Seguridad Informática

Actividad 1.2

EL CONTROL INTERNO DE TECNOLOGÍA DE LA INFORMACIÓN

Nombre: Santiago del valle

ID: 000427744

Definición de control interno

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para lograr o conseguir sus objetivos".2

El control interno será responsabilidad de cada institución y de las personas que tengan como finalidad crear las condiciones para el ejercicio del control.

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos. Constituyen componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación, y el seguimiento.

El control interno está orientado a promover eficiencia y eficacia de las operaciones de una organización y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

Objetivos del control interno

El control interno de las instituciones, organizaciones para alcanzar la misión institucional, deberá contribuir al cumplimiento de los siguientes objetivos:

- Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- Garantizar la confiabilidad, integridad y oportunidad de la información.
- Cumplir con las disposiciones legales y la normativa de la entidad para otorgar bienes y servicios de calidad.
- Proteger y conservar el patrimonio contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

Responsables del control interno

El diseño, establecimiento, mantenimiento, funcionamiento, perfeccionamiento, y evaluación del control interno es responsabilidad de la máxima autoridad, de los directivos y demás servidoras y servidores de la entidad, de acuerdo con sus

competencias.

Los directivos, en el cumplimiento de su responsabilidad, pondrán especial cuidado en áreas de mayor importancia por su materialidad y por el riesgo e impacto en la consecución de los fines institucionales. Las servidoras y servidores de la entidad, son responsables de realizar las acciones y atender los requerimientos para el diseño, implantación, operación y fortalecimiento de los componentes del control interno de manera oportuna, sustentados en la normativa legal y técnica vigente y con el apoyo de la auditoría interna como ente asesor y de consulta, si es que esta existiera.

En las organizaciones: La máxima autoridad, los directivos y demás servidoras y servidores, según sus competencias, dispondrán y ejecutarán un proceso periódico, formal y oportuno de rendición de cuentas sobre el cumplimiento de la misión y de los objetivos institucionales y de los resultados esperados.

La rendición de cuentas es la obligación que tienen todas las servidoras y servidores de responder, reportar, explicar o justificar ante la autoridad, los directivos, la ciudadanía y/o accionistas, por los recursos recibidos y administrados y por el cumplimiento de las funciones asignadas. Es un proceso continuo que incluye la planificación, la asignación de recursos, el establecimiento de responsabilidades y un sistema de información y comunicación adecuado.

Se deben presentar informes periódicos de su gestión ante la alta dirección para la toma de decisiones, en los que se harán constar la relación entre lo planificado y lo ejecutado, la explicación de las variaciones significativas, sus causas y las responsabilidades por errores, irregularidades y omisiones.

Tipos de control interno de TI

De acuerdo con el momento en que se realiza un control, estos se clasifican en:

- Preventivo
- De Detección
- Correctivo

Preventivos

Intentan evitar que ocurra el error. Se utilizan en las primeras etapas del flujo de datos de un sistema. Por ejemplo: el tener buenos formularios de entrada de datos ayuda a evitar que se produzcan errores en la captura, o un software de seguridad que impida los accesos no autorizados al sistema.
Son controles generales. Este hecho les hace inmunes a los cambios, pero posibilita la aparición de errores de muchas clases. Por ejemplo: la separación de tareas no cambia, aunque las tareas se realicen de diferente manera, pero no garantiza que las tareas estén bien ejecutadas. El hecho de tener buenos formularios no impide que se cometan errores en la captura.
En resumen los controles preventivos tratan de evitar el hecho.

De Detección

Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Identifican los errores después de que éstos ocurran. Tienden a ser controles específicos, utilizados en una fase posterior en el tiempo a los controles preventivos. El hecho de ser específicos hace que sean dependientes de los cambios. Ejemplo: programas de validación de entrada de datos, o el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

Correctivos

Facilitan la puesta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad. Estos controles tratan de garantizar que se corrigen los errores detectados.

CASO ZIKA S.A

La empresa ZIKA S.A. distribuye medicamentos en todo el Norte y Oriente Colombiano y en Venezuela.
Actualmente cuenta con sus operaciones en 3 ciudades, Cúcuta, Bucaramanga y Maracaibo.

Posee un sitio web que aparte de brindar información general y posibilidad de contactarse con un asesor comercial, ofrece la posibilidad de rastrear pedidos mediante el número de la factura o mediante la guía de envío de la mercancía (esta operación la hace un tercero, una reconocida empresa transportadora)
La empresa en la sede de Bucaramanga cuenta c
on 30 empleados y 25 computadores con Windows 8.1 professional. Existen 2 servidores con Windows Server 2016 y Red Hat Enterprise Linux 7 respectivamente.

Las otras 2 sedes de la empresa tienen 20 computadores cada una. La sede de Maracaibo cuenta con Windows 10 en todos los equipos y la sede de Cúcuta con 10 computadores con Windows 10 y 10 computadores con Fedora 16.

El servicio de correo institucional se contrata con Gmail. En el servidor con RHEL & está configurado el servidor web de la empresa y sobre este se encuentra el sitio de ZIKA S.A. Últimamente la empresa ha sufrido varias caídas de la página y quejas de clientes que no pueden acceder al rastreo de los envíos ni a la consulta de precios de los productos que ofrece la empresa.

La empresa, a través de su equipo de sistemas desarrolló su propia aplicación de almacén e inventario de productos médicos, facturación y nómina (CHIKUNMEDI). Ésta es una aplicación cliente servidor solo disponible en la LAN de la empresa.

No hay una política de copias de seguridad definida, solo se realiza una copia full cada 2 meses de la base de datos asociada a la aplicación CHIKUMENDI.

No existe control de acceso a ninguna de las instalaciones de la empresa, actualmente solo se hace un registro en portería principal si no se hace parte de la nómina de la empresa, sin embargo, hay gran tráfico de personal en las 3 sedes de ZIKA S.A porque muchos dueños de droguerías de la ciudad van a adquirir sus productos directamente ya que son más económicos.

Uno de los dueños de ZIKA S.A. tiene un conocido en una empresa de telecomunicaciones y este conocido fue quien hizo el cableado de las 3 sedes, utilizó algunos elementos de segunda para ahorrar costos (con el conocimiento de los socios de ZIKA). No existen puntos de red certificados ni manuales ni documentación sobre ningún dispositivo (routers y switches).

La aplicación CHIKUNMEDI genera reportes de ventas, stock de almacén, facturación y nómina de empleados.

El departamento de sistemas consta de 1 jefe de sistemas, 3 tecnólogos (2 desarrollo y 1 soporte a usuario) y 2 practicantes del SENA que cambian cada 3 meses.

Actividad en clase:

1. Diseñe 9 controles para ZIKA S.A. Clasifíquelos como preventivos, de detección o correctivos según sea el caso para la empresa ZIKA S.A.

2. Socialice con los compañeros los controles que elaboró para su ejercicio en clase.

Desarrollo

1. Bases de datos incrementales: Se debe realizar una copia incremental cada día y una completa cada semana con el fin de que si la base es robada, borrada o modificada por parte de terceros, se pueda recuperar la información íntegra de los clientes. Este es un control correctivo.

2. Regla 3,2,1 BD: El almacenamiento de las copias de seguridad debe regirse por la norma 3,2,1; 3 copias, en 2 sitios diferentes y que una esté en la nube. Todo esto se hace con el fin de evitar que, por alguna catástrofe natural/humana (Terremoto, incendios), se pierdan los servidores y, por ende, las bases de datos y sus respectivas copias de seguridad de la empresa. Este es un control correctivo.

3. Documentación y corrección de la infraestructura: En base a la documentación/buenas prácticas proporcionadas por la ISO 9001, se debe documentar cada dispositivo de la infraestructura y ejecutar un plan de mantenimiento. Al utilizar componentes de seguridad sin un aval de calidad, se pone en riesgo los componentes físicos (Servidores, PCs, Routers) además de la disponibilidad de los múltiples servicios. Además, sin la documentación, cualquier cambio ejecutado por un nuevo integrante del equipo podrá causar un gran daño debido a que no se tiene conocimiento de cómo están configurados los dispositivos. Esta es una norma preventiva.

4. Controles físicos: Depende del presupuesto de la compañía para ejecutar controles de acceso más robustos; sin embargo, se debe ejecutar controles a todo el personal con el fin de evitar robos y/o daños por parte de terceros. Este es un control correctivo.

5. Bloqueo de puertos físicos: Se debe ejecutar una política de acceso respecto a los equipos con el fin de evitar malware inyectado mediante USB que pueda afectar tanto el dispositivo en cuestión como la red de la empresa. Esta es una norma preventiva.

6. Bloqueo de puertos digitales: Sobre todo en los servidores, se debe cerrar todos los puertos que no estén ejecutando servicios esenciales respecto al funcionamiento de la empresa con el fin de evitar conexiones no deseadas. Esta es una norma preventiva.

7. Actualizar SO/Drivers: Actualizar tanto los controladores (W8, W10 a W11, WServer 2016 a WServer 2023, RHEL 7 a RHEL 10, etc.) como los sistemas operativos de las múltiples sedes con el fin de parchar brechas de seguridad y mejorar el rendimiento de los dispositivos. Esta es una norma correctiva.

8. Plantear escalado horizontal: Debido a las caídas constantes de la página web alojada en el servidor de RHEL, se debe plantear el desarrollo de un clúster que permita un flujo constante e incremental de usuarios a lo largo del tiempo (También se puede plantear un escalado vertical; sin embargo, a la larga, sale mejor y más económico tener diversos dispositivos que dividan la carga de trabajo). Esta es una norma correctiva.

9. Auditorías de seguridad: Es conveniente realizar auditorías de seguridad de forma periódica para identificar posibles vulnerabilidades y asegurar que se están cumpliendo con las políticas y controles establecidos. Esta es una norma de detección.

10. Logs del sistema: Configurar registros de auditoría para monitorear y registrar el acceso a sistemas críticos y datos sensibles. Esta es una norma de detección.