoS.	Alto	Medio	Bajo
Int-20	El Listener TNS Oracle permite el servicio de registro desde un host remoto.	Alto	Medio	Medio
Int-21	Vulnerabilidad firma de paquetes no está habilitada el servidor SMB remoto.	Alto	Medio	Bajo

D. De igual forma, en la segunda etapa de la Auditoría, la empresa contratista realizó el análisis correspondiente al seguimiento de las medidas tomadas por la Administración (Staff Informática), en atención a las vulnerabilidades internas determinadas.

Dicha revisión consistió en analizar e identificar oportunidades de mejora, para luego revisar los parámetros de acuerdo a las mejores prácticas de seguridad y así evitar que existan vulnerabilidades que puedan llegar a ser explotadas por agentes externos."

Esta fase de la Auditoría fue ejecutada entre el **21 y el 26 de setiembre de 2017**.

La revisión permitió la ubicación de cada una de las vulnerabilidades determinadas, de acuerdo con la siguiente clasificación, según su atención por la Administración:

Solucionada: Se refiere a que la vulnerabilidad ha sido mitigada en la totalidad de los recursos reportados como afectados durante el proceso de pruebas original.

Parcialmente solucionada: Se refiere a que la vulnerabilidad ha sido mitigada en parte de los recursos afectados; no obstante, todavía se encuentra en alguno o varios de los equipos.

No solucionada: Se refiere a que la vulnerabilidad no ha sido mitigada en ninguno de los equipos reportados como afectados por la misma.

Justificada: Se refiere a que la vulnerabilidad aún existe pero fue justificada por parte de la Municipalidad.

F. En el siguiente cuadro, se resumen los resultados obtenidos en la etapa de seguimiento descrita:

Clasificación de la Vulnerabilidad	Cantidad de vulnerabilidades
Solucionadas	20
Parcialmente solucionadas	6
No solucionadas	6
Justificadas	9
TOTAL	**41**

Como se puede observar, han sido atendidas por la Administración (Staff Informática) un total de 20 vulnerabilidades, un 48 % del total, las que fueron identificadas al cierre de Setiembre de 2017; además 6 de ellas, un 13 % del total se encuentran parcialmente solucionadas.

Por otra parte, nueve vulnerabilidades (un 23 %) fueron justificadas por la Administración; y finalmente seis (18 % del total) no han sido atendidas. Al respecto, en el cuadro siguiente, se enumeran las seis vulnerabilidades no solucionadas por la Administración (Staff Informática):

ID.	Vulnerabilidad
INT-07	El nombre de la comunidad de SNMP está por defecto.
INT-20	El Listener TNS Oracle permite el servicio de registro desde un host remoto.
INT-30	Debilidad en el servidor DNS por búsquedas recursivas.
INT-31	Debilidad en el servidor DNS posibilita el cache snooping.
INT-32	Servidor DNS permite realizar Ataques DDoS.
INT-40	El Servicio Mongo DB y API no cuenta con autenticación.

Complementariamente, a continuación se presenta un cuadro que compara los criterios plasmados en el Informe de la empresa Deloitte (referentes a las vulnerabilidades no solucionadas) y las opiniones opuestas, de la Unidad de Informática, según lo mencionado informe INFO-004-2017:

Vulnerabilidad	Informe de Deloitte	Criterio de Informática (Mejoras aplicadas)
INT-07: *El nombre de la comunidad de SNMP está por defecto.*	(Presenta un nivel de riesgo alto). **No solucionada.**	El informe INFO-004-2017 de la Unidad de Informática no se refiere a esta vulnerabilidad.
INT-20: *El Listener TNS*	(Presenta un nivel	Se actualizó completamente el equipo

Vulnerabilidad	Informe de Deloitte	Criterio de Informática (Mejoras aplicadas)
Oracle permite el servicio de registro desde un host remoto.	de riesgo alto). **No solucionada.**	mencionado en la vulnerabilidad, dicho equipo posee la versión 11G reléase 11.2.0.4.0, tal y como se menciona en las recomendaciones.
INT-30: *Debilidad en el servidor DNS por búsquedas recursivas.*	(Presenta un nivel de riesgo medio). **No solucionada.**	Se procede a deshabilitar las búsquedas recursivas en ambos servidores DNS, tal y como se recomienda en esta vulnerabilidad.
INT-31: *Debilidad en el servidor DNS posibilita el cache snooping.*	(Presenta un nivel de riesgo medio). **No solucionada.**	Con la nueva configuración de los nuevos equipos de comunicación de la municipalidad, así como las políticas o reglas establecidas en el Check Point, las consultas DNS son permitidas únicamente en la red local, con lo cual no se permite tráfico DNS hacia el exterior. De igual manera se procede a realizar los ajustes en los DNS internos para evitar ambas vulnerabilidades. ***(De acuerdo con el informe INFO-004-2017, esta respuesta aplica para las vulnerabilidades INT-31 e INT-32).***
INT-32: *Servidor DNS permite realizar Ataques DDoS.*	(Presenta un nivel de riesgo medio). **No solucionada.**	
INT-40: *El Servicio Mongo DB y API no cuenta con autenticación.*	(Presenta un nivel de riesgo medio). **No solucionada.**	Durante el primer trimestre del presente año se está en proceso de depuración de la Base de Datos y aplicando mejoras en su configuración, lo anterior mediante el proceso compra 2016CD-000107-0002600001.
Web-02: El sitio es vulnerable a ataques Cross Site Scripting.	(Presenta un nivel de riesgo alto). **No solucionada.**	Durante el último trimestre del año 2016 y el presente año se está trabajando en las mejoras de diseño y seguridad de la página web, así como los nuevos módulos que la conforman, lo anterior mediante el proceso de compra 2016LA-000013-0002600001.
Web-03: Software desactualizado.	(Presenta un nivel de riesgo alto). **No solucionada.**	Se aplicaron todas las actualizaciones de sistema operativo que estaban disponibles. Además, se actualizaron las versiones de los servicios. Mediante la contratación de mantenimiento y

Vulnerabilidad	Informe de Deloitte	Criterio de Informática (Mejoras aplicadas)
		desarrollo del sitio web se establecen políticas de actualización y control de versiones del sistema operativo y sus servicios.
Web-05: Vulnerabilidad en los certificados SSLv3	(Presenta un nivel de riesgo medio). **No solucionada.**	Dentro de las mejoras que se están realizando en el sitio web de la municipalidad se están modificando las aplicaciones para que excluyan o reemplacen las referencias a servidores internos o cualquier otro tipo de dirección. Además, se bloquea el acceso a directorios restringidos, así como la posibilidad de ejecutar comandos fuera del directorio raíz del servidor. Se renombrarán las pantallas de autenticación para administradores y se implementarán certificados de seguridad HTTPS para asegurar que las credenciales de los administradores se trasmitan por canales seguros y de forma cifrada. Se aplicarán configuración de seguridad para evitar el "clickjacking". **(*De acuerdo con el informe INFO-004-2017, esta respuesta aplica para las vulnerabilidades de la Web-04 a la Web-08).***
Web-09: Autocomplete no declarado en el código fuente.	(Presenta un nivel de riesgo medio). **No solucionada.**	Según las recomendaciones realizadas se procedió a deshabilitar el autocompletar en el campo de contraseña de todas las páginas que la requieran.
TOTAL	**10 Vulnerabilidades (6 Internas y 4 Externas)**	

Con referencia a las vulnerabilidades justificadas, es importante indicar que, las mismas, aun cuando poseen dicha condición, de conformidad con los criterios de la Encargada de la Unidad de Informática, la Administración debe buscar las soluciones a dichas vulnerabilidades.

Al respecto, esta Auditoría Interna, solicitó una ampliación sobre el concepto de vulnerabilidad justificada a la empresa contratista que realizó el estudio en referencia. En su respuesta, la empresa Deloitte, manifestó lo siguiente, en lo de relevancia:

"El justificado, indica que la administración de TI no cuenta con algún recurso en particular para atender la vulnerabilidad, o el servicio se encuentra obsoleto. Pero efectivamente (…) no necesariamente que se encuentre justificado no quiere decir que no deban buscarse soluciones. En este caso en particular la mayoría de "justificado" es de la base de datos del sistema Municipal anterior, el "viejo".

Con el fin de tener mayor claridad sobre los casos de vulnerabilidades justificadas, a continuación se describen las mismas, para que sean atendidas, según lo establecido anteriormente:

ID.	Vulnerabilidad	Justificación de la vulnerabilidad de la Unidad de Informática
INT-08	El demonio "telnetd" de FreeBSD es vulnerable a desbordamiento de buffer.	*"Dicha vulnerabilidad fue solventada bloqueando las conexiones por telnet al equipo mencionado, lo anterior mediante la desactivación en el propio equipo, así como bloqueo mediante el Check Point. Dicho equipo con la implementación del SIGMB no se encuentra en producción, únicamente está como consulta."*
INT-17	Acceso no autorizado al servidor VNC.	*"Se deshabilitó la opción "No Authentication" en las opciones de seguridad del servidor VNC con lo cual se solventó la vulnerabilidad existente".*
INT-19	El servidor Apache HTTP es vulnerable a ataques de DoS.	*"Dicha vulnerabilidad fue solventada actualizando el Apache a la versión 2.4.16 en el equipo mencionado. Dicho equipo con la implementación del SIGMB no se encuentra en producción, únicamente está como consulta".*
INT-26	Dispositivos utilizan protocolo telnet para las conexiones remotas el cual es considerado como no seguro.	*"Se hace revisión de todos los equipos enlistados y se procede a bloquear las conexiones por telnet en los equipos que aún están en funcionamiento. En los equipos de monitoreo de las UPS y sensores de temperatura, se mantiene el telnet exclusivamente para el personal autorizado. Se realiza bloqueo mediante el Check Point".*
INT-33	Servidor IP Forwarding habilitado en el host remoto.	*"Los equipos mencionados en esta vulnerabilidad, por la naturaleza de las funciones que realizan requieren tener habilitado el redireccionamiento IP. Cabe destacar que dichos equipos no están expuestos a Internet, sino utilizan conexiones MPLS o líneas dedicadas, lo cual no representa ningún riesgo".*
INT-34	Servidor inyección de código en texto plano en el servicio STARTTLS Y STLS del	*"Con los cambios establecidos en el correo electrónico institucional, el municipio ya no posee servidor de correo dentro de su LAN, sino que utiliza Office 365, ante lo cual el servicio de Exchange está en la nube,*

ID.	Vulnerabilidad	Justificación de la vulnerabilidad de la Unidad de Informática
	protocolo IMAP Y POP3	*por lo que dicha vulnerabilidad ya no está presente."*
INT-35	Habilitado el acceso anónimo al servicio FTP.	*"La IP corresponde a un equipo que se encontraba en proceso de reemplazo, debido a cambios en los sistemas utilizados anteriormente en la Municipalidad y la puesta en marcha del nuevo Sistema de Gestión Municipal (SIGMB). Dicho equipo ya no se encuentra en funcionamiento".* ***(De acuerdo con el informe INFO-004-2017, esta respuesta aplica para las vulnerabilidades de la INT-35, INT-36 e INT-37).***
INT-37	Divulgación de información debido a la versión Apache HTTP	La misma de la Vulnerabilidad anterior.
INT-41	Vulnerabilidad de divulgación de información en el servidor Apache.	*"La IP corresponde a un equipo que se encontraba en proceso de reemplazo, debido a cambios en los sistemas utilizados anteriormente en la Municipalidad y la puesta en marcha del nuevo Sistema de Gestión Municipal (SIGMB). Dicho equipo ya no se encuentra en funcionamiento".*
TOTAL	**9 Vulnerabilidades Internas**	

III. CONSIDERACIONES FINALES

De conformidad con los aspectos relatados en capítulos anteriores de este documento, a continuación se emitirán algunas consideraciones, las cuales conducen a la emisión de una recomendación general, con propósito de que la Administración o el Concejo, siga el correspondiente proceso de aprobación e implementación total de las medidas de control informático, para la atención plena de las recomendaciones del informe y consecuente subsanación de la totalidad de las vulnerabilidades determinadas.

Lo anterior, se formula con fundamento en lo dispuesto en el artículo 22, inciso d) de la Ley General de Control Interno, el cual indica textualmente: ***"Compete a la auditoría interna... Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento."***

Por lo expuesto anteriormente, esa Alcaldía debe tomar las acciones correspondientes, con respecto a los resultados obtenidos en el informe de Deloitte, relacionados con las vulnerabilidades, tanto internas como externas, a nivel de seguridad de la información y

las recomendaciones asociadas con cada una de ellas, de forma tal que:

El informe adjunto a este documento, sea remitido a la Unidad de Informática, con el fin de que las vulnerabilidades que tienen un estado de **no solucionadas** y las que presentan la condición de **justificadas**, sean atendidas, otorgando la solución respectiva a cada una de ellas.

De conformidad con lo descrito en este oficio, se le solicita informar a esta Auditoría Interna, **en un plazo de 30 días hábiles**, sobre los resultados de las acciones tomadas por esa Alcaldía y del traslado a la Encargada de la Unidad Informática, del citado informe de Seguridad Informática (Vulnerabilidades); lo cual conducirá a la implementación de las medidas de control interno, para la atención de las vulnerabilidades descritas.

Atentamente,

MARIBELLE SANCHO GARCÍA
AUDITORA INTERNA

CC: Concejo Municipal
Archivo