1. Contrato de locación. Si se puede realizar y que ventajas y desventajas tiene para trabajadores freelance.
Si se es freelance, el contrato de locación debe estar a nombre de uno. La ventaja es que se puede elegir un lugar adecuado dependiendo de las necesidades y se pueden trasladar los costos del lugar a los costos de producción que se cobren al cliente, pero la desventaja es que es uno el que debe hacerse cargo de pagar impuestos, servicios y alquiler, por lo que, si en algún momento se pierde la fuente de trabajo y el contrato de locación esta aun en vigencia será un gasto innecesario pero obligatorio, ya sea cancelarlo o seguir pagando a pérdida hasta que se encuentre otro trabajo.
Otra de las ventajas para un trabajador freelance de tener un lugar especial para trabajar es que no mezcla el ambiente familiar con el de trabajo, evitando distraerse y trabajar fuera de horario frecuentemente.
La empresa podría alquilar una oficina para que sus empleados no deban trasladarse hasta la sede central. En este caso se trata de teletrabajo y es la empresa quien se hace cargo. Probablemente esta modalidad no se ofrezca a un trabajador freelance, ya que lo que la empresa busca en esos casos es disminuir sus costos fijos.

2. Que recomendaciones darías para evitar el phishing en un acceso web.
Recomendaría no enviar datos privados (contraseñas o números de cuenta) como respuesta a emails que los soliciten espontáneamente. Si se está navegando en internet, antes de introducir datos privados debe verificarse que la pagina este siendo transmitida utilizando protocolos seguros, como HTTPS, con certificados de seguridad válidos y que la dirección sea la correcta. También debe verificarse que los links a los que se acceden sean a la página oficial del sitio al que supuestamente accedemos.

3. Teletrabajo, definición y ventajas y desventajas para ambas partes.
Es el trabajo que se realiza fuera de la oficina principal de la empresa, incluyendo oficinas externas más cercanas a la residencia de los trabajadores, oficinas móviles o en sus casas.
Las ventajas para el trabajador son:
- Menos o nulo tiempo de viaje a la oficina.
- Flexibilidad horaria
- Mayor tiempo con su familia

La ventajas para la empresa son:
- Menos costos fijos
- Menos problemas entre compañeros de trabajo
- No se necesita una oficina grande

Las desventajas para el trabajador son:
- Aislamiento
- Desmotivación
- Dificultad para concentrarse si trabaja fuera de un ambiente laboral

Las desventajas para la empresa son:
- Menor control sobre los empleados y el uso que hacen de los recursos de la empresa
- Menor fidelidad de los empleados

4. Conversión y que método aplicarías si es un equipo de gente con experiencia y disposición la cambio. Defina las actividades por parte del auditor.
La conversión se da cuando se migra de un sistema a otro más nuevo. Para gente con experiencia, lo ideal sería hacer una instalación en paralelo para reducir los riesgos de migración e ir probando el sistema nuevo teniendo al viejo como alternativa por si algo falla. Al tener experiencia se supone q los usuarios podrán adaptarse rápidamente al nuevo sistema sin mayores inconvenientes e identificar sus fallas a medida que ocurran.
Los auditores deben prestar atención a la administración del proceso de cambio y evaluar cuáles serían los riesgos si la instalación fuese abrupta. Deben planificar y controlar cuidadosamente las tareas de conversión, y al finalizar ajustar los controles, ya que se relajan durante el proceso.

5. ACM, nombrar los principios y explicar cuál es el espíritu de cada uno. Dar ejemplos de situaciones no ilegales que los violen.
- Interés público: Actuar de acuerdo al interés público.
  - *Espíritu: El trabajo que se realice no debe ir en contra de la vida de otras personas, su privacidad o al medio ambiente.*
  - *Ejemplo que lo viola: Empleados de empresas armamentistas, mineras o fabricantes de OGM que ayudan a su funcionamiento.*

- Cliente y empleado: Actuar de manera que esté de acuerdo con los intereses de sus clientes y empleadores consistentemente con el interés público.
  - *Espíritu: Al punto anterior, agrega que no debe perjudicar a su empleador ni clientes.*
  - *Ejemplo que lo viola: Empleados que antes de abandonar una empresa copian datos de contacto de clientes para uso personal.*
- Producto: El producto debe alcanzar los estándares más altos posibles.
  - *Espíritu: El buen trabajo de un profesional de IT, o grupo de estos, puede beneficiar el concepto que se tiene del resto de los trabajadores, incluso simplificar el trabajo del resto.*
  - *Ejemplo que lo viola: Microsoft lanza al mercado sistemas operativos con fallas sabiendo que tiene al mercado cautivo.*
- Juicio: Mantener la integridad e independencia en el juicio profesional.
  - *Espíritu: Un trabajador de IT no debe dejarse "comprar" para realizar tareas que no están de acuerdo con sus creencias, convicciones y el bien público.*
  - *Ejemplo que lo viola: La gerencia pide a un empleado de IT que instale en todas las PC de la empresa un software que monitorea y registra todo lo que los empleados hacen, texto que escriben y aplicaciones que abren, violando su privacidad.*
- Gestión: Los directores de proyecto deben suscribirse a un manejo ético de desarrollo y mantenimiento del software.
  - *Espíritu: El desarrollo y mantenimiento debe hacerse de la mejor forma posible, tanto para con los empleados que trabajan en él como con el producto en sí.*
  - *Ejemplo que lo viola: Directores de proyecto que exigen a los desarrolladores por sobre lo estipulado en los contratos porque no llegan a entregar un trabajo a tiempo.*
- Profesión: harán progresar la integridad y reputación de la profesión consistentemente con el interés público.
  - *Espíritu: Actuar de forma tal que genere confianza de la sociedad con los profesionales de IT y su trabajo, ya que como representante del sector, un trabajador de IT puede influir en la opinión que la gente tenga.*
  - *Ejemplo que lo viola: Técnicos que cobran a sus clientes pero no proveen soluciones reales a los problemas.*
- Colegas: Serán justos y proveerán soporte a sus colegas.
  - *Espíritu: Todos deben colaborar para elevar el nivel de servicios que pueden brindarse.*
  - *Ejemplo que lo viola: Saber la respuesta a una pregunta plateada en un foro de informática y no contestarla.*
- Aprendizaje: Participaran en un aprendizaje de por vida de su profesión y promoverán el acercamiento a la misma.
  - *Espíritu: La computación es una disciplina que avanza rápido y en la que constantemente surgen innovaciones con las que es fundamental mantenerse al día.*
  - *Ejemplo que lo viola: Programadores que no desean aprender lenguajes nuevos y continúan utilizando lo que aprendieron cuando eran jóvenes, dando como resultado sistemas de software obsoletos desde su concepción (Corren solo en DOS), justificando su realización solo en que son livianos y "andan".*

6. Sistemas de control. Que tipos hay y dar ejemplos de los mismos.

Son políticas y procedimientos manuales o automatizados que detectan, previenen, reducen y corrigen riesgos para asegurar que los objetivos de negocio serán alcanzados. Los 5 tipos son:

1- Evaluación de entorno: Pueden ser realizados mediante un comité de seguimiento de proyectos. Se evalúan:
- *Controles de sistemas y procedimientos*
- *Monitoreos de performance*
- *Filosofía de gerenciamiento y operación*
- *Asignación de responsabilidades.*

2- Evaluación de riesgo: También puede ser realizada mediante un comité de seguimiento de proyectos, en las planificaciones del mismo o en un documento aparte. Se evalúan elementos que identifican, analizan y administran los riesgos.

3- Actividades de control: Se evalúan elementos:
- *Administrativos, que aseguran eficiencia, eficacia y la actualización de documentos y registros.*
- *Contables, que aseguran distintos niveles de autorizaciones y responsabilidades.*

4- Información y comunicación: Se evalúan elementos que identifican, capturan e intercambian información para verificar que lo hagan en tiempo y forma, como notificaciones o resúmenes de reuniones. Permiten asignar responsabilidades al personal adecuadamente.

5- Monitoreo: Se evalúan elementos que aseguran que los controles internos operan confiablemente en el tiempo, como controles de calidad y performance.

7. Definir "Patentes de software" ¿Es posible patentar un programa?

El software puede patentarse pero, a diferencia de una patente común que se aplicaría a un programa, lo que se patenta es la idea de hacer algo. Son un capital para quien las posee pero un riesgo para otros, ya que cualquiera deberá pagarles por implementar algo que use esa idea y, cuando se trata de metodologías muy comunes, se podría estar actuando ilegalmente

sin intención. También son un obstáculo para el software libre, ya que no se poseen recursos económicos para pagar los derechos de uso. En general no suelen utilizarse, es más común el uso de los distintos tipos de licencia.

8. ¿Cuál es la ventaja de hacer un contrato de servicio para un trabajo? Siendo usted un programador independiente al que se lo contrata de una empresa extranjera para hacer una página web, ¿puede realizar un contrato de servicio? ¿Cómo se realiza?

La ventaja de hacer un contrato es que se tiene una especificación detallada de cómo será la relación entre las partes y como se procederá en caso de irregularidades.

Cuando se realiza un trabajo a distancia para una empresa extranjera, trabajando como freelance, se puede hacer un contrato de servicio, tomando las leyes de alguno de los dos países como referencia. Generalmente la empresa intentara regirse por las leyes del país que más la beneficien, aunque el trabajador podría intentar que no sea así, ya que esto debe acordarse por ambas partes.

9. Describir componentes principales de Plan de Backup y del de Recuperación ¿Qué controles debe llevar a cabo el auditor en cada uno? Explicar que se debe tener en cuenta a la hora de elegir el lugar de almacenamiento y cuál es la diferencia entre hot-site y cold-site.

Un Plan de Backup incluye:

- Tipos de backup a mantener
- Frecuencia de ejecución
- Procedimientos
- Ubicación de los recursos

Plan de recuperación:

- Sitio donde restaurar
- Operaciones para restaurar
- Personal responsable
- Prioridades para recuperar los sistemas y cronograma

Se debe controlar que el plan se actualice permanentemente, ya que el personal, hardware y software disponible va cambiando. La mayor dificultad es asegurar que todos los recursos críticos están resguardados.

Tipos de Sitio:

- Cold Site: No está en línea permanentemente, pero tiene el espacio para INSTALAR los equipos necesarios. Puede ser de la misma organización o contratado. Es adecuado solo si la organización tolera un tiempo sin sistema.
- Hot Site: Son compartidos y en ellos se guardan el software, hardware, datos e insumos. Todo el hardware y el espacio está disponible todo el tiempo, lo que los hace caros de mantener.

10. Explique las propiedades deseables de un sistema de cifrado. ¿Cómo se clasifican según su simetría? ¿Cuál de estas categorías se usa en e-commerce? ¿Por qué?

Los algoritmos están estandarizados y publicados, pero se ocultan las llaves, que son parte de la entrada del algoritmo.

Si se usa la misma llave para encriptar y desencriptar el algoritmo es simétrico, sino es asimétrico.

Los simétricos tienen una llave privada y los asimétricos un par de llaves publica/privada, en los que, cuando una encripta la otra desencripta y viceversa. Si encripto lo hago con mi llave privada y si me quieren enviar un mensaje encriptan con mi llave pública.

En el caso de e-commerce se requiere mayor seguridad que en otros servicios ya que hay recursos económicos en juego. Se utiliza un cifrado asimétrico y se aumenta la seguridad con el uso de certificados y firmas digitales. Para esto:

- El emisor calcula el hash, que se encripta con la clave privada del emisor para crear la firma digital.
- El emisor codifica el hash calculado con el mensaje usando la clave pública del receptor y lo envía junto con la firma.
- El emisor también envía un certificado digital, que contiene su clave pública.
- El receptor recibe el mensaje y lo decodifica con su clave privada
- El receptor recalcula el hash del mensaje y lo compara con el hash recibido para verificar integridad.
- El receptor obtiene el certificado digital del emisor y usa la clave pública que contiene para obtener el código hash codificado en la firma digital, el cual compara con el código hash recibido en el mensaje.
- El receptor compara la clave pública de la firma digital con la del certificado digital para evitar impostores.

11. ¿Cómo se clasifican los controles de acceso sobre Bases de Datos? Explicar su diferencia. Para cada uno de los enfoques, de un ejemplo de una Base de Datos basado en ese esquema de trabajo.

Un mecanismo de control de acceso se usa para hacer cumplir una política de control de acceso. Existen dos tipos:

- Políticas Discrecionales
  Los usuarios especifican quién puede acceder a sus recursos mediante una matriz de autorización, donde las filas son los usuarios, las columnas los

recursos y el contenido de la celda el privilegio del usuario para ese recurso. Ellos pueden agregar filas que representen recursos que han creado, pero sólo el administrador podrá borrar filas y columnas de la matriz.
Esta política se utiliza para que usuarios con permisos asignen permisos de consulta o modificación (depende del nivel de permisos que tengan) sobre vistas o tablas a otros usuarios utilizando la sentencia GRANT.

- Políticas Mandatorias
  Provee menor flexibilidad. A usuarios y recursos se les asignan atributos de seguridad fijos que solo el administrador puede cambiar y que no son transferibles a sus pares.
  Estas políticas se utilizan en sistemas jerárquicos, como los gubernamentales o los militares ya que proporcionan mayor control.

12. Nombrar 5 principios de ISACA y describir su espíritu

- Favorecer el cumplimiento de estándares, procedimientos y controles.
  Espíritu: La estandarización simplifica el trabajo cuando varios profesionales trabajan en un mismo proyecto, y los controles intentan maximizar la confiabilidad del sistema.
- Trabajar con diligencia y cuidado profesional de acuerdo con los estándares y mejores prácticas.
  Espíritu: Cuidar la imagen que se tiene del profesional de IT para que se valore la disciplina correctamente.
- Servir al interés de los stakeholders en forma legal y honesta manteniendo altos estándares, con conducta y carácter.
  Espíritu: Actuar de acuerdo con los intereses de quien contrata al profesional respetando el bien público.
- Mantener la confidencialidad de la información obtenida durante el trabajo a menos que sea requerido por una autoridad competente. La información no puede ser usada para beneficio personal.
  Espíritu: No abusar de los permisos que se le otorgan al personal de IT obteniendo información que no quiere ser divulgada para que el empleador no pierda la confianza.
- Ser competentes en los campos de trabajo y sólo acceder a realizar aquellas actividades que pertenezcan a las áreas de competencia.
  Espíritu: No cometer errores que puedan perjudicar el resultado final y a la imagen del profesional de IT por no saber cómo realizar el trabajo.
- Informar a las partes apropiadas sobre los resultados del trabajo realizado, incluyendo todos los hechos relevantes.
  Espíritu: Dejar registro para futuros profesionales que los requieran, o para uno mismo en el futuro, para no repetir errores o repetir buenas practicas.
- Promover la educación de los participantes para mejorar su entendimiento y control de la seguridad de SI.
  Espíritu: Si un cliente o empleador entiende mejor cómo funcionan los SI, cobra más valor el rol del profesional de IT ya que pueden comunicarse recomendaciones y problemas encontrados con mayor claridad.

13. Nombrar controles asociados con el manejo de personal, identificar distintas categorías para estos.

Controles de Selección de Personal

Al elegir nuevo personal se deben tener en cuenta:

- *Referencias*
- *Salud física y mental*
- *Obligaciones contractuales*
- *Doctrinas de la organización*
- *Acuerdos de confidencialidad*
- *Explicación de protocolos organizacionales. (Ej.: confidencialidad, cuidado de equipos)*
- *Códigos de ética*
- *Acuerdos de conflictos de intereses*

Controles de Desarrollo del Personal

Para monitorear el trabajo y determinar medidas a tomar con los empleados:

- *Identificar sus debilidades y fortalezas.*
- *Identificar oportunidades para su crecimiento personal y profesional*
- *Deben estar informados de la evaluación, comprender claramente las reglas de la misma, tener posibilidades de discutirla con su superior y apelar en caso de discordancia.*

Controles de Finalización de Servicios

Cuando un empleado se va, voluntaria o involuntariamente, la alta gerencia debe ser informada de inmediato, su supervisor debe reportar las razones que llevaron a esto y además:

- *Recuperar llaves, tarjetas de identificación y pertenencias de la empresa que se le hayan dado*
- *Cancelar claves de acceso*
- *Modificar las listas de distribución*
- *Si el empleado no está descontento, debe capacitar a su reemplazo.*
- *Si está descontento se lo debe separar de las áreas críticas y pedirle que abandone la organización cuanto antes.*

14. Plan estratégico y plan operacional, nombrar 3 cosas que debe cubrir cada uno

El plan operacional cubre los próximos 1 a 3 años:

- *Informes de avances*
- *Iniciativas a tomar*
- *Cronograma de implementación*

El plan estratégico cubre los próximos 3 a 5 años:

- *Evaluar la información actual*
- *Direcciones estratégicas*
- *Estrategia de desarrollo*

15. Definición de COBIT, sus dominios y cuando sería adecuado aplicarlo en una Pyme.

"Control OBjetives for Information and related Tecnology": Analiza si IT se alinea con los objetivos del negocio. A través de dominios y procesos, busca desarrollar y promover un marco de control de gobierno de IT actualizado y aceptado internacionalmente. Se organiza en cuatro dominios:

- *Planear y organizar (PO): Estrategias para identificar como la IT puede contribuir a los objetivos de negocio.*
- *Adquirir e Implementar (AI): Identifica, adquiere y mantiene software y hardware, administra los cambios y facilita el uso de nuevas tecnologías.*
- *Entregar y dar soporte (DS): La entrega o prestación de los servicios, administración de la seguridad y continuidad, el soporte a los usuarios, la administración de los datos e instalaciones operativas.*
- *Monitorear y evaluar (ME): Los procesos de IT deben evaluarse en cuanto a calidad y cumplimiento de los controles. Abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.*

Se debe aplicar a una Pyme si la empresa creció al punto en que necesita un soporte IT mas organizado o si es una empresa que está comenzando a utilizar IT para soporte de sus operaciones.

16. Procedimientos a seguir cuando se hace una auditoria externa en una empresa que no tiene planificación. La empresa es de tipo estratégica según McFarland.

Si la empresa es de tipo estratégico, es porque sus sistemas informáticos actuales y a futuro son críticos. Las actividades que realizara el auditor serán:

- *Planificar la auditoria*
- *Evaluar riesgos en general y para cada área y aplicación.*
- *Desarrollar un programa de auditoría con objetivos y procedimientos para resguardar los sistemas actuales y planificar los futuros.*
- *Recolectar evidencia*
- *Evaluar las fortalezas y debilidades basándose en la evidencia.*
- *Preparar un reporte presentando las debilidades, las recomendaciones para remediar los problemas y un plan a futuro para los sistemas.*

17. ¿Para qué sirven los estándares y procedimientos de ISACA? ¿Cuál es la diferencia? Nómbrelos y explique de qué se tratan.

Estándares: Su objetivo es hacer que los auditores tengan un nivel mínimo de performance para garantizar que se cumplan las expectativas de la gerencia en cuanto a la calidad del trabajo. Definen requerimientos para las auditorías:

S1: Audit Charter
Un documento aprobado a un nivel adecuado que contiene el propósito, responsabilidad y autoridad del auditor.
S2: Independencia
Entre quien audita y quien es auditado.
S3: Ética profesional
El auditor debe adherir al código de ética ISACA y a las normas profesionales.
S4: Competencia
Debe tener el conocimiento para realizar la tarea asignada y educarse continuamente.
S5: Planificación
Planificar para cumplir los objetivos respetando leyes y estándares. Desarrollar y documentar un acercamiento basado en riesgos y un plan de auditoría.
S6: Performance
Se debe supervisar al staff, recolectar evidencia y documentar el trabajo.
S7: Reportes
Se refieren a los tipos de reportes, medios de comunicación y a la información comunicada
S8: Seguimiento
Evaluar si se han tomado las acciones apropiadas de acuerdo a lo recomendado.
S9: Irregularidades
Concierne como lidiar con irregularidades y actos ilegales.
S10: Gobernanza
Evaluar si las políticas de IT se alinean con los objetivos de la organización, los controles y riesgos asociados.
S11: Riesgos
Usar un acercamiento basado en riesgos para la planificación de prioridades en el uso de los recursos.

Procedimientos: Son ejemplos que el Auditor de Sistemas puede utilizar en una revisión. Informan cómo cumplir con los estándares al auditar pero sin especificar requerimientos:

P1: Evaluación de riesgo
P2: Firmas digitales
P3: Detección de intrusos
P4: Virus
P5: Autoevaluación de control de riesgos

P6: Firewalls
P7: Irregularidades y actos ilegales
P8: Evaluación de seguridad
P9: Evaluación de métodos de encriptación.
P10: Control de cambios de aplicaciones empresariales
P11: Transferencia electrónica de fondos.
Para administrar la complejidad, se sugiere Factorizar el sistema en subsistemas y determinar su confiabilidad por separado y sus implicancias a nivel general.

18. Nombrar controles aplicables al desarrollo y el riesgo que mitigan.

Riesgos:

a- Decisiones erradas de la gerencia
b- Registros inexactos
c- Interrupción del negocio
d- Fraudes
e- Violación de leyes
f- Costos operativos excesivos
g- Objetivos no alcanzados

Controles en el desarrollo y riesgos que mitigan:

- *Methodology (SDLC) -> a, c, f, g*
- *Políticas de contratación -> d, e, f*
- *Entrenamiento -> e, f, g*
- *Revisiones técnicas -> c, f, g*
- *Participación en las auditorías ->a, b, d, e, g*
- *Testeo de los sistemas -> c, d, f, g*
- *Revisiones post-implementación -> a, c, d, f, g*
- *Documentación ->b, d*
- *Revisiones de Cronogramas ->a, g*
- *Asignación de trabajos -> c, f, g*
- *Monitoreos de performance -> a, c, f, g*
- *Monitoreos y reportes de estado ->b, d, f, g*

19. Suponga que debe auditar un sistema de bases de datos cliente-servidor. ¿A qué le prestaría más atención?
-a- Disponibilidad de las aplicaciones del S.O.
-b- Documentación sobre la seguridad
La opción "b" es más importante en el contexto de la auditoria, ya que la DB podrían estar en peligro. En el caso "a", aunque podría darse que los datos no estén siempre disponibles y se entorpezca la actividad laboral, no peligra toda la información.

20. Al auditar un mecanismo de control de acceso de bases de datos, se percata de que este se encuentra embebido sólo en el subsistema de bases de datos, sin que el sistema operativo provea mecanismos adicionales. ¿Qué opinión daría como auditor en este caso?
No es correcto ya que un posible usuario malintencionado podría acceder desde el sistema operativo sin autenticarse y copiar, eliminar o corromper la base de datos por fuera del subsistema. Deberían implementarse políticas de acceso desde el sistema operativo para complementar a los del subsistema de BD.

21. ¿En qué consisten las políticas de una organización? ¿Y los manuales de procedimientos? ¿En qué se diferencian?
Las políticas son lineamientos generales y teóricos de las normas por las cuales la organización se rige que son dictadas por la jerarquía más alta de la empresa. Por otro lado, los manuales de procedimientos explican paso a paso como realizar procedimientos que siguen e implementan las políticas y son redactados por personas expertas en el tema que tratan.
Las políticas se aplican a procesos, los procesos implementan políticas.

22. Suponga que es el auditor interno de una obra social cuyo sistema de ha vuelto obsoleto. El consejo directivo le encomienda la tarea de decidir si conviene desarrollar un sistema inhouse o tercerizar el desarrollo. ¿Qué elementos debe considerar antes de recomendar un determinado curso de acción?
- Costos de tiempo y económicos de tercerizar y de contratar un equipo de programadores.
- Si la empresa tiene un departamento de IT conformado y con experiencia.

- Menor control sobre el personal cuando se terceriza.
- La empresa con la que se tercerice debe ser de confianza.

23. Defina el concepto de separación de obligaciones. ¿Cuáles son las funciones que pueden ser realizadas por la misma persona sin que sea un problema desde el punto de vista de la separación de obligaciones?
a) Administrador de la seguridad y gestión de los cambios
b) Diseño de sistemas y desarrollo de sistemas
c) Desarrollo de sistemas y mantenimiento de sistemas
Justifique en cada caso su respuesta, sea esta negativa o positiva.
La separación de obligaciones es la división de tareas que hacen a los sistemas dentro de una empresa. Se da para reducir los riesgos por errores en el trabajo de los empleados o los que puedan producirse por empleados malintencionados.
a- No pueden ser realizadas por la misma persona. Los programadores pueden recibir indicaciones que mejoren la seguridad del sistema, pero no participar en ella.
b- Pueden ser realizadas por la misma persona, son actividades complementarias.
c- No pueden ser realizadas por la misma persona. Los desarrolladores deberían estar separados de los datos en producción y de la operación normal del software.

24. Defina el concepto de riesgo en forma general y en concreto de los sistemas de información. ¿De qué forma se clasifican usualmente los riesgos? Explique la naturaleza de cada clase.
Riesgo es la probabilidad de que una amenaza explote las vulnerabilidades de un activo o grupo de activos, causando daño. En informática, consiste de eventos relacionados con IT que podrían impactar en el negocio negativamente y está asociado con el uso, propiedad, manejo, influencia y adopción de IT dentro de la empresa. Clasificacion:
- Riesgo deseado: El riesgo que se desea correr.
- Riesgo inherente: Es la probabilidad de que una pérdida significativa suceda antes de que opere algún factor reductor del riesgo. Para evaluarlo, el auditor debe considerar cuales son los tipos y naturaleza de los riesgos, tanto como los factores que indican que un riesgo existe.
- Riesgo de control: Mide la probabilidad de que los procesos de control establecidos para limitar o manejar el riesgo inherente no sean efectivos. El auditor debe saber cómo medir si los controles son efectivos o no sabiendo qué controles son más efectivos que otros. Controles más fuertes reducen el riesgo pero pueden ser prohibitivos.
- Riesgo de auditoría: Es el riesgo que el cubrimiento no aborde exposiciones del negocio. Se pueden desarrollar programas para reducir este riesgo. Proveen guías sobre que controles sirven para cuales riesgos y los testeos substantivos y de compliance a ser realizados. Deben usarse con cuidado y adaptarse al contexto.