Auditoría de Sistemas 2020
Resumen de ejercicios

1. **El líder de proyecto de la implementación de un sistemas, renunció en el mes previo a la puesta en marcha. Qué acciones debería tomar la gerencia de sistemas con respecto a:**
    a. **La continuidad de las tareas de implementación.**
    b. **Terminación de funciones del líder de proyecto.**
    c. **Adquisición de un nuevo personal para cubrir el puesto.**
    d. **Intentar asegurar la continuidad del resto del staff.**

Respuesta:

Cuando un empleado toma la decisión de renunciar, la alta gerencia debe tener en cuenta el motivo por lo cual realizó esta acción ya que las acciones futuras estarán basadas en esto. Por un lado, la alta gerencia debe ser informada de inmediato y el supervisor del empleado que renuncia debe reportar las razones que llevaron a esto.

- La continuidad de las tareas de implementación:
    - Si el empleado que renuncia no está descontento debe capacitar a su reemplazo, de otra forma, si está descontento se lo debe separar de las áreas críticas y pedirle que abandone la organización cuanto antes.
    - Debe ser llevadas a cabo por el resto del equipo encargado de realizarlas.
- Terminación de funciones del líder de proyecto.
    - Cancelar sus claves de accesos
    - Modificar las listas de distribución
    - Recuperar sus llaves y tarjetas de identificación
    - Devolver libros, documentación, informes y cualquier equipo que esté haciendo uso.
- Adquisición de un nuevo personal para cubrir el puesto:
  A la hora de incorporar nuevo personal para cubrir el puesto la alta gerencia debe hacer las siguientes acciones:
        - Controlar o chequear las referencias del nuevo empleado
        - Seleccionarlo en base a salud física y mental
        - Obligación contractual para clave personal
        - Doctrinas propias de la organización
        - Acuerdo de confidencialidad
        - Explicación de protocolos organizaciones a observar
        - Codigos de etica
        - Acuerdos de conflictos de intereses
- Intentar asegurar la continuidad del resto del staff
    - Evaluar la respuesta del personal ante esta situación
    - Tomar medidas para alivianar la carga de los empleados y redistribuir de manera que sea apropiado.

2. **Una organización está considerando usar un nuevo proveedor de servicios de IT, en particular servicios de hosting de su sistema web. Desde la perspectiva del auditor, cual de los siguientes ítems sería más importante por revisar ? Justifique adecuadamente.**
    a. **Las referencias que otros clientes han brindado sobre el proveedor del servicio.**
    b. **El nivel de seguridad física de las facilidades del proveedor del servicio**
    c. **El service level agreement (SLA) que se firmará con el proveedor.**

Respuesta:

La opción correcta es la c). Justificación: El SLA es una forma contractual de ayudar al departamento de SI a gestionar los recursos de información bajo el control de un proveedor. Comprometen al proveedor a un nivel requerido de servicio y soporte, además establecen tanto los requerimientos de hardware y software, como también las penalidad de opciones de aplicación (enforcement).
Por esta razón, para el auditor, es importante a la hora de monitorear el outsourcing asegurar que se cumplan las condiciones establecidas en el contrato y el SLA.
También que los incidentes sean reportados y gestionados apropiadamente.
Al auditar outsourcing:

- Incorporar que se espera de la calidad del servicio (CMM, ISO, ITIL, etc)
- Reporte incumplimientos y seguimiento
- En el desarrollo asegurar que se incluyan controles de cambios y requerimientos de testeo
- Detallar parámetros específicos de performance
- Un criterio de resolución de conflictos
- Indemnización por daños
- Cláusulas sobre derechos a auditar

3.Suponga que un auditor en sistemas de información está analizando el proceso de desarrollo de software de una organización. ¿Cuáles de las siguientes funciones serían apropiadas para que las desarrollen los usuarios finales y por qué?

a) **Testeo de la salida de los programas**
b) **Especificación de la lógica de los programas**
c) **Ajuste (Tuning) de la performance del sistema**
d) **Configuración del sistema**

Sería apropiado que los usuarios finales participen del **testeo de la salida de los programas** ya que ellos serán quienes los utilicen y pueden brindar no solo opiniones críticas de cómo las salidas son representadas y/o la información o datos que se obtienen con el uso, sino también si se cumple con lo esperado, siempre recordemos que en la mayoría de los proyectos, en la actualidad, se promueve una activa participación de las partes interesadas y los usuarios son una parte importante de ellas. Sabiendo esto lo que podemos hacer para evaluar muchos aspectos del sistema es involucrar a los usuarios finales del mismo. En el caso particular de las salidas del sistema, se puede poner a los usuarios a utilizar o evaluar las diferentes funcionalidades y deducir con esto desde que tan

efectiva fue la captura de requerimientos hasta si el diseño y el desarrollo del sistema fue apropiado para satisfacer las necesidades del cliente.

4. Indique qué principio/s del Código de Ética del ACM es/son violado/s en la siguiente situación y por qué.

Usted es líder de proyecto en la compañía de desarrollo de software "Program". Su compañía está por cerrar contrato con una empresa internacional de gran envergadura ("Importante SRL"), para ser su única proveedora de software, y usted es asignado como responsable del mismo. Una de las condiciones es formar tres equipos de desarrollo compuestos de: Un desarrollador SR, Un desarrollador SSR, un Analista Funcional y un Analista de Testing. Para cada puesto el gerente de sistemas Importante SRL, hará entrevistas técnicas.

Luego de un tiempo, solo queda conseguir un desarrollador SR para uno de los equipos, tarea que se dificulto ya que los últimos 3 entrevistados no fueron aceptados. Usted, como líder de proyecto para Importante SRL, decide grabar una de las entrevistas, para luego poder "entrenar" al próximo entrevistado. Este pasa exitosamente la entrevista, pero gracias a la ayuda que usted le brindó. Al iniciarse el proyecto, el gerente de sistemas de Importante SRL que este último entrevistado no tiene los skills que demostró en la entrevista, y esto genera problemas para la relación a largo plazo entre Importante SRL y Program.

Respuesta:

Cliente y empleador, Producto, Juicio y Profesión

a) **"Grabar una de las entrevistas":**
   - **Ser honesto y confiable:** Como líder de proyecto y profesional, no se estaría siendo transparente. Dado que estaría filmando sin su consentimiento y con el fin de usar ese material para entrenar al siguiente. Es algo que una persona confiable no debería hacer.
   - **Respetar la privacidad:** Está recopilando información personal del entrevistado para luego mostrarla a otra persona (intercambio) sin el conocimiento de la persona filmada, por lo que estaría violando sus derechos. Esto podría culminar en problemas legales para el líder y compañía.

b) "Entrenar" al próximo entrevistado. Éste pasa exitosamente la entrevista, pero gracias a la ayuda que usted le brindó.
   - Relacionado con el Juicio, la Profesión y el producto, buscando una alternativa no ética para contratar a una persona no capacitada para mantener al producto con los estándares más altos posibles. Al involucrarse en el proceso de selección de personal para seleccionar a alguien que no posee los skills requeridos no tuvo en cuenta su juicio y lo hizo de una manera poco profesional.
   - Pasar por una entrevista más allá del resultado, son situaciones que te hacen crecer como profesional. Ganar un puesto debería relacionarse totalmente con la formación, conocimiento y esfuerzo de cada uno, no con ayudas externas. Cometiendo este acto no ético, promueve una reputación negativa hacia nuestra profesión.

- Nuevamente no estaría siendo confiable por buscar una alternativa “fácil” para ocupar un puesto que finalmente generó problemas en la relación a largo plazo con la compañía.

5. Considere una entidad educativa ofrece el dictado de cursos a distancia a través de una plataforma que fue desarrollada para estos fines. La plataforma está instalada en un servidor que está situado en las oficinas de la entidad educativa, en el microcentro de la ciudad de Buenos Aires. La interacción con los alumnos se realiza de forma virtual, en una primera etapa los interesados deben darse de alta como usuarios del sistema, para ello deben ingresar sus datos personales, dar un correo electrónico en el cual recibirán un usuario y contraseña para acceder por primera vez en el sistema; luego de ese primer ingreso deben modificar la contraseña de acceso. Para todas las contraseñas elegidas por los usuarios se requiere que contengan al menos 8 caracteres, un número y alguna letra mayúscula. Una vez realizados estos pasos los alumnos accederán al material de los cursos, la plataforma virtual correspondiente y los exámenes a realizar en el tiempo establecido. Al momento de finalizar el examen la plataforma genera un ticket virtual que será la referencia a tener en cuenta para el seguimiento del mismo. Cabe destacar que para acceder a los exámenes los usuarios deben haber pagado los importes estipulados y el sistema controlará tal situación para habilitar la opción. El pago de estos importes sólo puede realizarse mediante una tarjeta de crédito. Los resultados de los exámenes se reflejarán en el sistema y por cuestiones de privacidad sólo deberían poder ser accedidos por quienes rindieron el examen y por el personal administrativo con los privilegios adecuados. Como auditor, se le solicita:

a) Identificar tres debilidades de control de esta aplicación y establecer el riesgo asociado.
b) Proponer tres controles que usted juzgue serán importante para este contexto. Clasificar estos controles, justificando en que categoría los ubica.

a) Debilidades y riesgos
   - Manejo de contraseña: Se solicita que el alumno ingrese primero todos sus datos sensibles para luego obtener un usuario y una contraseña manejada por un operador de la plataforma lo que permite que estos datos sean accedidos por el operador en el período entre que se cargan los datos y el alumno puede cambiar la contraseña. Esta sería una debilidad en el Control de Inputs, ya que los datos ingresados por el usuario quedan accesibles a un empleado sin su consentimiento, pudiendo modificar estos datos o hacer uso de ellos para un beneficio personal.
   - El pago: Se posee un único y en caso de falla este único método, se inhabilita completamente a un alumno por una falla que lo excede. Este seria una debilidad en el control de autorización, ya que en caso de falla en el único sistema se podría dejar inhabilitado al alumno de cursar y esto es crítico.
   - El acceso a los resultados del examen: Se menciona que se “debería” dar solo acceso a quienes rindieron el examen pero no se menciona que medidas se toma o como realmente se verifica que se de este control de

privacidad. Esta sería una debilidad en el control de autorización, ya que no se valida correctamente o no se asegura de que se valide correctamente a quienes tienen acceso a los resultados. En caso de que cualquier alumno tenga acceso a resultados, no solo se estaría violando la información privada de un alumno sino que además se podría llegar a utilizar esta información para realizar plagios o copia teniendo las resoluciones.

b) Controles a agregar:

- Se debería controlar que la solicitud de información sensible por parte de la plataforma para el alumno se de una vez que el alumno ya ingresó una nueva contraseña y solo él tiene acceso a esa cuenta. Control preventivo, con el fin de evitar una posible falla en la integridad y preservación de los datos personales.
- Se debería controlar que el usuario posea otros medios de para los importes y no únicamente por tarjetas de crédito, pensando en posibles casos de falla de ese sistema. Control preventivo
- Se debería tener un control claro de quienes realizaron cada examen y de que el resultado de dicho examen solo sea accesible por quién lo rindió. Un control detectivo, que valide los datos entre quien solicita los resultados y quien rindió realmente dicho examen.

6. En un acercamiento para una auditoría basado en riesgos, el auditor en sistemas de información debe considerar el riesgo inherente existente y además:

a) Considerar como eliminar el riesgo mediante la aplicación de controles
b) Considerar el balance de las pérdidas potenciales versus el costo de implementar controles
c) Determinar si el riesgo residual es más alto que el costo de la cobertura de seguros adquirida.

Justifique adecuadamente su respuesta.

Respuesta (CORREGIDA COMO CORRECTA)

La opción b)

Esta percepción de costo beneficio es importante en un auditor porque le permite juzgar si las medidas de control a proponer a las empresas son beneficiosas o no para la misma. Un auditor no comprende en profundidad los controles que exige o propone para que una empresa pueda no brindar un resultado de auditoría útil.