Cuestionario de Autoevaluación del Tema 1

1. En cuanto a las normas generales para hacer auditorías, está la de “Relación Organizativa”, esta se refiere a:

   Completar de manera objetiva la auditoria

2. Cuál de los siguientes modelos podría establecerse antes de usar COBIT en una empresa considerando que COBIT está más orientado al control

   ITIL

3. Una persona extraña, logró entrar a un curso o aula virtual del ecampus, dado que el código de acceso fue divulgado. EL valor comprometido es:

Confidencialidad

4. Un ejemplo de control de influencia directiva, en el desarrollo de proyectos de software es:

El seguimiento a las actividades del plan

5. Se dice que la auditoría de sistemas es un control de tipo selectivo porque:

Selecciona controles

6. De las siguientes actividades, seleccione la que no pertenece a un proceso de auditoría de sistemas:

Implementar controles definidos

7. Si en un sistema informático utilizamos una bitácora de accesos al sistema, es porque se quiere garantizar:

No repudio

8. Si en un sistema informático definimos un nivel de acceso para cada usuario del sistema (esto quiere decir que el usuario solo puede acceder a las funciones e información permitidas), es porque se quiere garantizar la:

Confidencialidad

9. Existen dispositivos de red y conexiones de red que no están protegidas y se encuentran en áreas de circulación del personal y clientes, lo cual da lugar a que fácilmente puedan ser violados por personas extrañas a la organización o los mismos empleados. El valor comprometido es:

Integridad

10. Cuál de los siguientes activos informáticos tiene mayor valor para un empresa:

Información almacenada

11. Las tres dimensiones de COBIT son:

Procesos, Recursos de TI, y Criterios de Información

12. Cuál de las siguientes etapas, es la primera que debe realizar el auditor para establecer y/o evaluar un sistema de control?:

Establecer estándares

13. Desde el punto de vista de la jerarquía que ocupan en una organización, un sistema de control gerencial permite:

Planeamiento táctico

14. Un programador de sistemas de la empresa ha cometido fraude a través de un código oculto en un programa, del cual también es usuario. El valor comprometido es:

Autenticidad

15. Un principio de la auditoria operacional utilizada en la auditoria de sistemas es:

La eficiencia operacional de usuarios y administradores de TI.

Cuestionario de Autoevaluación del Tema 2

1. Es el dominio donde se identifica la mejor manera en que TI puede contribuir al logro de los objetivos del negocio:

PO

2. Dominio Cobit donde todos los procesos deben evaluarse de forma regular en cuanto al cumplimiento de los objetivos de control:

ME

3. El Grupo de Control es el encargado de definir y ejecutar el control .

Falso

4. Son características del Alineamiento Estratégico de COBIT

   Garantiza un vinculo entre los planes de negocio y planes de TI

   Relaciona las operaciones de TI con las operaciones de la empresa

5. Rellenar con el Proceso de TI correcto, use el código del proceso, por ej DS5 para Seguridad de la Información

La Administración del Portafolio de TI es un objetivo de control del proceso **PO1**

El Esquema Clasificación de Datos es un objetivo de control del proceso **PO2**

La Administración de Beneficios es un objetivo de control del proceso **PO5**

La Identificación de Eventos o Amenazas es un objetivo de control del proceso **PO9**

AI

Estudio de Factibilidad y Formulación Cursos de Acción Alternativos es un objetivo de control del proceso **AI1**

Transferencia de Conocimiento al Personal de Operaciones y Soporte es un objetivo de control del proceso **AI4**

El Plan de Prueba es un objetivo de control del proceso **AI7**

DS

Almacenamiento de Respaldos Fuera de las Instalaciones es un objetivo de control del proceso **DS4**

6. Son los beneficiados de aplicar COBIT en una Organización:

   Auditores

   Gerentes

   Usuarios

7. Identificación de soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes:

   Adquirir e Implementar

8. Que la información sea generada con uso más óptimo de los recursos de TI:

   Eficiencia

9. Arrastre las palabras a los cuadros correctos

   PO Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
   AI Proporciona las soluciones y las pasa para convertirlas en servicios.
   DS Recibe las soluciones y las hace utilizables por los usuarios finales.
   ME Monitorear todos los procesos para asegurar que se sigue la dirección provista.

10. Asocie correctamente:

    Proceso del Dominio PO:
    Evaluar y Administrar los Riesgos
    Proceso del Dominio AI :
    Administrar cambios
    Proceso del Dominio DS:
    Educar y entrenar a los usuarios
    Proceso del Dominio ME:
    Proporcionar Gobierno de TI

11. Incluye la Administración de las Infraestructura Informática y su seguridad:

    Entrega y Soporte

12. El Sensor, tiene la capacidad de medir la desviacion del elemento a controlar respecto a un estándar, ademas de poder corregir dicha desviación.

    False

13. Arrastre las palabras a los cuadros correctos

    Requerimientos de Negocio dirige la inversión en Recursos de TI que es utilizado por Procesos de TI para entregar Información que responde a Requerimientos de Negocio

14. Según COBIT, que la información sea relevante y pertinente para los procesos de negocio, y se proporcione de una manera oportuna, consistente y utilizable:

    Eficacia

15. Son principios de COBIT:

    Separar el Gobierno de TI de la Gestión de TI

    Aplicar un marco de referencia único e integrado

    Satisfacer las necesidades de las partes interesadas

CUESTIONARIO DE AUTOEVALUACION TEMA 3

1. Ordene las Etapas del Proceso de Auditoria

   Planeacion

   Programa de Auditoria

   Recoleccion de Evidencia

   Evaluacion de Fortalezas y debilidades

   Elaboracion del informe de auditoria

   Monitoreo

2. Relaciones amenzas con tipo (STRIDE)

   Descubrimiento de la información => **Sniffing**

   Spoofing => **Navegación invisible**

   Repudio => **Desfragmentación de Disco Duro**

   Escalamiento de Privilegios **=> Usuario con derechos por encima de su rol**

   Tampering **=> SQL Inyectión**

3. Cuales Dos de los siguientes son objetivos de una auditoria de sistemas informáticos o auditoria informática.

   Comprobar la exactitud de los reportes que emiten los sistemas de información

   Evaluar la suficiencia del control de TI establecido, respecto a los riesgos que controlan

4. A menor cantidad de pruebas de cumplimento exitosas, mayor será la cantidad de pruebas sustantivas que realizar

   Verdadero

5. Alguno de los posibles elementos de un informe final de auditoria podría ser:

   Aspectos positivos que se encontraron en la evaluación

   Evidencia material

   Hallazgos

6. Asocie riesgo con ámbito de Auditoria

   Operaciones **=> Perdida de información de la BD**

   Administrativo **=> No hay alineamiento estratégico entre TI y gerencia.**

   Desarrollo **=> Tasa de Defectos muy alta en las aplicaciones de negocio.**

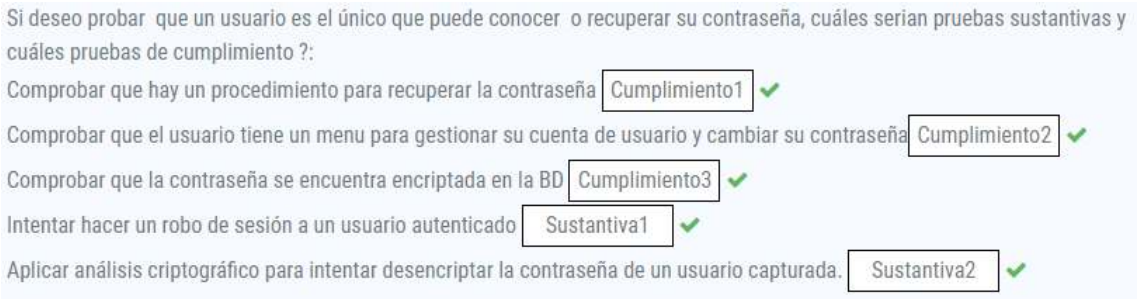
7. En que sección del contrato de auditoria se define la contraparte por parte de la Empresa para el control del trabajo de Auditoria

   Responsabilidad

8. En que sección del contrato de auditoria se define los informes que el auditor mínimamente debería entregar

   Obligación de Rendir cuentas

9. Si deseo probar que un usuario es el único que puede conocer o recuperar su contraseña, cuales seria pruebas sustantivas y cuales seria pruebas de cumplimiento



10. Si el control está bien establecido en un sistema de información de tal manera que el nivel de riesgo se bajó, entonces habrá que realizar menos pruebas sustantivas.

    Verdadero

CUESTIONARO AUTOEVALUACION TEMA 4

1. Cuál de los siguientes es un riesgo que se puede controlar con el Proceso de Definir la Arquitectura de la Información

   Falta de niveles de confidencialidad de la Información

2. Cuáles son objetivos de control relacionados con los Planificación estratégica de TI

   Alineamiento estratégico

   Planificación a largo plazo

   Planificación táctica

3. La fase de Nolan donde ya se adoptan estándares para todos los productos del servicio informático, más allá de la administración y control de los mismos, es la fase de

   integración

4. Cuáles son características de Soporte Técnico:

   Mantener el middleware de las plataformas operativas

   Gestionar la instalación de la plataforma operativa

5. Cuál refleja mejor la integración entre Auditoria de Sistemas y Seguridad de la Información como unidades de TI

   Auditoría se enfoca en la evaluación de riesgos de Ti y la seguridad en la evaluación de riesgos de Seguridad de manera más específica

6. Cuál de los siguientes roles asume la Propiedad de un Proyecto de Sistemas

   Usuarios representantes

7. Asocie objetivo de control con Proceso de TI

   Propiedad y Custodio de la información=> **Definir Organización y sus relaciones**

   Administración formal de Riesgo asociados a un proyecto=> **Administrar Proyectos**

   Fomentar la Estandarización asociadas a la tecnología => **Dirección Tecnológica**

8. La fase de Nolan donde ya se piensa en el desarrollo de aplicaciones gerenciales y en la integración de sistemas de la organización, es la fase de :

   Control

9. Cuál sería la ecuación que mejor se aplicaría en el caso de proyectos de TI con retorno de inversión a 3 o 4 periodos?

«math xmlns=¨http://www.w3.org/1998/Math/MathML¨»«mi»R«/mi»«mi»O«/mi»«mi»I«/mi»«mo»§#160;«/mo»«mo»=«/mo»«mo»§#160;«/mo»«mfrac»«mrow»«munder»«mo»§#8721;«/mo»«mi»i«/mi»«/munder»«mi»V«/mi»«mi»A«/mi»«mi»N«/mi»«mo»(«/mo»«mi»B«/mi»«msub»«mi»N«/mi»«mi»i«/mi»«/msub»«mo»)«/mo»«mo»-«/mo»«mi»I«/mi»«mi»n«/mi»«mi»v«/mi»«mi»e«/mi»«mi»r«/mi»«mi»s«/mi»«mi»i«/mi»«mi»o«/mi»«mi»n«/mi»«/mrow»«mrow»«mi»I«/mi»«mi»n«/mi»«mi»v«/mi»«mi»e«/mi»«mi»r«/mi»«mi»s«/mi»«mi»i«/mi»«mi»o«/mi»«mi»n«/mi»«/mrow»«/mfrac»«/math»

El mas LARGO

1PARCIAL – EXAMEN

1. Cuál de las siguientes etapas, es la primera que debe realizar el auditor para establecer y/o evaluar un sistema de control?:

   Establecer estándares

2. Que la información se generada con el uso más óptimo de los recursos de TI:

   Eficiencia

3. Son principios de la auditoría contable que se aplican en la auditoria de sistemas:

   La oportunidad de datos que presenta un sistema

   La protección de activos informáticos

   La exactitud de los resultados del sistema

4. Se dice que la auditoria es una crítica que se hace al sistema, porque:

   Destaca los aspectos positivos y negativos del control

5. Un programador que también es usuario de una aplicación que el mismo desarrollo para una empresa, podría cometer fraude aprovechando su doble rol. Valor amenazado:

   No repudio

6. En cuanto a las normas generales para hacer auditoria, está la de “Relación Organizativa”, esta se refiere a:

   Completar de manera objetiva la auditoria

7. Si a variable observado es un numero de 8 dígitos. Pasando por la sintaxis, semántica, relevancia, un ejemplo de información en relación a esa variable podría ser:

   Que un número de celular del docente de una materia en la que estoy matriculado

8. Un principio de la auditoria operacional utilizada en la auditoria de sistemas es:

   La eficiencia de usuarios y administradores de TI

9. Seleccione las afirmaciones ciertas en relación a COBIT

   Los procesos de TI proveen información a los procesos de negocio para alcanzar los objetivos de negocio

   Las necesidades del negocio conducen las inversiones de Recursos de Ti que son usados por los procesos de TI

10. Si el examen parcial de una materia es un SENSOR, entonces el DOCENTE es el grupo de control, el elemento a controlar es el aprovechamiento del estudiante, entonces el GRUPO activante es:
    Estudiante

11. 2 diferencias entre ITIL v3 y COBIT5 son:

    ITIL está orientado a la mejora de los servicios de TI y COBIT mas a la mejora del control de los procesos de TI

    COBIT 5 está más orientado al "QUE" se debe controlar e ITIL esta mas orientado al "COMO"

12. ¿Cuál de las siguientes actividades, es la que NO realiza un auditor?

    Ejecutar acciones correctivas

13. Según COBIT, que la información sea relevante y pertinente para los procesos de negocio, y se proporcione de una manera oportuna, consistente y utilizable:

    Eficacia

14. A través de un ataque de escalamiento de privilegios en el sistema, un simple vendedor de la empresa logra tener acceso a una cuenta gerencial. ¿Valor amenazado?

    Autenticidad

15. Asocie Objetivo de control con Dominio Val IT

    Gestión de la Inversión => **Definir y documentar un caso de negocio detallado, incluyendo el detalle de los beneficios**

    Gobierno de Valor =>**Definir las características de la cartera de Inversiones**

    Gestión de la Cartera => **Evaluar, priorizar y seleccionar, aplazar o rechazar las inversiones**

16. Cuáles de los siguientes son un control de influencia directiva:

    Se hace una planificación de un Proyecto de desarrollo de Software

    Se establecen roles para el equipo de desarrollo de Software

17. Empareje adecuadamente

    Grupo de Control => **Sensor de huella digital (subsistema de comparación)**

    Elemento a controlar => **Acceso autorizado**

    Grupo Activante => **Sensor de huella digital (subsistema de acceso)**

    Objetivo de control => **Evitar el acceso no autorizado**

    Control => **Acceso por huella digital**

18. Se dice que la auditoria de los sistemas es un control de tipo selectivo porque:

    Selecciona controles

19. El valor opuesto que se deduce de esta amenaza: Phising

    Falsificación

20. Relacione con el par Correcto

    Administración de Recursos => **Cuidar la inversión de TI y administrarla adecuadamente**

    Alineamiento estratégico => **Las operaciones de TI deben estar en concordancia con las operaciones del negocio**

    Administración de Riesgos => **Identificar amenazas y niveles de aceptación del riesgo**

    Medición del Desempeño => **Establecer metas medibles y hacer un monitoreo de la entrega del servicio**

    Entrega de Valor => **Asegurarse que las TI le den a la empresa los beneficios esperados**

21. Asocie riesgo con ámbito de Auditoria

    Operaciones **=> Perdida de información de la BD**

    Administrativo **=> No hay alineamiento estratégico entre TI y gerencia.**

    Desarrollo **=> Tasa de Defectos muy alta en las aplicaciones de negocio.**

22. Un principio de la auditoria operacional utilizada en la auditoria de sistemas es

    La eficiencia de usuarios y administradores de TI

23. La etapa más subjetiva y difícil de realizar del proceso de análisis y gestión de riesgos ISO27005 Debido a que depende mucho a la experiencia y conocimiento de los que realizan este proceso es la ……**evaluacion**……del riesgo

24. Cuales DOS de los siguientes son objetivos de una auditoria de sistemas informáticos o auditoria informática.

    Evaluar la suficiencia del control de TI establecido, respecto a los riesgos que controlan

    Comprobar la exactitud de los reportes que emiten los sistemas de información

25. Según COBIT, que la información sea relevante y pertinente para los procesos de negocio, y se proporcione de una manera oportuna, consistente y utilizable:

    Eficacia

26. Identificación de Soluciones, desarrollo o adquisición, cambios y/o mantenimiento de sistemas existentes:

    Adquirir e Implementar

27. Incluye la administración de la arquitectura informática y la seguridad

    Entrega y Soporte

28. Un ejemplo de control de influencia directiva, en el desarrollo de proyectos de software:

    El seguimiento a las actividades del plan

29. Es una característica de Alineamiento Estratégico de COBIT

    Dos características

    Garantiza un vínculo entre los planes de negocio y planes de TI

    Relaciona las operaciones de TI con las operaciones de la empresa

30. Relaciones amenzas con tipo (STRIDE)

    Descubrimiento de la información => **Sniffing**

    Spoofing => **Navegación invisible**

    Repudio => **Desfragmentación de Disco Duro**

    Escalamiento de Privilegios **=> Usuario con derechos por encima de su rol**

    Tampering **=> SQL Inyectión**

31. Asocie Correctamente

    Reglas de filtrado de Trafico en un fireware para aislar la red interna de la red externa **Control Técnico**

    Tipo de control para darse cuenta que estamos en riesgo (por ej. Una prueba covid-19)

    Control Detectivo

    Tipo de Control relacionado con las actividades del personal en el trabajo diario **Control Administrativo**

    Debilidades en el control o inexistencia del mismo=>**Vulnerabilidades**

    Acceso a ambientes por huella Digital => **Control Físico**

32. Cual de los Siguientes modelos deberían implementarse antes que los demás

    ITIL

33. Alguno de los posibles elementos de un informe final de auditoria podría ser:

    Aspectos positivos que se encontraron en la evaluación

    Evidencia material

    Hallazgos

34. Se dice que la auditoria de sistemas es un tipo de control selectivo por que :

    Selecciona Controles

35. Un estándar Genérico que nos ayuda mucho en el enfoque de auditoria basada en riesgos es

    Iso31000

36. Relacione con el par correcto

    Administración de Recursos => **Cuidar la inversión de TI y administrarla adecuadamente**

    Alineamiento estratégico => **Las operaciones de TI deben estar en concordancia con las operaciones del negocio**

    Administración de Riesgos => **Identificar amenazas y niveles de aceptación del riesgo**

    Medición del Desempeño => **Establecer metas medibles y hacer un monitoreo de la entrega del servicio**

    Entrega de Valor => **Asegurarse que las TI le den a la empresa los beneficios esperados**

37. Ordene las etapas de un proceso de Auditoria

    Planeacion

    Programa de Auditoria

    Recoleccion de Evidencia

    Evaluacion de Fortalezas y debilidades

    Evaluacion de informe de auditoria

    Monitoreo

38. En el trabajo de auditoria realizado, la parte correspondiente al “Programa de Auditoria” dentro del proceso de auditoría que realizaron, sería el acápite:

    Definición de las pruebas de cumplimiento y sustantivas a realizar

2 PARCIAL - EXAMEN

1. Seleccione los elementos que podría ir en un informe de auditoría:

- **Hallazgos**
- **Evidencia material recolectada**
- **Debilidades del control**
- **Fortalezas de control**

2. Si tengo un roi de 50% significa que:
   Por cada peso invertido recuperado el mismo y demás tengo medio peso adicional

3. ¿Cuáles de los siguientes son beneficios de los SLAs?

- **Cuantificación del uso de servicios de información**
- **Conocimiento de la cantidad del servicio de manera formal por parte del usuario**

4. Qué elementos son los que se relacionan directamente con el impacto del riesgo en un análisis DREAD de la amenaza?

- **Daño potencial**
- **Usuarios afectados**

5. Para que un BCP se active las operaciones en cuestión deben ser operaciones _____ del negocio
   críticas

6. Cuál de los siguientes cumple con la función disuasivo
   Camaras de vigilancia

7. Si el emisor encripta un mensaje con la clave pública del receptor, entonces se garantiza
   La confiabilidad para el receptor

8. Asocie correctamente en función a los objetivos de control que se buscan:

- Control de incidentes => **Aprender de eventos inesperados y establecer posibles soluciones**
- Soporte técnico => **Mantenimiento de la plataforma operativa**
- Control de problemas => **Respuesta a necesidades ya identificadas previamente**
- Control de cambio => **Separación entre aplicaciones en desarrollo y aplicaciones en operación**
- Uso eficiente de recursos => **Evitar el abusivo de los equipos**
- Operación sobre HW => **Control de cambio sobre los equipos**

9. Asocie los procesos con la actividad relacionada en función a su objetivo de control:

Segregación de funciones:

- Aplicar ISO 3100 = **P09 Evaluar riesgos**
- Planificación táctica de sistemas = **P01 Planeamiento estratégico**
- Comparación de alternativas de solución tecnológica a una necesidad empresarial =
- Desarrollar un POA = **PO5 administrar Inversiones**
- Cumplir con obligaciones regulatorias de la ASFI para entidades financieras =
- Clasificación de activos de información: = **PO2 arquitectura de la información**
- Aplicar TDD = **PO11 Administrar Calidad**

……..

10. Qué algoritmos se podrían utilizar en una firma digital
    Asimétricos y de hashing

11. Cuál serían prerrequisitos para aplicar la técnica Delphi correctamente

- **Tener un panel de expertos del mismo nivel de experiencia**
- **Tener un criterio de comparación establecido**

12. Delphi es una técnica de valoración de riesgos que permite que un grupo de personas de diferente nivel y experiencia en cuento riesgo pueden valorar los mismos
    Falso

13. Si quiero tener un objetivo del punto de control de recuperación muy alto entonces cuál de los siguientes controles debo seguir
    Espejamiento

14. Además de la iso 31000 para la gestión de riesgo el auditor para utilizar otro estándar iso es muy conocido y muy aplicable a todo entorno de control este estándar es la iso
    27005

15. Identifique que actividades podrían ser parte del análisis de riesgos :

- **Aplicar Delphi**
- **Identificar los riesgos**
- **Evaluar el impacto total de cada riesgo**
- **Priorizar los riesgos**
- **Establecer el contexto de los riesgos**

16. En un proceso de autenticación para acceder la una aplicacion web (ej ecampus), aplicar diferentes casos de prueba de combinación usuario/contraseña para recibir diferentes mensajes de error de la funciones, es una prueba
    Sustantiva

17. Asocia correctamente los riesgos con procesos de TI que lo controlan

- Poca conciencia sobre la seguridad y manejo de incidentes = **Educar y capacitar usuarios**
- Falta de puntos de restauración ante problemas con modificaciones realizadas = **Administrar la configuración.**
- Perdida de informacion por falta de respaldos =
- Robo de equipo informatico = **Administrar las instalaciones**
- No se tienen expectativas claras sobre la calidad del servicio del area de sistemas =
- Filtracion de informacion para la empresa en contratos con proveedores de servicios en la nube => **Administrar Servicios de Terceros**

18. La etapa del BCP que mide peligrosidad de riesgos y determina los activos más críticos el tipo de interrupción que podría causar en el negocio se llama:
    Análisis de impacto de negocio

19. Marque las características que están asociadas al modelo nolan

- **Permite identificar en qué fase de crecimiento TI estamos**
- **Permite valorar el grado de madurez en el uso de las TI en una organización**
- **Permite mejorar la inversión en proyectos de TI a partir de crecimiento que se ve**

20. Asocie correctamente función o responsabilidad con la unidad de dirección de TI:

- Realizar un monitoreo de los servicios de red que brindan el área usuaria = **Operaciones**
- Establecer criterios de aceptación de riesgos en el manejo de información = **Auditoria de sistemas**
- Diseñar una arquitectura de seguridad de profundidad para la empresa = **Seguridad de la información**
- Implementar y configurar equipos de red perimetrales acordadas a una política definida = **Telecomunicaciones y rede**
- Acreditar y adecuar aplicaciones de negocio a ser instaladas en la empresa = **Desarrollo y mantenimiento**

1. Pilares del gobierno de TI

alineación estratégica, Entrega de Valor, Administración de Riesgos, Administración de Recursos, Medición del Desempeño

2. Diferencia entre la planificación táctica y estratégica

   El tiempo de entrega de las soluciones a las necesidades

   planificación táctica: es a corto plazo es más operativa

   planificación estratégica: es a largo plazo

3. El gobierno de TI es responsabilidad de la alta gerencia y dirección de las empresas.

   IT gobernante no es lo mismo que IT management

   en IT managenet administramos equipamiento, configuraciones de Sistemas Op, Redes, Desarrolladomos.

4. ¿Cuáles son los efectos de TI_?

   Mayor entendimiento de las areas

   La justificacion de inversiones

   Dpto de TI tiene un rol protagonico en la Organizacion

   Menor riesgo, mayor control

5. Cobit esta orientado al negocio lo que quiere es reducir la brecha entre lo que quiere la empresa y lo que quiere los del area de TI

   El modelo Cobit tiene 4 grandes fases o ciclo de vida del uso de control

   Implementación

   Revisión

   Corrección

   garantizando la Seguridad, Confiabilidad, Conformidad y cumplimiento.

6. Características de cobit

   está orientado a negocios

   orientado a procesos

   Basado en controles

   Impulsado por medición

7. El objetivo de control el efecto que se quiere alcanzar aplicando control que se quiere lograr con el control

y el objetivo de control es independiente de la tecnología

1. La materialidad de la evidencia en una auditoria se refiere a:

Comprueba un riesgo prioritario de la auditoria (Correcto)

2. Si se decide proteger a través de un IDS de host a sistemas críticos es porque se quiere garantizar principalmente:

La Integridad

3. Complete usando el elemento correcto

Las **Amenazas** aprovechan las **Debilidades** para generar **Riesgo** de robo, perdida o daño en los **Activos informáticos**, el mismo que puede ser prevenido o reducido con los **Controles** que a su vez pueden tener **Vulnerabilidades**.

La Gerencia **Protege** sus activos informáticos porque generan **Valor**

4. El riesgo inherente es aquel que

Existe sin control definido

5. Si el control está bien establecido en un sistema de información de tal manera que el nivel de riesgo se bajó, entonces abra que realizar menos pruebas sustantivas

Verdadero

6. Cuales son características del control interno

Correctivo ● Preventivo continuo

7. COBIT trata a la informacion como el resultado de la aplicación en combinación de los recursos de TI que se gestiona a traves de:

Procesos TI

8. COBIT tiene 4 caracteristicas principales: enfocado a negocios, orientado a procesos, basado en controles y la otra es:

Impulsado por mediciones

9. Cual de los siguientes es un requerimineto de seguridad

Disponibilidad

10. COBIT es un:

Marco y una base de conocimiento para los procesos de TI y su Gestion

11. Cual de las siguientes es un problema común que se encuentra al tratar de alinear las TI y el negocio

Brechas en la comunicación entre negocios TI

12. Cual de los siguientes es un recurso TI identificado por COBIT

Personas

13. Para satisfacer los requerimientos del negocio, la informacion debe ajustarse a ciertos criterios, COBIT se refiere a:

Criterios de Informacion

14. Cual de los siguientes es un criterio de Informacion

Eficiencia

15. Ubique correctamente

Elemento a controlar = **el acceso al celular**

Objetivo de control = **Lograr que solo acceda al celular la persona autorizada**

Control = **Sistema de Acceso Basado en Huella Digital**

Sensor = **Sensor de Huella Digital – Subsistemas de toma de Huella**

Grupo de Control => **Sensor de Huella Digital – Subs De Comparacion**

Grupo activante => **Sensor de Huella Digital – Subs de Acceso**

16. Para determinar el nivel de exposición de un activo, es importante considerar los siguientes aspectos

Vulnerabilidades posibles

Amenazas posibles

17. Reglas de filtrado de trafico en un firewall para aislar la red interna de la red externa:

Control técnico

18. Los controles pueden tener RIESGOS que a su vez pueden ser mitigados por CONTROLES Básicamente existen tres estados en los cuales evaluamos el impacto de un riesgo:
    Riesgo sin control Riesgo con control
19. La técnica manual de recolección de evidencia que no requiere que el auditor sea un experto en el tema y aun asi pueda aplicar en su auditoria es:

Checklist

20. En el modelo de Nolan si los demandantes de TI son:

USUARIOS y APLICACIONES los proveedores de TI son RECURSOS DE TI y PLANIFICACIÓN Y CONTROL (GERENCIAMIENTO)

21. La fase de crecimiento NOLAN en la se aplica la adopción de estándares, un sistema global, tecnologías que permitan la centralización es la fase de

INTEGRACIÓN

22. Escoger una de las siguientes herramientas e indique que evidencia técnica que resulte material podría proporcionar en caso de una auditoria de sistemas

Lvnis La evidencia que nos otorga son amenzas, debilidades

23. Tipos de controles

Control de tipo retroalimentación

Control correctivo

Control de secuencia abierta

Control selectivo

24. Que se refiere BIA (análisis de impacto de negocios) o en que se basa

bia es la guia que determina que necesita ser recuperado y el tiempo que tardará de dicha recuperación

25. cuáles de los siguientes activos tendría mayor valor para una empresa

Información

26. Desde el punto de vista de la jerarquía que ocupa en una organización un sistema de control gerencial permite

Planeamiento táctico

27. En cuanto a las normas gerenciales para hacer auditoria esta la de relación organizativa esta se refiere a

Completar de manera objetiva

28. Asocie riesgos con procesos de TI

Perdida de inforacion por falta de respaldo => **DS4**

Robo de Equipo informatico => **DS12**

Falta de puntos de restauración ante problemas con modificaciones realizadas => **DS9**

29. cuál sería la ecuación que mejora se aplicaría en el caso de proyectos de TI con retorno de inversión 3 o 4 periodos

$$ROI = \frac{\sum_i VAN(BN_i) - Inversion}{Inversion}$$

30. Las tres dimensiones de COBIT son:

Procesos, Recursos de TI, y Criterios de Información

31. Cuál de los siguientes activos informáticos tiene mayor valor para una empresa:

Información almacenada

32. Cuál de los siguientes modelos podría establecerse antes de usar COBIT en una empresa considerando que COBIT está más orientado al control.ISO27002

ITIL

33. Existen dispositivos de red y conexiones de red que no están protegidas y se encuentran en áreas de circulación del personal y clientes, lo cual da lugar a que fácilmente puedan ser violados por personas extrañas a la organización o los mismos empleados. El valor comprometido es

Integridad

34. De las siguientes actividades, seleccione la que no pertenece a un proceso de auditoría de sistemas:

Implementar controles definidos

35. Una persona extraña, logró entrar a un curso o aula virtual del ecampus, dado que el código de acceso fue divulgado. EL valor comprometido es:

Confidencialidad

36. Un programador de sistemas de la empresa ha cometido fraude a través de un código oculto en un programa, del cual también es usuario. El valor comprometido es

Autenticidad

37. Si en un sistema informático definimos un nivel de acceso para cada usuario del sistema (esto quiere decir que el usuario solo puede acceder a las funciones e información permitidas), es porque se quiere garantizar la

Confidencialidad

38. Dominio Cobit donde todos los procesos deben evaluarse de forma regular en cuanto al cumplimiento de los objetivos de control:

ME

39. Asocie correctamente:

Un conjunto de buenas prácticas para mejorar la calidad de los servicios de TI através de un ciclo de vida => **ITIL**

Un conjunto de objetivos de control para la seguridad de la información de manera corporativa => **BMIS**

Estándar genérico para la gestión de riesgos => **ISO31000**

Un conjunto de controles para los procesos de TI a través de un ciclo de vida => **COBIT**

Un estándar para la gestión de riesgos de seguridad => **ISO27005**

Estándar certificable => **ISO27001**

40. Cuál de los siguientes modelos debería implementarse antes que los demás considerando sus características

ITIL

41. En que situación de las mostradas, es mas difícil encontrar los elementos del sistema de control : sensor, grupo de control, y grupo activante

Cuando se trata de controles preventivos preestablecidos

42. Complete: Para la amenaza [**suplantación de identidad**] , una vulnerabilidad podria ser :[**descubrimiento de contraseñas de acceso al perfil**] , que iria en contra del valor de [**autenticidad de la información**], [**falsificando la identidad**] de la persona.

43. El grupo de control: Es el que determina el desvío respecto al valor o condición deseada del elemento a controlar y define las medidas correctivas

44. En la programación de a pares, un programador puede probar el código del otro y viceversa, ese es un ejemplo de control de secuencia

Abierta

45. Son características del Gobierno de TI

El alineamiento estratégico.,

La medición y control del desempeño,

La generación de valor en el uso de TI

46. Cuáles son características del Control Interno:

Es continuo,

Es preventivo,

Es externo a las funciones a auditar

Tema 3

1. Proceso de Auditoria de Sistemas de información

CARTA DE AUDITORIA:

2. Contrato de Auditoria: Es el elemento que define el principal OBJETIVO

de la auditoria el

ALCANCE: Hasta donde llega la auditoria, que procesos, que sistemas que procesos, etc.

3. la OBLIGACION DE RENDIR CUENTAS: Está relacionado con los informes que el auditor va a

presentar

AUTORIDAD: Consiste en darle acceso al auditor a todos los elementos como ambientes sistemas documentos, etc. Este permiso lo concede el que tiene mayor poder

RESPONSABILIDADES: Tiene que ver con lo que puede hacer el auditor, hasta dónde puede llegar el auditor, también lo controlan al auditor.

4. CICLO DE VIDA de una AUDITORIA:

PLANEACION: se trata de encontrar las áreas más importantes en función a los riesgos mas importantes.

PROGRAMA DE AUDITORIA: Es básicamente un plan detallado de la planeación donde se define

- **Objetivos**
- **Alcances**
- **Procedimientos de auditoria: estos procedimientos son los más importantes son los procedimientos que el auditor va a realizar sobre los diferentes elementos ya sea sistemas, equipos, BD. Son esos procedimientos de inspección que realiza**

RECOLECCION DE EVIDENCIA: En esta fase se expone los conocimientos técnicos que pueda tener el auditor, el resultado de la recolección es obviamente la EVIDENCIA (informes BD, capturas de pantallas, videos, entrevistas, etc.).

A partir de la evidencia se tiene que encontrar cuales son las

EVALUACION FORTALEZAS Y DEBILIDADES DEL CONTROL: Que tan bien está definido el control y que debilidades hay. Para este punto es muy importante el análisis de la evidencia.

Una vez realizado esto se elige de manera OBJETIVA, demostrables se elige los hallazgos más importantes rescatamos las fortalezas más importantes y se critica de manera constructiva las debilidades y esto es el INFORME de AUDITORIA

INFORME de AUDITORIA: entonces este informe vendría a ser las cosas que están bien, las cosas que están mal y todo esto respaldadas.

MONITOREO: Después de un tiempo el auditor puede hacer un monitoreo, incluso este monitoreo puede dar lugar a una nueva auditoría o mejorar los controles establecidos

AUDITORIA BASADA EN RIESGOS

MODELO ISO 27005

TRATAMIENTO DEL RIESGO

OPCIONES DEL TRATAMIENTO DEL RIESGO:

Reducir el riesgo: Minimizar con los controles.

Retener el riesgo: es postergar el tratamiento, para un futuro.

Evitar el Riesgo: tratar de ir por otra vía evitando el riesgo.

Transferir el riesgo: Que otros tomen el riesgo por mí.

METODO DELPHI

Metodo para cuantificar los riesgos

Video parte 2

EVIDENCIAS

Las evidencias pueden tener las siguientes cualidades:

Ser Suficiente:

Ser Relevante:

Ser competente Confiable:

Una evidencia puede ser más confiable que otra:

Independencia del que provee la evidencia

Credenciales del que provee las evidencia

Objetividad

Tiempo de evidencia disponible

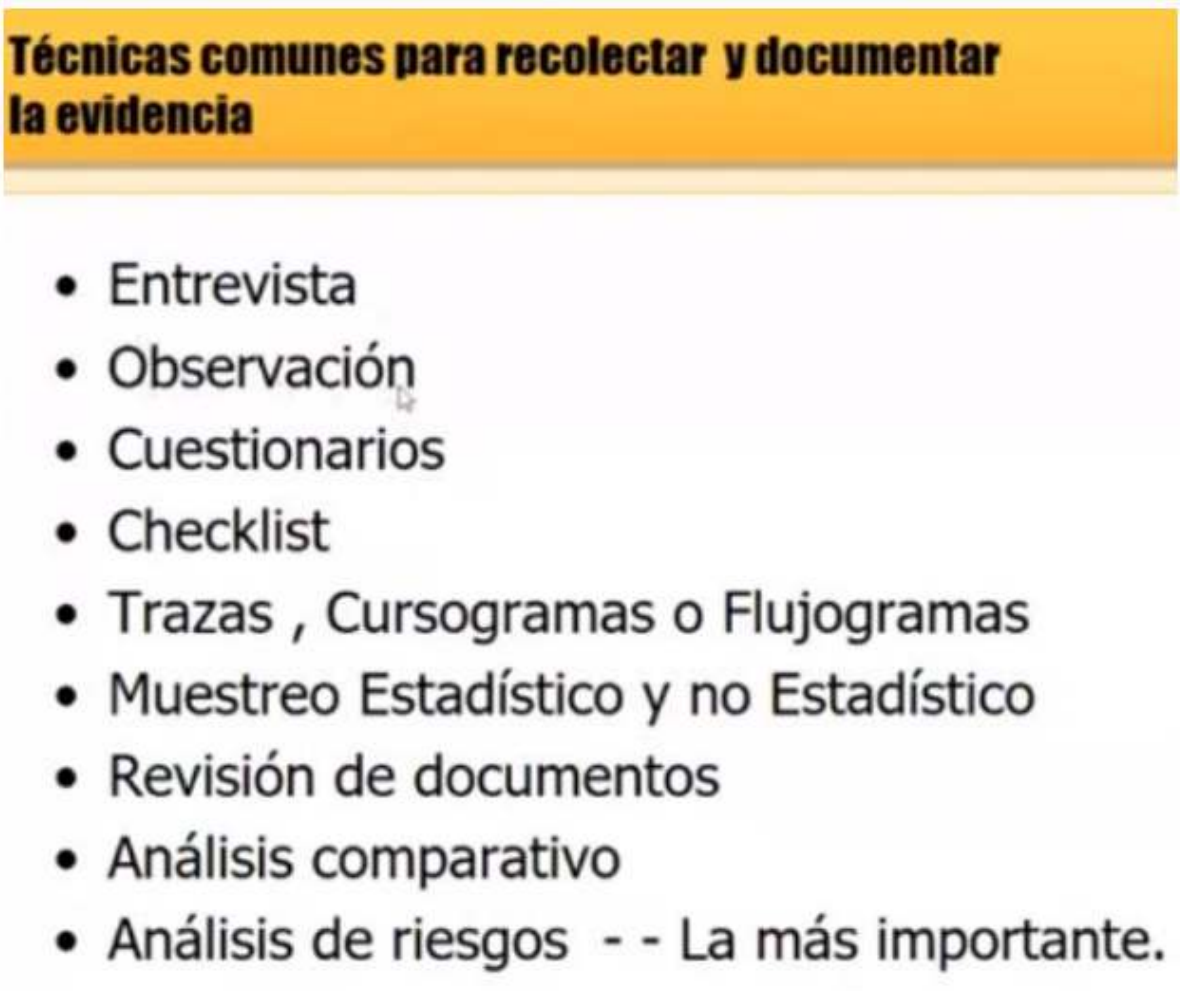
Pruebas de Cumplimiento**: Son pruebas a los controles que están definidos, revisión de informes, checklist.** Aquellos que comprueban los controles**.**

Pruebas sustantivas: Son las pruebas que rompen las reglas, el muestreo de variables,

Análisis de la integridad de la base de datos.

Pruebas de validación de entrada de datos.

Técnicas comunes para recolectar y documentar la evidencia



Video parte 3

Valoración de Amenazas

STRIDE: Te permite valorar las amenazas dándote 6 elementos :

Spoofing: Engaño o falsificación. En contra de la autenticidad.

Tampering de BD: Modificación de la información original de manera no autorizada.

Repudio o negación: Borrar registros, Borrar cosas que ayudan a saber que paso

Información Disclosure: En contra de la confidencialidad

Denegación de Servicios: en contra de la Disponibilidad

Escalamiento de privilegios:

DREAD: es otra forma de cuantificar los riesgos al igual que Delphi