Práctico Unidad 7 – Control de la Gestión de Tecnologías de Información

Objetivos: que el alumno pueda:

- Identificar factores de riesgo de control interno en un ambiente informático
- Conocer las técnicas de revisión de auditoria asociadas a los riesgos y a la particularidad de cada proceso o Áreas de actividad de ASI

Tarea previa:

Lectura del material teórico distribuido por la cátedra sobre el tema y asistir a las clases teóricas

Areas de Actividad posible:

Auditoría de SI
Auditoría del Plan Estratégico de Sistemas
Auditoría del Desarrollo o Adquisición
Auditoría de Explotación y Mantenimiento
Auditoría de la Seguridad

Teniendo en cuenta las pautas de la estructura anterior, detecte los problemas en los textos y elabore un informe de auditoría que cumpla con el esquema planteado en teoría.

La empresa Servitodo contrató nuestros servicios de una auditoría integral de sistemas. Comenzamos por auditar el Plan Estratégico y relevamos que la empresa tiene tres responsables y el dueño (D) en su nivel directivo. Un responsable de Ventas y Compras (RV), un responsable de Facturación y Cuentas Corrientes (RF) y un responsable Administrativo Financiero (DA) (RA) a cargo de todas las decisiones de sistemas informáticos y fija los límites de los clientes en cuenta corriente.

Auditoría del Plan Estratégico de Sistemas

I) Los responsables tienen reuniones individuales con el dueño y se comunican entre ellos en la gestión diaria del negocio. D tiene previsto abrir dos sucursales una en otra provincia y una en el interior. El hardware y software y licencias que están contratando y comprando son una renovación de las PC actuales por tecnología más moderna

II) El RV tenía previsto y conversado con D una ampliación de los servicios a vender y hasta preveían desarrollar un producto propio para los cual necesitarían almacenar productos y como el local no era suficiente deberían contratar un anexo para la gestión del stock y producción. Nadie más en la empresa conocía este plan.

Auditoría del Desarrollo o Adquisición

III) EL RA no tenía un Plan de reemplazo, no encontramos ningún análisis de tiempos o costos del proyecto. Había una carpeta con folletos de productos de Hardware, otra con folletos de sistemas de gestión comercial y otra con folletos productos de oficina. Solo el RA conocía que y a quien había comprado, tiempos de entregas e impactos sobre la gestión, implementación y capacitación.

IV) RV tiene pensado cambiar los remitos de los trabajos efectuados de manual a un sistema de ingreso de tiempos en unidades móviles de registro. Lo conversó solo como idea alguna vez con FA.

Auditoría de Explotación y Mantenimiento

V) La empresa Servitodo , recibe en CD los detalles de las cobranzas efectuadas en una boca externa (contratada con pagodificil). La empleada descarga el archivo en su PC, lo abre, le efectúa los cambios necesarios para adecuar el archivo y procesa una aplicación que los importa al sistema de cuentas a cobrar y caja, se registra la cobranza, el ingreso o depósito de los fondos y se dan de baja las cuentas a cobrar.

VI) Las facturas de venta de la empresa Servitodo se efectúan en forma bach en base a remitos de los servicios prestados que los entregan numerados y con el precio fijado en cada caso. El empleado de facturación procede a realizar las facturas, las imprime en formularios prenumerados, las facturas emitidas las entregan para distribución y los remitos se archivan.

VII) La facturación del caso VI es transferida en un único archivo con valores sumarizados por cuenta contable al sistema contable una vez al mes. El empleado exporta del sistema de facturación, se graba una archivo de texto y desde el sistema contable captura ese archivo y genera el asiento de facturación mensual.

VIII) Al local lo abre el D todos los días, no hay separación de puertas cerradas entre los ambientes, empleados, responsables y D circulan por todo el local. El RA o RF habilitan el sistema y las PC. Se mantienen habilitadas por todo el día una por función (facturación y cobranza y administración) más la de los responsables.

IX)El RF habilita una vez al día con su clave la PC y la aplicación para el manejo de cuentas corrientes: facturación, notas de débito, notas de crédito y cobranzas, durante el día los encargados facturan, hacen las NC o ND gestionan las cobranzas y el encargado emite los informes y cierra los procesos de Cuentas Corrientes.

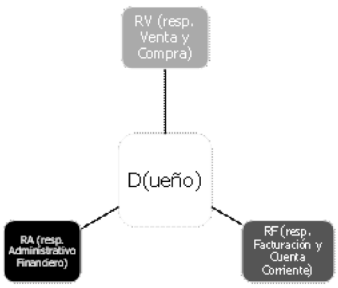
Auditoría de la Seguridad

X) No firman contratos por mantenimiento de hardware. Los suministros se compran en función de las necesidades, dice el RA que es más económico así usan lo necesario. Hay matafuegos cuya vigencia está operativa, no se observa cableado independiente de las Pc ni fichas térmicas independientes.

XI) Solo una vez se les quemaron dos PC con una tormenta eléctrica. Los archivos no se dañaron . No se hacen copias de seguridad. Si se corta la luz esperan a que regrese para facturar u operar con las PC. Hay un programador que viene a reparar los programas actuales, nadie sabe lo que hace pero corrige e indica que ya está listo y se va, siempre con su maletín a cuestas y ahora con su pen-driver.

RESOLUCION SUGERIDA

1. Problemas detectados



DA (RA) también está a cargo de todas las decisiones de sistemas informáticos y fija los límites de los clientes en cuenta corriente.

Se identifican 5 equipos PC.

Auditoría de SI	Problema detectado
a del Plan Estratégico de Sistemas	
esponsables tienen reuniones individuales dueño y se comunican entre ellos en la liaria del negocio. D tiene previsto abrir dos es una en otra provincia y una en el El hardware y software y licencias que contratando y comprando son una ón de las PC actuales por tecnología más	• **A nivel de gestión estratégica la comunicación es lineal dueño-responsables.**
/ tenía previsto y conversado con D una ón de los servicios a vender y hasta desarrollar un producto propio para los esitarían almacenar productos y como el era suficiente deberían contratar un anexo gestión del stock y producción. Nadie más presa conocía este plan.	• **Comunicación insuficiente entre responsables de Servitodo.** • **Alineación insuficiente negocio-sistema informatico.**
a del Desarrollo o Adquisición	
RA no tenía un Plan de reemplazo, no mos ningún análisis de tiempos o costos ecto. Había una carpeta con folletos de s de Hardware, otra con folletos de de gestión comercial y otra con folletos de oficina. Solo el RA conocía que, y a abía comprado, tiempos de entregas e sobre la gestión, implementación y ción.	• **Ausencia de continuidad del negocio respecto a personal.** • **Ausencia de análisis de riesgos, evaluación de proyecto.** • **Ausencia de proceso de adquisición.** • **Ausencia de gestión de proveedores.**
iene pensado cambiar los remitos de los efectuados de manual a un sistema de de tiempos en unidades móviles de Lo conversó solo como idea alguna vez	• **Ausencia de administración de proyecto de TI.** • **Ausencia de análisis de riesgo de TI del sistema de ingresos de tiempos.**
a de Explotación y Mantenimiento	
presa Servitodo , recibe en CD los detalles obranzas efectuadas en una boca externa da con pagodificil). La empleada descarga o en su PC, lo abre, le efectúa los cambios os para adecuar el archivo y procesa una n que los importa al sistema de cuentas a caja, se registra la cobranza, el ingreso o de los fondos y se dan de baja las cuentas	• **Ausencia de medidas de seguridad en el tratamiento de datos de cobranza.** • **Ausencia de segregación funcional.** • **Ausencia de asignación de atributos sobre transacciones.**
acturas de venta de la empresa Servitodo ian en forma bach en base a remitos de los prestados que los entregan numerados y ecio fijado en cada caso. El empleado de ón procede a realizar las facturas, las en formularios prenumerados, las facturas las entregan para distribución y los remitos an.	• **Ausencia de segregación funcional.** • **Ausencia de asignación de atributos sobre transacciones.**
acturación del caso VI es transferida en un chivo con valores sumarizados por cuenta al sistema contable una vez al mes. El o exporta del sistema de facturación, se n archivo de texto y desde el sistema captura ese archivo y genera el asiento de ón mensual.	• **Ausencia de segregación funcional.** • **Ausencia de niveles de supervisión.**

Auditoría de SI	Problema detectado
ocal lo abre el D todos los días, no hay ón de puertas cerradas entre los es, empleados, responsables y D circulan el local. El RA o RF habilitan el sistema y Se mantienen habilitadas por todo el día r función (facturación y cobranza y ración) más la de los responsables.	• **Ausencia de medidas de seguridad en sistemas y PC.**
F habilita una vez al día con su clave la PC olicación para el manejo de cuentas s: facturación, notas de débito, notas de cobranzas, durante el día los encargados hacen las NC o ND gestionan las as y el encargado emite los informes y s procesos de Cuentas Corrientes.	• **Ausencia de segregación funcional.** • **Ausencia de asignación de atributos sobre transacciones.** • **Ausencia de niveles de supervisión.**
a de la Seguridad	
firman contratos por mantenimiento de e. Los suministros se compran en función ecesidades, dice el FA (RA) que es más co así usan lo necesario. Hay matafuegos gencia está operativa, no se observa independiente de las Pc ni fichas térmicas lientes.	• **Ausencia de gestión de proveedores.** • **Ausencia de programa de mantenimiento de PC.** • **Ausencia de medidas de seguridad en redes y comunicaciones.**
una vez se les quemaron dos PC con una eléctrica. Los archivos no se dañaron . No n copias de seguridad. Si se corta la luz a que regrese para facturar u operar con Hay un programador que viene a reparar ramas actuales, nadie sabe lo que hace rige e indica que ya está listo y se va, con su maletín a cuestas y ahora con su er.	• **Ausencia de medidas de seguridad en PC y suministro eléctrico.** • **Ausencia de medidas de seguridad en base de datos.** • **Ausencia de gestión de proveedores.**

2. Informe de auditoría según esquema planteado en teoría:

Introducción	Se indica: **Objetivo, Alcance y Posición** de la auditoría frente al objeto auditado
Resultados	Se indica: **Evidencias y hallazgos claves** obtenidos durante la revisión, que sean significativos y que sirvan de base para las conclusiones
Conclusiones	Se expone: el **diagnóstico** en función de los resultados obtenidos. Ordenar: problema y causalidad (causa-efecto) Incluir **siempre** opinión del personal auditado.
Recomenda-ciones	Cursos de acción que se estimen pertinentes. Importante: **participación** del personal auditado
Anexos	Incluir: **El detalle** que respalda los hallazgos y explica el método empleado.

INFORME DE AUDITORIA

i) Introducción

(1) Objetivo:

Efectuar una auditoría integral del Sistema Informático de la Empresa Servitodo

(2) Alcance:

Las tareas de auditoría vinculadas al Sistema Informático integral se efectuaron en la empresa desde 04/2020 a 05/2020

(3) Posición:

Frente al objeto auditado se trata de una auditoría externa independiente

ii) Resultados

(1) Evidencias y hallazgos claves

Auditoría del Plan Estratégico de Sistemas

1. A nivel de gestión estratégica solo existe comunicación lineal dueño-responsables.
2. Comunicación insuficiente entre responsables de Servitodo.
3. Alineación insuficiente negocio-sistema informático (No hay integración de la Estrategia general de la empresa, ni la de los diferentes sectores con el Plan de Sistemas de Información)

Auditoría del Desarrollo o Adquisición

1. Comunicación insuficiente entre responsables de Servitodo.
2. Ausencia de análisis de riesgos, evaluación de proyecto.
3. Ausencia de proceso de adquisición.
4. Ausencia de gestión de proveedores.
5. Ausencia de administración de proyecto de TI.
6. Ausencia de análisis de riesgo de TI del sistema de ingresos de tiempos.

Auditoría de Explotación y Mantenimiento

1. Ausencia de medidas de seguridad en el tratamiento de datos de cobranza (archivos de importación editables, falta de totales de control, control de integridad).
2. Ausencia de segregación funcional.
3. Ausencia de asignación de atributos sobre transacciones.
4. Ausencia de medidas de seguridad en el tratamiento de datos de facturación (falta de totales de control, control de integridad).
5. Ausencia de medidas de seguridad en el tratamiento de datos de cobranza (falta de totales de control, control de integridad).
6. Ausencia de niveles de supervisión.
7. Ausencia de medidas de seguridad en sistemas y PC (1. password son conocidas por dos responsables simultáneos. 2. Se habilitan las PC por todo el día con perfiles únicos para todos los usuarios)

Auditoría de la Seguridad

1. Ausencia de gestión de proveedores.
2. Ausencia de programa de mantenimiento de PC.
3. Ausencia de medidas de seguridad en redes y comunicaciones.
4. Ausencia de medidas de seguridad en PC y suministro eléctrico (no hay planes formales de administración y resguardo de suministros).
5. Ausencia de medidas de seguridad en base de datos (no hay plan formal de back up).

6. Ausencia de Plan de Contingencia y Plan de Continuidad del Negocio

i) Conclusiones

Como resultado de la auditoria integral del sistema informático de la empresa Servitodo podemos manifestar que se ha cumplido con el objetivo.
De las evidencias y hallazgos claves identificados se observan ausencia de planificación integrada e integral, ausencia de medidas de seguridad significativas, las cuales representan oportunidades de mejora que facilitarían la eficiencia, efectividad, disponibilidad, confidencialidad, integridad, confiabilidad del sistema de información.

ii) Recomendaciones

Auditoría del Plan Estratégico de Sistemas

(1) Se deben establecer estrategias generales y que sean conocidas por el personal responsable de los Planes de SI

Auditoría del Desarrollo o Adquisición

(2) Se deben establecer formalmente normas y procedimientos apropiados de autorización a usuarios para operar el sistema; gestionar proyectos de TI; adquisición de recursos de TI; gestionar proveedores.

Auditoría de Explotación y Mantenimiento

(3) Se deben asignar funciones segregadas con la menor incompatibilidad posible. De acuerdo con las funciones, asignar transacciones, atributos por usuario, niveles de supervisión.

(4) Se deben establecer cuentas de usuarios con sus claves con vencimientos y habilitar el sistema y aplicación para cada necesidad específica.

(5) Se deben analizar, probar y autorizar todas las adaptaciones y/o desarrollos realizadas al sistema y tener un responsable de su implantación.

(6) Se deben incorporar totales de control y controles de integridad de los archivos externos

(7) Se debe monitorear prestaciones de proveedores.

Auditoría de la Seguridad

(8) Se debe realizar un plan de copias de seguridad del sistema y de los datos

(9) Se debe realizar un plan de mantenimiento del SI y un Plan de administración y resguardo de suministros

(10) Se debe diseñar, implementar y mantener un plan de contingencia y continuidad del negocio

iii) **Anexos**: se anexan datos, información respaldatoria de los hallazgos y evidencias; metodología de revisión utilizada.

Firma Auditor de Sistemas