Auditoría Interna

Nuestra chamba: Encontrar Riesgos.

TRAFASA

INFORME DE AUDITORIA

Dirigido a:

Sr. Pedro Pablo Kuczynski

C.C.:

Sr. Fernando Zavala
Sr. Miguel Tupac Y.

Revisado y aprobado por:

El profesor del curso.

XIX.	TECNOLOGIA DE INFORMACION	RIESGO: **Alto** (17)
XIX.1.	**Insuficientes controles para el acceso a la información de Sistema de Ventas.**	

De la revisión a la seguridad lógica de servidores, el servidor de pruebas SRVBACKUP cuya funcionalidad es referido al "Sistema de ventas", se evidenció que la información de la Base de Datos (BD) del Sistema se encontraba en la siguiente ruta \\10.18.132.61\Backup\ sin permisos de seguridad asignados y de libre acceso a la red de usuarios TRAFASA.

Asimismo, se observó que dicha información estuvo como una copia de respaldo y que luego de las pruebas de restauración efectuadas, y se accedió a la BD del Sistema, visualizando la información contenida como credenciales de los clientes (usuarios y contraseñas), entre otros.

RIESGOS	(a)	Acceso irrestricto a información crítica de la Sistema usuarios y contraseñas de los Clientes.
	(b)	Pérdida de la seguridad y confidencialidad de la información.

RECOMENDACIONES	(a)	La Jefatura de TI, a través de la Coordinación de Servidores, deberá efectuar una revisión al 100% de los servidores con la finalidad de identificar ausencia de permisos en carpetas con información crítica para la compañía.
	(b)	La Jefatura de TI, a través de la Coordinación de Seguridad, deberá gestionar y establecer controles de seguridad lógica para el almacenamiento y acceso seguro a los archivos almacenados en los servidores.
	(c)	La Jefatura de TI deberá establecer un procedimiento que valide aquellas copias de respaldo que no se encuentran en la herramienta de backup y que es almacenada en servidores como SRVBACKUP.

XIX.	TECNOLOGIA DE INFORMACION	RIESGO: **Alto** (17)
XIX.2.	**Establecer mejores controles a la actividad de aseguramiento.**	

En setiembre 2016 se incorporó a la compañía el nuevo Coordinador de Servidores y como parte de las labores de aseguramiento se tiene como responsabilidad el monitoreo, configuración, aseguramiento de servidores y el cumplimiento de políticas de seguridad de información.

Tal es así que, al asumir dicha responsabilidad, el Coordinador de Servidores aplicó el "retiro de derechos de accesos" a aquellas cuentas con privilegios de administrador como buena práctica ante la presunción de que dichas cuentas carecían de confidencialidad y eran de conocimiento por varios colaboradores de la compañía.

En tal sentido, el Coordinador de Servidores ejecutó el cambio de credenciales (usuarios y contraseñas de cuentas con privilegio administrador); sin embargo, fue ejecutado sin determinar un procedimiento que determine su impacto, urgencia, prioridad o categoría.

Debido a esta situación se vio comprometida la disponibilidad de equipos de autenticación de usuarios a la red física e inalámbrica, perjudicando el acceso de usuarios a la red TRAFASA.

De otro lado en diciembre 2016 se incorporó también a la compañía el nuevo Coordinador de Redes y Comunicaciones; sin embargo, situación contraria descrita anteriormente, al cierre de nuestra visita el actual responsable sigue utilizando las mismas credenciales (usuarios y contraseñas de los equipos de comunicación que gestionaba su predecesor), lo cual podría permitir el acceso de usuarios no autorizados a la red de TRAFASA como Administrador de la red.

RIESGOS	(a)	Incremento del riesgo operativo por efectuar cambios críticos sin procedimientos establecidos que perjudiquen la continuidad operativa de usuarios de la red de TRAFASA
	(b)	Acceso no autorizado a la red de la compañía, debido a que las credenciales asociadas a los equipos de comunicación fueron de conocimiento del anterior Coordinador de Redes y Comunicaciones.

RECOMENDACIONES	(a)	La Jefatura de TI, a través del Coordinador de Servidores, deberán elaborar procedimientos que aseguren un control de cambios adecuado que contemple por lo menos: Documentos de petición de cambio, descripción del cambio y el objetivo, aceptación del cambio para determinar su impacto, urgencia, prioridad y categoría, pruebas en ambientes controlados luego en producción y en caso de tener interrupciones graves, contar con planes de back-out.
	(b)	La Jefatura de TI, a través del Coordinador de Redes y Comunicaciones, deberá gestionar el cambio de credenciales de los equipos de comunicación y aquellos dispositivos que fueron anteriormente gestionados por su predecesor.

XIX.	TECNOLOGIA DE INFORMACION	RIESGO: **Moderado** (9)
XIX.3.	**Implementar certificados digitales en aplicaciones web desarrolladas en TRAFASA.**	

De acuerdo a lo establecido en la Política Corporativa de aseguramiento de los sistemas de información PO-01, sobre los controles de protección en Internet se indica que: "*Todo Sistema de Información Web en Internet deberá contar con un certificado digital y conexión segura*."

Al respecto, se observó que existen 2 aplicaciones web en Internet desarrolladas localmente en TRAFASA (Sistema Georeferencial y Consulta de Saldos), que no cuentan con un certificado digital ni una conexión segura ("https:"), tal como lo requiere la Política Corporativa.

RIESGO	(a)	Posibilidad de que un tercero intercepte la información comercial de la Compañía y de los clientes a través de aplicaciones que se encuentran sin seguridad de conexión a internet.

RECOMEND.	(a)	Implementar certificados digitales y una conexión segura en las aplicaciones web mencionadas que se encuentran en Internet.

XIX.	TECNOLOGIA DE INFORMACION	RIESGO: **Moderado** (9)
XIX.4.	**Evaluar el cambio del sistema operativo (Windows 2003) y base de datos (Windows 2000) de aplicaciones relacionadas a la Sistema.**	

De la revisión realizada al inventario de servidores de TRAFASA, se observó que existen 14 servidores que cuentan con Windows 2003 Server (ver Anexo 1), debiendo indicar que dicho sistema operativo dejó de contar con el soporte de Microsoft desde julio de 2015, tal como se muestra en su página web:

El soporte técnico para Windows Server 2003 finalizó el 14 de julio de 2015

Microsoft finalizó el soporte técnico para Windows Server 2003 el 14 de julio de 2015. Este cambio ha afectado a las actualizaciones de software y las opciones de seguridad. Sepa qué significa esto en su caso y cómo puede mantenerse protegido.

Asimismo, se observó que existen 4 aplicaciones que utilizan como base de datos SQL Server 2000 (Ver Anexo 2), el cual dejó de contar con el soporte técnico de Microsoft desde abril 2013.

Cambios en el soporte técnico de SQL Server 2000

El 9/4/2013 finalizará el soporte extendido para SQL Server 2000 y ya no se ofrecerá soporte técnico para SQL Server 2000. Para obtener más información, vea la página Actualizaciones de soporte técnico de SQL Server. Lea más información acerca del final del soporte técnico para SQL Server 2000 Service Pack 3a y Service Pack 4.

RIESGO	(a)	Posibles brechas de seguridad en la plataforma tecnológica de TRAFASA, al mantener sistemas operativos y bases de datos que ya no cuentan con soporte ni actualizaciones de seguridad del proveedor.

RECOMEND.	(a)	Efectuar un plan de migración y actualización de sistemas operativos (Windows 2003 Server) y bases de datos (SQL Server 2000) que ya no cuentan con soporte técnico de Microsoft.

XIX.	TECNOLOGIA DE INFORMACION	RIESGO: **Moderado** (9)
XIX.5.	**Efectuar revisiones periódicas para garantizar que la información de los usuarios almacenada en sus equipos se encuentre debidamente respaldada.**	

De la revisión realizada a la información respaldada por la solución de respaldo, se observó que existen usuarios a los cuales no se viene realizando copias actualizadas de la información almacenada en sus equipos (laptops y desktops), como, por ejemplo:

Cuenta de usuario de red	Tamaño del backup realizado (en Kb)	Tipo de respaldo	Fecha de Creación / Modificación	Área	Cargo
MFIGUEROA	4	VIP	21/02/2015	Operaciones	Director de Operaciones Logísticas
ACACHAZA	2	VIP	13/09/2015	TI	Director de Infraestructura
PFIUZZA	21,304	VIP	11/02/2016	Ventas	Director de Vtas Estratégicas

De acuerdo a lo informado por la Jefatura de TI, existen algunos usuarios que mueven la ubicación de la carpeta de respaldo y algunos que no almacenan su información en dicha ruta, por lo cual la aplicación no realiza el respaldo programado.

RIESGO	(a)	Posible pérdida de información de la Compañía, almacenada en equipos de colaboradores, a los cuales no se les realiza un respaldo periódico y actualizado.

RECOMENDACIONES	(a)	Implementar procedimientos periódicos de monitoreo, sobre la información que se viene respaldando con la herramienta de respaldo, a fin de identificar usuarios que no cuentan con respaldos de su información o si ésta no se encuentra debidamente actualizada.
	(b)	En coordinación con el área de Recursos Humanos, elaborar una estrategia para concientizar a los colaboradores que no vienen respaldando su información local, y evaluar posibles sanciones para aquellos que no cumplan con respaldar su información.

XX.	DESARROLLO DE SISTEMAS	RIESGO: **Alto** (18)
XX.1.	**Existen desarrollos y mantenimientos realizados localmente que no cuentan con documentación técnica requerida.**	

De la revisión realizada a la documentación técnica, en una muestra de 9 desarrollos y mantenimientos ejecutados sobre las aplicaciones locales de TRAFASA, se observó que no se viene documentando de forma adecuada los cambios realizados, principalmente en información relacionada a Análisis Técnico, Análisis Funcional, casos de prueba de desarrollo y plan de pruebas de usuario.

Asimismo, se encontró que no se cuenta con documentación técnica actualizada.

RIESGOS	(a)	Dependencia funcional de los 2 responsables del mantenimiento y desarrollo de aplicaciones.
	(b)	Posibles retrasos en nuevos mantenimientos y desarrollos relacionados a la Sistema, debido a que no se cuenta con documentación actualizada.

RECOMENDACIONES	(a)	En coordinación con la Gerencia de Sistemas, definir e implementar la documentación mínima que se debe mantener para los desarrollos y mantenimientos locales en TRAFASA.
	(b)	Evaluar la viabilidad de documentar aquellas aplicaciones que no cuentan con documentación técnica mínima, en función a su relevancia y complejidad para el mantenimiento.

XX.	DESARROLLO DE SISTEMAS	RIESGO: **Alto** (17)
XX.2.	**Establecer controles que aseguren la continuidad operativa del Sistema de Distribución en tiempos aprobados por la Unidad de Negocio**	

El proceso de despacho de pedidos de clientes es soportado en un software desarrollado localmente, cuenta con dispositivos móviles que permiten la atención de un promedio de 5,000 órdenes diarias a despachar y además dicho software se encuentra alojado en el Centro de Datos local de TRAFASA.

Teniendo en cuenta que el proceso de despacho es importante para la atención de las ordenes de los clientes, el Sistema de Distribución presenta las siguientes situaciones:

- No cuenta con un plan de contingencia ante una posible indisponibilidad operativa en el cual se hayan validado los tiempos de recuperación considerando el volumen de información; si bien se tiene un plan de contingencia tecnológica ante un posible desastre, no se estimó operativamente las actividades a realizar par ano afectar la continuidad operativa. De otro lado, la actividad final del proceso de despacho (carga de pedidos) requiere la aprobación previa de las facturas electrónicas, sin embargo, durante las semanas de despacho, ésta actividad no puede ser culminada debido a que las autorizaciones de las facturas electrónicas del Sistema de Tributación no vienen siendo reflejadas. Esta situación implica que las guías electrónicas para el despacho de los pedidos, tenga que efectuarse de forma manual previa intervención y cambio de las configuraciones en producción del sistema por parte de personal de desarrollo de software.
- Finalmente, no se ha actualizado en una de las computadoras destinada a la gestión de despacho, la versión del sistema de distribución. Esta situación impide que los reportes de transporte, ingreso de informes de reparto y registro de 2dos envíos no puedan ser soportados por la versión antigua del Sistema de Distribución.

RIESGOS	(a)	Indisponibilidad del sistema y servicio de despacho que conllevaría a un retraso en el envío de los pedidos.
	(b)	Pérdida de información del proceso de despacho por indisponibilidad del Sistema de Distribución.

RECOMENDACIONES	(a)	La Dirección de Tecnología deberá efectuar un relevamiento de información a fin de recoger las necesidades de la Unidad de negocio respecto a los niveles de tolerancia en pérdida de información y tiempos de recuperación ante un posible desastre o contingencia del proceso de despacho, para luego efectuar un análisis de las brechas del sistema de Distribución a fin de actualizarlo con los requerimientos nuevos de la Unidad de Negocio y establecer una estrategia de recuperación.	
		Responsable	Fecha

XXI.	TECNOLOGÍA DE INFORMACIÓN - RECURSOS HUMANOS	RIESGO: **Alto** (18)

XXI.1. Deficiencias en la administración de seguridad del sistema de nómina permiten el acceso a datos confidenciales – Seguimiento al Informe AÑO 2016.

Durante las auditorías realizadas en setiembre 2014 y julio 2015, se identificaron vulnerabilidades en la configuración del servidor AS400, que permitían el acceso a datos confidenciales del sistema de nómina.

Al respecto, durante la auditoría realizada en marzo 2016, se observó que se implementaron cambios para restringir el acceso de algunos perfiles de usuarios y mejorar la seguridad en la configuración del servidor AS400. Sin embargo, aún existen vulnerabilidades en el servidor AS400, que permiten el acceso a toda la información de la Nómina de TRAFASA (sueldos, datos personales, etc.), tanto de lectura como de modificación.

Las vulnerabilidades identificadas son las siguientes:

a. Existen 2 cuentas de usuario con autorizaciones especiales (OPERADOR1 y OPERADOR2), con contraseñas fáciles de descifrar (contraseña “operador” y “operador1”). Si bien se implementó la política de contraseñas, ésta no fue asignada a todos los perfiles de usuarios creados, para exigirles complejidad en sus contraseñas.

b. Los accesos al spool de impresiones de los colaboradores del área de Recursos Humanos, no cuentan con restricciones que les impidan visualizar las impresiones de otros usuarios. Al respecto, realizamos una prueba con la cuenta de usuario de la Asistenta Social de la Planta y se logró acceder al spool de impresiones de la Coordinadora de Compensaciones, pudiendo visualizar información de sueldos de todo el personal, en impresiones de cheques y roles (boletas de pago).

c. Todos los usuarios del área de Recursos Humanos cuentan con acceso habilitado para la ejecución de consultas a toda la base de datos del sistema de nómina.

RIESGOS	(a)	Posibles accesos no autorizados al sistema de Nómina y Recursos Humanos, por vulnerabilidades en la configuración de los parámetros de seguridad del servidor AS400.
	(b)	Posible pérdida de confidencialidad e integridad de la información registrada en el sistema de Nómina y Recursos Humanos, permitiendo visualizar, modificar y eliminar pagos, sueldos, bonificaciones cuentas bancarias, etc. de todo el personal de TRAFASA.

RECOMENDACIONES	(a)	Efectuar el cambio en la configuración de los usuarios OPERADOR1 y OPERADOR2, así como el cambio de sus contraseñas.
	(b)	Revisar y modificar la configuración del spool de impresiones de colaboradores del área de Recursos Humanos, de tal forma que cada usuario pueda visualizar solo sus impresiones en el servidor AS400.
	(c)	En coordinación con el área de Recursos Humanos, definir qué usuarios contarán con acceso a la opción de consultas a la base de datos del sistema de Nómina, y restringir dicho acceso a usuarios no autorizados.