Ejemplos de Observaciones de Auditoria de Infraestructura Tecnológica

1. **Algunas PCs del parque informático de la Entidad cuentan con el Sistema Operativo Windows XP que ya no cuenta con soporte del fabricante.**

   De la revisión al parque informático de la Entidad, se encontró que existen equipos informáticos que cuentan con el sistema operativo Windows XP. Dicho sistema operativo ya no es soportado por Microsoft desde el 08 de abril del 2014, lo cual significa que los equipos que aún cuentan con dicho sistema operativo se encuentran vulnerables, ya que el fabricante ya no emite parches de seguridad. La información completa del fin del soporte para el sistema operativo Windows XP se encuentra disponible en el sitio web oficial de Microsoft, en el link. http://windows.microsoft.com/en-us/windows/products/lifecycle#section_2

   Esta situación expone a los equipos con dicho sistema operativo ya que no reciben actualizaciones de software ni parches de seguridad, lo que convierte a dichos equipos en altamente vulnerables a las amenazas informáticas tales como virus, gusanos, troyanos, spyware, rootkits, etc, lo que a su vez, podría originar falta de disponibilidad en dichos equipos y comprometer a los demás equipos conectados a la red.

   Se recomienda que el Rectorado disponga que la Jefatura de Tecnología de Información y Comunicaciones evalúe y planifique la renovación tecnológica de los equipos vulnerables o en su defecto se programe la migración del sistema operativo Windows XP instalado en los equipos de la Entidad a una versión más reciente y que cuente con el soporte de parches y actualizaciones vigentes.

2. **El parque tecnológico de la Entidad no se encuentra adecuadamente parchado.**

   De la revisión al proceso de actualización de parches, se pudo evidenciar que los equipos informáticos PCs y laptops basados en el sistema Operativo Windows, no se encuentran correctamente actualizados.

   Esta situación podría originar que los equipos informáticos se encuentren permanentemente en riesgo, lo que convierte a dichos equipos en altamente vulnerables a las amenazas informáticas tales como virus, gusanos, troyanos, spyware, rootkits, etc, lo que a su vez, podría originar falta de disponibilidad en dichos equipos y comprometer a los demás equipos conectados a la red.

   Se recomienda que la Jefatura de Oficina de Tecnologia de Información y Comunicaciones priorice la implementación de un procedimiento de actualización periódico y que se utilice alguna herramienta centralizada de distribución de parches tal como WSUS o similar.

3. **No se cuenta con controles para los usuarios de la red.**

   De la revisión a los controles de seguridad de los usuarios en la red, se encontró que la Oficina de Tecnologías de Información y Comunicaciones no cuenta con un servicio de dominio de red que permita centralizar las tareas administrativas y de seguridad de los accesos de los usuarios en la red. Dada la falta de un dominio de red, los usuarios ingresan a sus equipos con una cuenta de usuario local, la cual no cuenta con ninguna configuración de seguridad para los usuarios.

Esta situación origina que los usuarios puedan contar con contraseñas débiles, no se les obligue a cambiar la contraseña, entre otros, lo cual podría originar un riesgo a la protección de la información manejada por los usuarios.
Se recomienda que el Rectorado disponga que la Jefatura de la oficina de tecnologías de Información y Comunicaciones incluya en su plan operativo, la implementación de un dominio centralizado de red, de tal manera que se implementen controles mínimos para los usuarios, tales como:

- Obligación de cambio de contraseña en periodos determinados, como por ejemplo cada 120 días.
- Obligación de robustez de contraseña. Por ejm mínimo 8 posiciones y exigencia de al menos una mayúscula, minúscula y números.
- Bloqueo del usuario si es que la contraseña no es correcta por más de un número definido de intentos fallidos consecutivos.
- Obligación de no repetir las 6 últimas contraseñas.
- Auditoria de accesos válidos y fallidos.

Asimismo, se recomienda que la Oficina de Tecnologías de Información y Comunicaciones realice un programa de seguridad basado en charlas de concientización para comunicar a los usuarios las recomendaciones y trucos para generar y recordar contraseñas robustas.

4. **<u>En enlace de la red de datos de la Sede del rectorado no cuenta con suficiente capacidad para soportar la carga actual de conexiones actuales de los usuarios.</u>**

   De la revisión a la infraestructura de la red de datos del Universidad, se identificó que la red de datos de la sede del Rectorado de la Universidad se encuentra comunicada con el Campus Universitario a través de un radio-enlace de 10MB. Este ancho de banda es insuficiente para atender las necesidades del personal que labora en las instalaciones del Rectorado

   Esta situación afecta la performance y desempeño de la red, ocasionando lentitud en el procesamiento de los diversos sistemas y servicios informáticos.

   Se recomienda que el Rectorado disponga que la Jefatura de la Oficina de Tecnologías de Información y Comunicaciones efectúe una evaluación integral de los niveles de utilización y performance de la red de datos, y en función a dichos resultados se disponga la mejora o actualización de los componentes de la infraestructura de red que corresponda.

Ejemplos de Observaciones de Auditoria de Gestión de Tecnología de Información

5. **<u>La Oficina de Tecnologías de Información y Comunicaciones (OTIC) no se encuentra adecuadamente ubicada en la estructura organizacional de la Universidad.</u>**

   De la revisión a la estructura organizacional del área de Tecnologías de Información y Comunicaciones se encontró que dicha Oficina se encuentra jerárquicamente ubicada dentro de la estructura de la Oficina Central de Información y Comunicación. Esta situación se debe a que la Oficina de Tecnología de Información y Comunicaciones inicio sus actividades dentro de la

Oficina Central de Información y Comunicación, la cual no es un área idónea para gestionar los temas tecnológicos con un alcance para toda la Universidad.

La dependencia del área de Tecnología de Información a la Oficina de Administración podría originar que las iniciativas tecnológicas no cuenten con el suficiente respaldo para beneficiar el uso de la tecnología en toda la Universidad. Asimismo, esta situación origina que los esfuerzos del área se concentren en proyectos locales y/o puntuales, pudiendo afectar la atención de soluciones tecnológicas a las otras áreas de la Universidad.

Se recomienda que el Rectorado disponga que la Oficina Central de Personal evalúe la conveniencia de que la Oficina de Tecnologías de Información y Comunicaciones reporte a una instancia superior que permita tomar las decisiones de implementación de tecnología de información, en beneficio de toda la Universidad.

6. **La Oficina de Tecnologías de Información y Comunicaciones no cuenta con indicadores de Gestión.**

   De la revisión a los indicadores de Gestión de la Oficina de Tecnología de Información y Comunicaciones, se encontró que el área no cuenta con indicadores de gestión internos que permitan medir el impacto beneficioso de las tecnologías de Información en la Universidad.

   Esta situación origina que el área de Tecnología de Información no pueda medir su efectividad ni contribuir eficientemente a los objetivos de la Entidad.

   Se recomienda que la Oficina de Tecnologías de Información defina indicadores de gestión que permitan medir adecuadamente la gestión del área y su contribución a los objetivos estratégicos de la Entidad. Entre los indicadores recomendados se podrían considerar:
   - Nivel de satisfacción de los usuarios con el servicio informático
   - Nivel de disponibilidad de la infraestructura tecnológica
   - Nivel de integración de los proyectos de Informática a los objetivos estratégicos de la Entidad
   - Nivel de cumplimiento de los proyectos en el Plan anual de Informática.

   Asimismo, se recomienda que estos indicadores estén incluidos dentro del Plan Estratégico de Tecnologías de Información y Comunicaciones.

Ejemplos de Observaciones de Auditoria de Sistemas Informáticos

7. **El Sistema de información de SIGA requiere mejoras en sus mecanismos de Seguridad.**

   Durante la revisión al Sistema Integrado de Gestión Administrativa SIGA, se encontraron debilidades de control tales como:
   - El sistema no exige la definición de contraseñas robustas
   - El sistema exige una longitud muy corta de contraseñas
   - El sistema no obliga a cambiar la contraseña
   - La contraseña puede ser igual al nombre del usuario
   - La cuenta de accesos no se bloquea al tercer intento fallido de acceso
   - No es posible definir una fecha de vencimiento de las cuentas.

Esta situación podría originar el riesgo de ataques externos e incluso podría generar accesos no autorizados al Sistema SIGA.

Se recomienda que la Jefatura de la Oficina de Tecnologías de Información y Comunicaciones, priorice la implementación de las mejoras a los controles de acceso que permitan mitigar las vulnerabilidades encontradas. Asimismo se debe evaluar la factibilidad de que la contraseña de los usuarios del Sistema se integre al Directorio Activo (cuando este disponible) de la Universidad, lo cual beneficiara a los usuarios ya que no tendrán que recordar una contraseña adicional.

8. <u>Algunas páginas web de la Universidad requieren implementación de controles de protección.</u>

De la revisión a las páginas web que gestionan la información Académica de la Entidad, se encontró que la navegación por parte de los usuarios a dichas páginas no cuenta con una adecuada protección. Así tenemos que todo el tráfico de datos intercambiado entre los alumnos y docentes que acceden dichas páginas y los servidores web de la Universidad se encuentra en estado vulnerable a diversos ataques informáticos. Las páginas involucradas que se encuentran desprotegidas son:

- Intranet Alumnos
- Intranet Docentes

Esta situación podría originar una interceptación o pérdida de la información procesada por las páginas web indicadas. Asimismo, debido a la falta de protección referida, un atacante podría registrar información errada en dichas páginas web.

Se recomienda que el Rectorado disponga que la Jefatura de la Oficina de Tecnología de Información y Comunicaciones, evalúe la implementación de certificados digitales de al menos 2048 bits en los servidores Web de la Universidad; e implemente el protocolo TLS para la transmisión de datos, lo que permitirá conexiones seguras y confiables entre el público usuario que accede a las páginas web indicadas y los servidores web de la Universidad.
Asimismo, se recomienda que se evalúe la posibilidad de definir la contratación periódica (al menos una vez al año) de servicios externos de análisis de vulnerabilidades que incluya la revisión de la infraestructura y aplicaciones disponibles en todas las páginas web de la Universidad ya que dado el entorno cambiante de la tecnología, todos los días aparecen las vulnerabilidades y riesgos de ataques que podrían comprometer la información gestionada en Internet por la Universidad.

9. **<u>Existen adquisiciones y sistemas de Información que no son coordinados con la Oficina de Tecnología de Información y Comunicaciones.</u>**

   De la revisión a las adquisiciones tecnológicas de la Entidad, se evidenció que existen adquisiciones que no son coordinados con la Oficina de Tecnología de Información y Comunicaciones. Asimismo existen Sistemas de Información que no han sido coordinados con la referida Oficina.

   Esta situación origina que la tecnología existente y los sistemas no cuenten con una uniformidad tecnológica. Asimismo origina que no se implementen controles para mejorar el control de la tecnología y los diversos sistemas de información.
   Se recomienda que el Rectorado disponga que todas las áreas de la Universidad s tengan la obligación de coordinar con la Oficina de Tecnología de Información y Comunicaciones, en lo relacionado a adquisiciones tecnológicas y a la implementación de Sistemas de Información.

Ejemplos de Observaciones de Auditoria de Cumplimiento de Leyes y Regulaciones

10. **<u>La Entidad aún no ha implementado controles para cumplir con la ley de Protección de datos personales.</u>**

    A la fecha de nuestra revisión, la Oficina de Tecnología de Información y Comunicaciones aún no tenía planificada la incorporación de controles para cumplir con la Ley 29733 de protección de datos en los procesos internos que tratan información personal y sensible.
    La Ley 29733 de Protección de datos personales promulgada el 03 de junio del 2011 y reglamentada mediante Decreto Supremo Nº 003-2013-JUS del 22 de marzo del 2013, desarrollan y garantizan el derecho fundamental a la protección de los datos personales, previsto en el numeral 6 del artículo 2° de la Constitución Política del Perú, según el cual toda persona tiene derecho "*a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*". En ese contexto, dentro de las disposiciones establecidas en la referida ley, se encuentra la obligación de cumplir con controles tecnológicos para asegurar los bancos de datos que contienen datos personales.

    Esta situación podría exponer a la Universidad a multas y sanciones de parte de la autoridad correspondiente.

    Se recomienda que el Rectorado priorice la conformación de un Comité de Alto Nivel para la planificación e implementación de los controles a nivel de los procesos, recursos humanos y Tecnología de Información para cumplir con la referida Ley. En ese contexto, la oficina central de Asesoría Legal debe tener una participación activa para guiar a las diversas áreas en dicho cumplimiento.

Ejemplos de Observaciones de Auditoria de Accesos

1. **Se identificaron cuentas de personal cesado que permanecen activas en el Sistema ERP SAP.**
   Durante la revisión identificamos cuentas de usuarios de personal cesado, según el reporte de cese emitido por Recursos Humanos, que permanecen activos en el sistema SAP, tales como:

Código empleado	Descripción	Unidad organigrama	Fecha de Cese	Módulo SAP
795835	Bochelli, Andrea	LOGISTICA	09/01/2009	Order Management
795842	Boyle, Susan	LOGISTICA	09/01/2009	Order Management
795455	Riu, Andre	CONTABILIDAD	31/03/2009	General Ledger

Esta situación incrementa el riesgo de accesos no autorizados al sistema, mediante el uso de cuentas de personal cesado que se mantienen activas, después de su fecha de cese. El impacto asociado al riesgo identificado, dependerá de los permisos relacionados a los accesos asignados a cada una de las cuentas.

Se recomienda realizar un seguimiento sobre la desactivación de dichas cuentas de usuarios en el Sistema SAP y realizar un monitoreo continuo sobre las cuentas de usuario de personal cesado.

Ejemplos de Observaciones de Bases de Datos

1. No se registran los eventos de auditoría de la base de datos Oracle del sistema de Planillas ADRYAN

Durante nuestra revisión, verificamos que la base de datos que almacena la información del Sistema ADRYAN tiene la opción de registro de auditoría "audit_trail" en true, sin embargo, se observa las siguientes situaciones:

- No se encuentran definidos los valores a ser auditados para todas las cuentas de usuarios
- No se encuentra definido el registro de operaciones sensibles en los objetos de la base de datos, como DROP TABLE, CREATE TABLE, SELECT TABLE, entre otros.
- No registra los intentos de inicio de sesión exitosos y fallidos en la tabla DBA_AUDIT_SESSIONS.

Esta situación implica el riesgo de no poder identificar actividades no autorizadas realizadas en la base de datos.

Se recomienda evaluar la habilitación de los parámetros de auditoría o activaciones de comandos que permitan el registro de actividades relacionadas con accesos, eliminaciones, modificaciones a las tablas principales que se realizan a la base de datos del Sistema ADRYAN.

2. Existen 7 personas de la compañía de Outrsourcing con privilegios de administrador para las bases de datos del SAP, GAD y ADRYAN.

Durante la revisión de las bases de datos del SAP, GAD y Adryan, se identificó que existen 7 operadores de GMD con privilegios de administrador (DBA), los cuales son:

1. Leonel Messi
2. Diego Maradona
3. Juan Veron

4. Carlos Alvarez
5. Jorge Benvides
6. Magaly Medina
7. Miguel Barraza

Esta situación implica un alto riesgo de modificación no autorizada de información para las bases de datos del SAP, GAD y ADRYAN; así como la falta de identificación de las actividades realizadas por cada operador, por el uso compartido de las cuentas de acceso para la administración de la base de datos.

Se recomienda evaluar la definición de cuentas diferentes para cada operador del Outsourcing y definir a los operadores que deben de contar con el perfil administrador, a fin de delimitar el acceso y puedan cumplir con las funciones establecidas de DBA.

Ejemplos de Observaciones de Proyectos

2. Se carece de una adecuada gestión de comunicación sobre las actividades realizadas en el proyecto de automatización de captura de información, así como de la documentación utilizada en el proyecto.

Durante nuestra revisión, se observaron las siguientes situaciones sobre la gestión del proyectos de automatización de captura de información:

- No se evidenciaron las actas de reunión que sustenten la comunicación de las actividades realizadas en el proyecto, ya que tan sólo se evidenciaron las actas de reunión hasta el mes de Abril 2009, habiendo culminado el proyecto en Febrero 2010.
- Se observó el uso de dos formatos diferentes de actas de reunión, no siguiendo lo estandarizado por la metodología de proyectos de LA COMPAÑIA, que figura en los anexos del documento.

Esta situación implica el riesgo de no evidenciar los acuerdos y decisiones relevantes que afecten la ejecución del proyecto. Asimismo, la falta de estandarización de documentos implica la falta de monitoreo sobre el uso apropiado de los formatos definidos por la metodología de proyectos de LA COMPAÑIA.

Se recomienda establecer en cada proyecto una frecuencia fija para llevar a cabo las reuniones de coordinación, registro y comunicación de las actas correspondientes. Así como también, establecer el control sobre la documentación elaborada para los proyectos de LA COMPAÑIA, a fin de cumplir con la "Metodología de Gestión de Proyectos" definida por la compañía.

3. Se identificó que los parámetros de contraseña del sistema operativo Windows 2000 del servidor de base de datos del Sistema ADRYAN, no se encuentran alineados con las políticas de contraseñas establecidas por la compañía.

Durante nuestra revisión, se observó que los valores de los parámetros de contraseña, configurados en el servidor de la base de datos del ADRYAN no se encuentran alineados a lo definido en la "Norma sobre definición de contraseñas" de la compañía.

Parámetro	Norma	Configuración Servidor
Intentos fallidos	>=3	>5
Historial de la contraseña	5	10
Máximo tiempo de antigüedad	**60**	**30**

La falta de configuración de los dos primeros parámetros de la tabla según la norma, implica el riesgo de accesos no autorizados por la vulnerabilidad de las contraseñas o mediante el uso de contraseñas más factibles de identificar por la reutilización de las mismas.

Se recomienda alinear los parámetros configurados en el servidor del ADRYAN hacia lo definido en las políticas de seguridad de la empresa. Respecto al parámetro de "máximo tiempo de antigüedad" de contraseña, tiene como valor asignado en el servidor 30 días; mientras que la política indica 60 días. A pesar que la regla en el servidor es más fuerte; se recomienda evaluar si dicha configuración está acorde a las necesidades de la compañía.

4. La cuenta "administrador" del sistema operativo Windows 2000 del aplicativo ADRYAN, no ha sido renombrada.

Durante nuestra revisión validamos que la cuenta con privilegios de administración del sistema operativo Windows ("Administrator") no ha sido renombrada. Esta cuenta administra todos los recursos y configuraciones del sistema operativo del servidor que soporta el sistema de Planillas.

Esta situación incrementa el riesgo de realizar intentos de accesos utilizando la cuenta de "administrador" por personal no acreditado, lo que podría llevar a realizar cambios no autorizados.

Se recomienda adicionar en la "Norma sobre definición de contraseñas" una sección que incluya el procedimiento de cambios de contraseña para las cuentas con privilegios de administración que considere:

- Periodicidad del cambio de contraseña
- Responsable de ejecutar el cambio.
- Complejidad de contraseña
- Método de cambio (manual o automático).

5. No se han activado logs de auditoría en el Sistema SAP.

Durante la revisión de configuración de logs de auditoría, se identificó que no se han activado logs de auditoría para la aplicación SAP.

Esta situación incrementa el riesgo de no detectar cambios críticos en la configuración o a nivel transaccional del sistema.

Se recomienda evaluar la implementación de logs de auditoría tales como el reporte "Signon Audit Forms" y realizar revisiones periódicas sobre los resultados de éstos, con el objetivo de identificar situaciones irregulares.

6. Se carece de una política de administración de contraseñas que aplique para el ERP SAP.

Durante la revisión de configuración de contraseñas se identificó que no se ha establecido la activación de los siguientes parámetros de contraseñas.

- Historial de contraseñas.
- Complejidad de contraseñas.
- Máximo número de intentos fallidos.

La situación mencionada, incrementa el riesgo de vulnerabilidad de las cuentas de usuario del SAP, ya que la falta de lineamientos de seguridad sobre las contraseñas podría ocasionar el uso de contraseñas que no sean lo suficientemente robustas y en consecuencia podría existir una mayor probabilidad que personal no autorizado pueda acceder a dichas cuentas.

Se recomienda añadir una sección en las políticas de contraseñas de usuarios, donde se definan los parámetros de contraseñas específicos para cuentas del sistema SAP y para las aplicaciones en general.

7. No se ha configurado la opción de "Sequential Numbering" en el Sistema SAP.

Durante la revisión de las configuraciones del SAP se verificó que la opción "Sequential Numbering", la cual está referida a la secuencia numérica que deben tener todos los documentos que se ingresan en el SAP, se ha configurado con el valor "Parcialmente usado".

La situación mencionada incrementa el riesgo de omitir las reglas de correlatividad y registrar documentos duplicados, lo cual conllevaría a una inadecuada administración de los mismos y posibles registros erróneos de información en las áreas comerciales o financieras.

Se recomienda evaluar la configuración del campo "Sequential Numbering" de acuerdo a las necesidades que se presenten en el flujo del negocio para los procesos administrativos, comerciales y financieros.