TP2: Auditoría de sistemas de información

Etapa 2 - Identificación de riesgos potenciales

Realizado por los grupos 8 y 19

¿Que es la identificación de riesgos potenciales?

Es la parte del proceso de auditoría en la que conocemos e inspeccionamos los riesgos.

El objetivo de la identificación del riesgos es conocer los sucesos que se pueden producir en la organización y las consecuencias que puedan tener sobre los objetivos de la empresa.

Según los autores ¿Que es un riesgo?

- **Riesgo** es el impacto y la probabilidad de que una **amenaza** (o de una serie de eventos/ amenazas) puedan **afectar** de manera adversa la consecución de los **objetivos**.
- El **riesgo de auditoría** es el riesgo de que un auditor fracase al detectar las pérdidas materiales reales, o potenciales, o los registros incorrectos
- Un riesgo implica el resultado de la falta de certeza acerca de los efectos/implicaciones de que traen diversos eventos sobre algo valorado, generalmente consecuencias negativas e indeseables.
- El manejo de riesgos como definido en la ISO 31000 se Refiere a las actividades coordinadas de una organización con el fin de controlar y dirigir sus riesgos.

¿Cómo clasificamos los riesgos según su gravedad?

Crítico: Si ocurrieran, resultarían en bancarrota.

Importantes: Si ocurrieran podrían llevar a posibles pérdidas, que no llevarían a la bancarrota pero que requerirían que el negocio pida préstamos para poder continuar con las operaciones.

No Importantes: Si ocurrieran podrían ser solucionados usando activos existentes o los ingresos sin tener que imponer ninguna presión financiera innecesaria.

Tipos de riesgos de auditoría

1. **Riesgo Deseado:** el riesgo que se desea correr.
2. **Riesgo Inherente:** refleja la probabilidad que una pérdida material o una imputación errónea exista en algún segmento de la auditoría, antes de que sea considerada la confiabilidad de los controles internos.
3. **Riesgo de Control:** refleja la probabilidad que en algún segmento de la auditoría, los controles internos no prevengan, detecten o corrijan pérdidas materiales o imputaciones erróneas que puedan surgir.
4. **Riesgo de Detección:** refleja la probabilidad que los procedimientos de auditoría utilizados en algún segmento, fallen en detectar pérdidas materiales o imputaciones erróneas.

Instrumentos para identificar riesgos

1. **Indagaciones ante la dirección y ante las personas que conforman la entidad en general**: consiste en la libertad que tiene el auditor de realizar las labores de investigación e inspección directamente con el personal que considere poseedor de información valiosa para la identificación de los riesgos.
2. **Procedimientos analíticos:** pueden incluir la comparación de estados financieros de períodos anteriores, la indagación por la existencia de personal nuevo, los sistemas de información internos y las características de control para la generación y alimentación de la información contable.
3. **Observación e inspección**: está direccionada a la recopilación de la información obtenida de los procedimientos anteriores, a fin de recopilar los resultados y de esta manera lograr la identificación de los riesgos.

Maneras de manejar los riesgos

1. **Evitar el riesgo**
2. **Prevenir que el riesgo ocurra**
3. **Reducir el “daño” que podría realizar el riesgo en caso de que ocurra**
4. **Transferir el riesgo (ej: conseguir un seguro)**

Riesgos Potenciales para Starship

Posibles riesgos en el acceso a las instalaciones (físicas y virtuales)

- **Seguridad física débil**: Falta de staff de seguridad y/o falta de conocimiento de las normas por parte de los usuarios.
- **Acceso no autorizado o cambios en los datos o programas**: Todas las aplicaciones deberían requerir varios niveles de autorización para el ingreso y la aceptación de transacciones.
- **Información inexacta**: Los usuarios pueden ingresar información sin entender el formato o la información requerida. Puede producir información redundante o imprecisa en el sistema.

Posibles riesgos en el acceso a las instalaciones (físicas y virtuales)

- **Entrada de datos errónea o falsificada:** Que el sistema sea incapaz de detectar información evidentemente falsa o incorrecta al momento de su ingreso.
- **Mal uso por usuarios finales autorizados:** Fallar en determinar cuando los usuarios autorizados están usando las instalaciones virtuales de acuerdo a las formas legítimas del trabajo.
- **Procesamiento incompleto:** Incluye archivos o solicitudes que no puedan ser procesadas debido a errores en el sistema.

Posibles riesgos en el acceso a las instalaciones (físicas y virtuales)

- **Procesamiento fuera de término:** Esto incluye el procesamiento retrasado debido a problemas tecnicos.
- **Fallo del sistema de comunicaciones:** Información que transmitirse por líneas de comunicación es vulnerable a fallos accidentales o intercepción intencional por usuarios no autorizados.
- **Tests inadecuados:** Las pruebas independientes a los programas usados son necesarias para encontrar fallas que pueden haber sido ignoradas por los programadores originales.

Posibles riesgos en el acceso a las instalaciones (físicas y virtuales)

- **Soporte inadecuado:** Puede ocurrir que los usuarios no reciban soporte efectivo debido a una falta de staff o de formación del departamento IT.
- **Documentación insuficiente:** Todo sistema usado por múltiples usuarios, o que produzca beneficios a largo plazo, debería estar bien documentado.
- **Destrucción prematura de registros de acceso:** El acceso a las instalaciones de la empresa debe quedar registrado durante al menos 6 meses

Posibles riesgos en la asignación de los recursos informáticos

- **Uso ineficiente de los recursos:** Los costos de operación podrían aumentar debido a la falta de formación técnica o soporte. También puede resultar en la compra de hardware y/o software inapropiado, redundante o incompatible con la arquitectura de sistemas de la organización.
- **Análisis incompleto del sistema:** La identificación de los problemas puede ser incompleta o inapropiada, y el sistema completo podría ser incapaz de resolver el problema de negocio.

Posibles riesgos en la asignación de los recursos informáticos

- **Acceso no autorizado a datos o programas:** El uso de controles de acceso, tales como contraseñas, normalmente son débiles en sistemas controlados por los usuarios. En algunos casos, las contraseñas pueden ser compartidas o fácilmente determinables.
- **La destrucción de la información por virus informáticos:** En el ambiente de hoy en día, existe un número casi ilimitado de fuentes por las que un virus puede introducirse, y pueden causar varios problemas, entre ellos, la destrucción de información, software y/o hardware.


RIESGOS
EMPRESA
AUDITORES

FIN