***Seguridad y auditoria informática***

Unidad 1° RED TEAM, Riesgos, vulnerabilidades y Amenazas.

Contenidos:

1. Análisis de riesgos.
2. Delitos informáticos
3. Tipos de atacantes
4. Ingeniería social
5. Virus, troyanos.

**Trabajo en grupo de 3 primera evaluación 15%**

* Problemática “Identificación de riesgos e impacto”
* Riesgos, vulnerabilidades y amenazas
* Informe de trabajo
* Pauta de evaluación

***La información***

Por ello:

* Las gerencias deben establecer sistemas de control interno que soporten en forma adecuada los procesos críticos del negocio.
* Las organizaciones exitosas entienden y administran los riesgos asociados de la implementación de tecnología de información.
* Todo lo anterior justifica la necesidad de contar con una herramienta de control como lo es la auditoria informática.

***Concepto de auditoria.***

Consiste en la emisión de una **opinión profesional** sobre si el objeto sometido a análisis (programa) presenta adecuadamente la realidad que pretende reflejar y/o cumple con las condiciones que le han sido prescritas (procedimientos, normas, etc.). La auditoria opina y recomienda sobre cualquier proceso.

***Auditar consiste en:***

Estudiar los mecanismos de control que están implantados en una organización o proyecto, para determinar si los mismos son adecuados y cumplen unos objetivos y estrategias, estableciendo los cambios que se deberían realizar para la consecución de sus resultados los objetivos.  
considerando:

1. Evidencias: las evidencias son las pruebas que tenemos que probar que son reales.
2. Riesgos: los riesgos son distintos tipos de situación a las que estamos expuestos, que afectan el buen funcionamiento de los procesos.
3. Controles: buscan minificar los riesgos, controlarlos, atenuarlos, etc.

|  |  |  |  |
| --- | --- | --- | --- |
| Clase | Contenido | Objeto | Finalidad |
| Financiera | Opinión | Cuenta anual | Presentar real |
| Informática | Opinión | SIAS. Planes | Operatividad |
| Gestión | Opinión | Dirección | Eficacia, eficiencia, economicidad |
| Cumplimiento | Opinión | Normas estab | Si opera adecuado a las normas |

Puede ser:

1. Total
2. Parcial
3. Permanente
4. Verificativas
5. Técnicas

Concepto de consultoría

Concepto de consultoría.

La consultoría consiste en dar asesoramiento o consejo sobre lo que se ha de hacer, o como llevar a cabo adecuadamente una determinada actividad para obtener los fines deseados, se relaciona directamente con la solución al problema del cliente.

***Clases de consultoría***

|  |  |  |  |
| --- | --- | --- | --- |
| Clase | Contenido | Objetivo | Finalidad |
| Financiera | Asesoramiento | Planes de cuenta Procedimientos | Diseño implementación Administrativos |
| Informática | Asesoramiento | Aplicaciones Planes de contingencia | Desarrollo, Diseño e implementación |

***Definiciones de auditoria.***

Definición “La auditoría informática es el proceso de”:

1. Recoger
2. Agrupar
3. Evaluar evidencias

Para determinar si un sistema informático o proceso informático salvaguarda los ***activos*** empresariales informáticos, mantiene la integridad de los datos y lleva a cabo eficazmente los fines de la organización, utilizando eficientemente los recursos.

***Activos informáticos:***

1. Información
2. Hardware
3. Software
4. Sistemas
5. Documentación
6. Personas

***Objetivos de la auditoria***

1. Control de la función informática
2. La operatividad
3. Seguridad (física y lógica)->planes de contingencia
4. Identificación de las áreas de mejora
5. Atenuación de los riesgos(controles)
6. El análisis de la eficiencia y eficacia de los sistemas informáticos
7. La verificación del cumplimiento de la normativa->normas internacionales
8. La revisión de la gestión de los recursos informáticos
9. Protección de los activos e integridad de datos

***La función de la auditoria.***

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones y queda a cargo de la organización tomar las decisiones pertinentes.

La auditoria contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias para eliminar las debilidades antedichas; estas sugerencias son plasmadas en el informe final de la auditoria que recibe el nombre de recomendaciones.

Aunque la auditoria interna sea independiente del departamento de sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorias externas como para tener una visión desde afuera de la empresa.

***Causas que justifican auditorias informáticas***

* Síntomas de descoordinación y desorganización:

Cuando no coinciden los objetivos de la informática con los de la organización compañía (no hay alineamiento) cuando los estándares de productividad se desvían sensiblemente de los promedios habitualmente conseguidos cuando ocurre algún cambio masivo de personal, o una restricción de alguna área que puede resultar fallida.

* Síntomas de inseguridad:

**Evaluación del nivel de riesgos**

1. Seguridad lógica.
2. Seguridad física.
3. Confidencialidad [Los datos son propiedad inicialmente de la organización que los genera, los datos de personal con especialmente confidenciales].
4. Continuidad del servicio es un concepto aun mas importante que la seguridad establece las estrategias de continuidad entre fallos mediante planes de contingencia totales y locales.
5. Centro de proceso de datos fuera de control si tal situación llegara a percibirse, sería prácticamente inútil, la auditoria. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

* Síntomas de mala imagen e insatisfacción de los usuarios:

Cuando no se atienden las peticiones de los usuarios, ejemplo: cambios de software en los terminales de usuario. Refrescamiento de paneles, etc.

* Síntomas de debilidades económico-financiero:

Cuando ocurre un incremento desmesurado de costos como necesidad de justificación de inversiones informáticas (La empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

Desviaciones presupuestarias significativas

Costos y plazos de nuevos proyectos (deben auditarse simultáneamente con el desarrollo del proyecto y al órgano que realizo la petición)

***Áreas de la auditoria informática***

Conceptos previos

* CPD (centro de procesamiento de datos)
  + Estructura del CPD
  + Funciones principales de un CPD
* Externalización de servicios
* El data center
* Servicios de I.S.P
  + Hosting
  + Hausing
  + Seguridad
  + Comunicaciones
* Servicios de A.S.P (Application system provider)
  + World class
* Servicios Cloud

**Áreas de especialización:**

1. Auditoria de la explotación
2. Auditoria del desarrollo
3. Auditoria de sistemas
4. Auditoria de sistemas operativos
5. Auditoria de sistemas licenciados
6. Auditoria de redes
7. Auditoria de seguridad
8. Auditoria física
9. Auditoria lógica
10. Auditoria de la ofimática
11. Auditoria de la dirección
12. Auditoria del mantenimiento
13. Auditoria de las bases de datos
14. Auditoria de la calidad
15. Auditoria de proyectos