M19/3/ITGSX/BP2/SPA/TZ0/XX/M

Diploma Programme
Programme du diplôme
Programa del Diploma

Esquema de calificación

Mayo de 2019

Tecnología de la información en una sociedad global

Nivel medio y nivel superior

Prueba 2

18 páginas

Uso de los criterios de evaluación en la evaluación externa

Para la evaluación externa, se ha establecido una serie de criterios de evaluación. Cada criterio de evaluación cuenta con cierto número de descriptores; cada uno describe un nivel de logro específico y equivale a un determinado rango de puntos. Los descriptores se centran en aspectos positivos aunque, en los niveles más bajos, la descripción puede mencionar la falta de logros.

Los examinadores deben valorar el trabajo de evaluación externa del NM y del NS con relación a los cuatro criterios (del A al D) utilizando los descriptores de nivel.

- Se utilizan los mismos criterios para el NM y el NS.
- El propósito es encontrar, para cada criterio, el descriptor que exprese de la forma más adecuada el nivel de logro alcanzado por el alumno. Esto implica que, cuando un trabajo demuestre niveles distintos para los diferentes aspectos de un criterio, será necesario compensar dichos niveles. La puntuación asignada debe ser aquella que refleje más justamente el logro general de los aspectos del criterio. No es necesario cumplir todos los aspectos de un descriptor de nivel para obtener dicha puntuación.
- Al evaluar el trabajo de un alumno, los examinadores deben leer los descriptores de cada criterio hasta llegar al descriptor que describa de manera más apropiada el nivel del trabajo que se está evaluando. Si un trabajo parece estar entre dos descriptores, se deben leer de nuevo ambos descriptores y elegir el que mejor describa el trabajo del alumno.
- En los casos en que un mismo descriptor de nivel comprenda dos o más puntuaciones, los examinadores deben conceder las puntuaciones más altas si el trabajo del alumno demuestra en gran medida las cualidades descritas. Los examinadores deben conceder puntuaciones inferiores si el trabajo del alumno demuestra en menor medida las cualidades descritas.
- Solamente deben utilizarse números enteros y no notas parciales, como fracciones o decimales.
- Los examinadores no deben pensar en términos de aprobado o no aprobado, sino que deben concentrarse en identificar el descriptor apropiado para cada criterio de evaluación.
- Los descriptores más altos no implican un desempeño perfecto y los examinadores no deben dudar en utilizar los niveles extremos si describen apropiadamente el trabajo que se está evaluando.
- Un alumno que alcance un nivel de logro alto en un criterio no necesariamente alcanzará niveles altos en los demás criterios. Igualmente, un alumno que alcance un nivel de logro bajo en un criterio no necesariamente alcanzará niveles bajos en los demás criterios. Los examinadores no deben suponer que la evaluación general de los alumnos haya de dar como resultado una distribución determinada de puntuaciones.

Los criterios de evaluación deben estar a disposición de los alumnos antes del examen.

Área temática: Empresas y empleo

Información general:

Por favor, lea atentamente ya que los alumnos pueden confiar en este conocimiento que no está especificado en el artículo y recuerde que ésta no es una prueba técnica sobre RFID. Ésta no es una prueba técnica sobre RFID.

Algunos alumnos habrán estudiado RFID detalladamente y otros no, pero la transferencia de conocimientos desde otros sistemas similares a este debe calificarse positivamente, ***incluso si esta transferencia no es correcta técnicamente al 100%.*** *Esto se aplica especialmente a los desarrollos de la pregunta 2 y las soluciones técnicas de la pregunta 4.*

El sistema del artículo parece dar a entender que puede tener capacidades significativas de almacenamiento y transmisión, por ejemplo, "leer los datos" (línea 12), puede ser RFID pasivo o activo, la cantidad y el tipo de "datos" no se especifica, pero parece ser significativo, "chip RFID que contiene su información personal" (líneas 3 y 17).

Información importante: especialmente sobre el GPS y los chips que los estudiantes pueden confundir en la P2(a) o P4:

http://www.bbc.com/capital/story/20170731-the-surprising-truths-and-myths-about-microchip-implants

RFID pasivo y activo

https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

Capacidad de almacenamiento de RFID

http://www.asiarfid.com/rfid-basics/how-much-information-can-rfid-card-store.html

Criterio A — La cuestión y las partes interesadas **[4]**

1. (a) Describa **una** inquietud o problemática de carácter social o ético en relación con el sistema de TI que se menciona en el artículo.

***[1]**: por la identificación del problema (que puede no ser nombrado explícitamente o nombrado de modo vago o incorrecto).*

***[2]**: debe haber una descripción explícita del impacto/resultado/consecuencias/efecto/resultado para el empleado/empresa. Si la descripción es clara pero no contiene una identificación específica como privacidad o seguridad, se deben otorgar dos puntos igualmente. Se pregunta por la preocupación que se debe describir.*

Si se identifican dos preocupaciones vinculadas o superpuestas, por ejemplo, privacidad y seguridad, califique la mejor respuesta y esa preocupación debe explicarse en (2)(b).

La descripción debe hacer referencia al sistema de TI en el artículo.

*Si se plantean **dos** preocupaciones diferentes, solo califique la primera ya que la pregunta especifica **una** preocupación;* s*alvo en caso de que estén comúnmente vinculadas, como por ejemplo, seguridad y privacidad.*

Las preocupaciones sociales/éticas pueden incluir lo siguiente:
Tenga en cuenta que los alumnos pueden confundir privacidad y seguridad. Si se indica una preocupación clara pero hay confusión entre privacidad y seguridad, asigne un punto.

Si no está seguro de la preocupación social/ética identificada por el alumno y cree que debería estar en el esquema de calificación, póngase en contacto con su jefe de equipo.

Preocupaciones sobre la privacidad: una brecha de privacidad es un acceso a información sin el consentimiento del propietario

- personas no autorizadas que leen/acceden a la información almacenada del empleado
- la empresa podría usar los datos con otros fines no deseados si no hay política para controlar el uso: referencia a leyes sobre privacidad
- posible seguimiento de los empleados dentro del edificio de la empresa
- privacidad continua del empleado: quién tiene acceso a los datos (o quién puede obtener acceso a ellos en el futuro) y qué podrían hacer con ellos
- personalización del chip para fines más amplios por parte de los empleados - capacidad para que los empleados utilicen el RFID único como identificador para otras instalaciones, etc.
- el empleado debe firmar un contrato para que la empresa pueda implantar el chip y el empleado se siente vulnerable ya que teme perder el empleo si no firma el contrato.

Preocupaciones sobre la seguridad: una brecha de seguridad es un acceso no autorizado a información mediante técnicas u otros medios ilegales

- seguridad de los datos personales de un empleado en el chip
- seguridad de los datos personales del empleado enviados a/almacenados por la empresa
- seguridad de las instalaciones y equipos de los empleadores si un chip no funciona correctamente
- seguridad (física) de la persona con datos valiosos e implantes de chip deseados por otros

Preocupaciones de confiabilidad

- confiabilidad de los datos almacenados en el chip o en la base de datos de la empresa. Los datos almacenados pueden estar desactualizados
- confiabilidad de la infraestructura del sistema/red. Si el sistema no funciona correctamente, a las personas se les puede negar el acceso a áreas/recursos legítimos o posiblemente se les permita el acceso a áreas/recursos para los que no están autorizados
- los microchips pueden ocasionar problemas médicos e interferir con escáneres médicos, como MRI, y con dispositivos de seguridad en aeropuertos
- reutilización del chip después de que el empleado termine su trabajo.
- portabilidad del identificador único dentro del chip más allá de la empresa - estándares múltiples RFID en una mano interfiriendo entre sí, o en la ropa preocupaciones éticas y religiosas sobre los implantes en el cuerpo, la preocupación de la gente y las máquinas. Necesidad de asegurarse de que no se relaciona con hipótesis demasiado lejanas en el futuro (por ejemplo, ciborgs).
- empleado que se retira/deja el trabajo: extracción (cirugía invasiva aunque sea menor)
- propiedad del chip – ¿pertenece a la empresa o al empleado? - Empresa que exige la eliminación del chip del empleado saliente
- el chip podría degradarse con el paso del tiempo y ocasionar que no responda con datos correctos.

(b) Describa la relación de **una** parte interesada primaria con el sistema de TI que se menciona en el artículo.

Describir significa incluir quién, qué y dónde, pero no cómo y por qué para la puntuación completa.

***[1]**: quién: identificación de la parte interesada.*

***[2]**: dónde y qué: 'qué' haría la parte interesada con el Sistema de TI, 'dónde' estarían el chip o el sistema de TI asociado. .*

Las partes interesadas primarias pueden incluir lo siguiente:

- el empleado que tiene el chip implantado
- el empleador/empresa responsable de emitir los chips/dar soporte a la tecnología
- el empleado debe estar autorizado por el sistema de TI de la empresa para obtener acceso a los recursos de la empresa.
- persona técnica responsable de mantener el sistema - no una parte interesada principal a menos que sea descrita como tal por el estudiante de una manera significativa.
- el personal médico responsable de los procedimientos de inserción (y extracción potencial) - No es primario en el funcionamiento diario, pero sí lo es en la implementación del sistema de TI..

Nivel	***Descriptor de nivel***
0	*La respuesta no alcanza ninguno de los niveles especificados por los descriptores que figuran a continuación.*
1	*Se identifica una inquietud o problemática de carácter social o ético pertinente **o bien** la relación de **una** parte interesada primaria con el sistema de TI que menciona el artículo.*
2	*Se describe una inquietud o problemática de carácter social o ético pertinente **o bien** la relación de **una** parte interesada primaria con el sistema de TI que menciona el artículo, **o bien** se identifican ambas.*
3	*Se describe una inquietud o problemática de carácter social o ético pertinente **o bien** la relación de **una** parte interesada primaria con el sistema de TI que menciona el artículo; la otra se identifica.*
4	*Se describen una inquietud o problemática de carácter social o ético pertinente **y** la relación de **una** parte interesada primaria con el sistema de TI que menciona el artículo.*

Criterio B — Conceptos y procesos de TI **[6]**

2. (a) Describa, paso a paso, cómo funciona el sistema de TI.
Sistema de TI: Implantes de chip de identificación por radiofrecuencia (RFID) para empleados.

Muchas de las respuestas no encajarán perfectamente en un descriptor de calificación, por lo que será necesario aplicar el mejor ajuste.

***[1]**: el alumno puede mostrar algo de comprensión del proceso pero no en un enfoque paso a paso: utiliza la información del artículo y posiblemente falten algunos pasos.*

***[2]**: el alumno puede proporcionar un desarrollo lógico paso a paso utilizando la información del artículo, pero carece de algunos detalles. El mejor ajuste si la respuesta contiene desarrollos/información más allá del artículo, pero no en un enfoque paso a paso. Debe contener al menos DOS de los pasos principales que se mencionan más abajo.*

***[3]**: el alumno puede proporcionar una descripción paso a paso que puede ser detallada. Espere al menos DOS pasos principales más, al menos, DOS desarrollos.*

***[4]**: al menos cuatro desarrollos técnicos y todos los pasos principales en detalle.*

Los principales pasos proporcionados en el artículo son:
- el escáner RFID lee los datos del chip
- el sistema informático autentica al empleado
- el sistema de TI confirma que el empleado está autorizado para realizar la acción solicitada y/o se realiza la acción.

Respuestas en el artículo:
- RFID conectado a una cerradura de puerta
- escáneres/lectores RFID en equipos, incluidas fotocopiadoras y computadores.

Las respuestas con información adicional a la que se encuentra en el artículo pueden incluir lo siguiente:
- cuando el chip se implanta por primera vez, los empleados deben registrarlo en la empresa, y cada uno contiene un número RFID único
- el número RFID único se agrega a la base de datos (como la clave principal u otro campo del registro del empleado), junto con otros detalles relevantes del empleado
- cuando el empleado pasa su mano cerca de un escáner, la energía eléctrica de este proporciona energía para activar el chip y transmitir sus datos
- el escáner lee el número de identificación único del chip RFID (y la otra información personal) de los datos recibidos
- el número de ID se envía a una base de datos donde se compara con el número de RFID exclusivo del chip en la tabla de empleados para recuperar el registro del empleado
- el sistema también verifica si al empleado se le permite realizar la acción solicitada (por ejemplo, desbloquear una puerta)
- si el número de identificación coincide con un número almacenado y se permite la acción, el sistema envía una confirmación al equipo para que realice/permita al empleado realizar la acción solicitada.

- si no se encuentra el número de ID o no se permite la acción solicitada, el sistema deniega el acceso.
- el sistema puede registrar la hora del intento de acceso o del acceso al recurso
- el precio del almuerzo se lee desde el teclado o el lector de código de barras
- el número de RFID del empleado se coteja en la base de datos para recuperar el registro del empleado
- agregar el costo del almuerzo al registro del empleado
- sonido de un pitido para confirmar que se ha utilizado el chip - pitido del escáner
- el implante del RFID es pasivo (no tiene fuente de energía propia) y se activa en la proximidad de un escáner RFID
- detalles tales como una lista de acciones que el empleado puede realizar (abrir la puerta, entrar en el almacén, etc.) y están almacenadas en los servidores de la empresa
- la energía electromagnética del escáner emite continuamente señales de radio a una longitud de onda particular que activa cualquier chip en las proximidades
- el volumen de datos almacenados en el chip RFID suele ser de hasta 2 KB, y suele ser sólo un identificador único.

(b) Explique la relación entre el sistema de TI y la inquietud o problemática social o ética descrita en el **Criterio A**.

Explicar el vínculo entre la preocupación y partes específicas, o la totalidad, del sistema de TI significa que el alumno debe incluir cómo y por qué la problemática ha surgido a partir de la utilización del sistema informático. El nombramiento del problema identificado en el criterio A puede ser implícito.

La P2(b) claramente requiere una vinculación a la P1(a), pero esta vinculación podría ser solo genérica, por ejemplo, para un problema de seguridad específico descrito en la P1(a), en la P2(b) el alumno podría explicar una debilidad de seguridad sin referencia a la inquietud específica en la P1(a).

Si la preocupación tratada en la P2(a) es completamente diferente a la de la P1(a), no se puede establecer un vínculo y, por lo tanto, ***[0]****.*

La P2(b) también se puede relacionar con la P1(b) donde se describen el quién, el qué y el dónde del uso del sistema de TI.

[1]*: si el alumno identifica la relación entre la inquietud y el sistema de TI. Esto puede ser una repetición o una nueva redacción de la respuesta a (1)(a) o la falta de detalles para el cómo y por qué.*

[2]*: cómo y por qué se puede producir la problemática debe describirse: por ejemplo, privacidad: las respuestas deben especificar cómo (técnica) se puede acceder los datos (similar a algunos de los pasos para P2(a)) y por qué se ha permitido el acceso (por ejemplo, falta de configuración de privacidad, debilidad técnica).*

Relación del sistema informático con cuestiones de privacidad:

Personas no autorizadas que leen/acceden a la información almacenada del empleado

- (cómo) los datos almacenados en el chip o en la base de datos de la compañía pueden ser accesibles para personas no autorizadas (por qué) dentro o fuera de la compañía.
- (cómo) empleado preocupado por perder su empleo y/o su privacidad (por qué) El empleado debe firmar un contrato para que la empresa pueda implantar el chip y el empleado se siente vulnerable ya que teme perder el empleo si no firma el contrato.

Posible seguimiento de los empleados dentro del edificio de la empresa

- (cómo) con los escáneres de ubicación adecuados, el chip implantado permitiría a la compañía rastrear la ubicación del empleado mientras se mueve por el edificio de la empresa. (Por qué) esto podría hacerse sin que el empleado se dé cuenta de que están siendo vigilado. Al registrar la fecha/hora de accesos por puertas, los pagos del almuerzo, el empleado(r) puede calcular el tiempo que pasó en la oficina/fuera del escritorio.

Potencial para rastrear a los empleados más allá de la empresa

- (cómo) Los lectores/escáneres RFID en lugares públicos (u otros edificios de la compañía) podrían permitir que las personas sean identificadas y rastreadas (a través de registros de fecha/hora) incluso cuando no están dentro de los edificios de la empresa, sin que la persona se dé cuenta de que esto está sucediendo. (por qué) El RFID no está asegurado y una persona que tenga un escáner puede acceder fácilmente.

Relación del sistema informático con temas de seguridad:

Seguridad de los datos en el chip
- el chip puede ser leído por cualquier lector/escáner que esté lo suficientemente cerca, ya sea legítimo (por ejemplo, de propiedad de la empresa) o no. (por qué) El RFID no está securizado y una persona que tenga un escáner puede acceder fácilmente.

Seguridad de los datos enviados/almacenados por la empresa.
- (como) los datos pueden ser vulnerables a la intercepción durante la transmisión del chip al lector o dentro de la red de la empresa(por qué) los datos almacenados en la base de datos pueden ser inseguros/vulnerables. Una violación de la seguridad de la base de datos puede difundir información (por ejemplo, número RFID de empleados de alta jerarquía) que permitiría a una parte maliciosa obtener acceso a los edificios/equipos de la empresa.

Seguridad de locales y equipos del empleador
- (cómo) un chip comprometido/clonado podría permitir que personas no autorizadas accedan a áreas, materiales o equipos confidenciales, ya que el escáner/lector RFID se basa únicamente en los permisos almacenados en el chip o buscando el número de identificación del chip con los permisos almacenados en la base de datos. (por qué) El RFID no está securizado y una persona que tenga un escáner puede acceder fácilmente.

Relación del sistema informático con problemas de confiabilidad:

Confiabilidad de los datos almacenados en el chip o en la base de datos de la empresa
- (cómo) a menos que se registre un cambio en los permisos de acceso en la base de datos de la compañía (o se actualice al volver a escribir la información almacenada en el chip), (por qué) el sistema no será confiable en términos de otorgar los permisos correctos al empleado correcto.

Confiabilidad de la infraestructura del sistema/red
- (cómo) si el sistema tiene una falla o el número de RFID no se lee correctamente, (por qué) se le puede negar a las personas el acceso a áreas/recursos legítimos o posiblemente se les permita el acceso a áreas/recursos para los que no estén autorizados.

Uso adicional del ID único
- (cómo) algunas personas que tienen múltiples RFID incrustados con posibles interferencias o problemas de malinterpretación, ya que varios chips se activan a la vez. (por qué) el chip RFID utiliza un identificador a medida/diferente, es posible que el chip no pueda utilizarse en otros sistemas o que la empresa restrinja el acceso para utilizar el identificador RFID en otro sistema.

Propiedad del chip.

- (cómo) el chip RFID es proporcionado por la empresa y se requiere como herramienta de acceso dentro de la estructura de la empresa. El chip está incrustado en el interior de un empleado, lo que plantea el problema de que cuando el empleado se va, puede volver. (por qué) el chip no ha sido desactivado en la base de datos, cuando el empleado se va el chip no se ha extraído.

Se espera que los alumnos hagan referencia a partes interesadas relevantes, tecnologías de la información, datos y procesos. Se espera que se refieran a "cómo funciona el sistema de TI", utilizando la terminología de TI adecuada.

Nivel	***Descriptor de nivel***
0	*La respuesta no alcanza ninguno de los niveles especificados por los descriptores que figuran a continuación.*
1–2	*La comprensión del proceso paso a paso del funcionamiento del sistema de TI es escasa o nula y no va más allá de la información que aparece en el artículo.* *Se identifican los principales componentes del sistema de TI usando un mínimo de terminología técnica de TI.*
3–4	*Hay una descripción del proceso paso a paso del funcionamiento del sistema de TI que va más allá de la información que aparece en el artículo.* *Se identifica la mayoría de los principales componentes del sistema de TI usando alguna terminología técnica de TI.* *Se identifica la relación entre el sistema de TI del artículo y la inquietud o problemática presentada en el criterio A, con cierto uso de terminología de TISG.*
5–6	*Hay una descripción detallada del proceso paso a paso que muestra una clara comprensión del funcionamiento del sistema de TI y que va más allá de la información que aparece en el artículo.* *Se identifican los principales componentes del sistema de TI usando terminología técnica de TI adecuada.* *La relación entre el sistema de TI del artículo y la inquietud o problemática presentada en el criterio A se explica usando terminología de TISG adecuada.*

Criterio C — El impacto de las cuestiones sociales o éticas sobre las partes interesadas [8]

3. Evalúe el impacto de las cuestiones sociales o éticas sobre las partes interesadas.

Impacto = resultado/consecuencia/efecto/resultado en las partes interesadas.

Hay una serie de impactos que pueden compararse y analizarse críticamente. Dadas las limitaciones de tiempo, no todos son necesarios. Por lo menos se requieren dos partes interesadas para ingresar a la banda de puntuación superior.

[1]: *uno o dos impactos identificados.*

[2]: *más de dos impactos descritos de tipo positivo o negativo.*

[3]: *análisis por estructura: división en grupos, por ejemplo, positivos/negativos y/o varios interesados.*

[4–5]: *debe incluir conexiones analíticas de enlace (entre positivos/negativos, varios interesados, diversos problemas) y/o comentarios evaluativos adicionales sobre las implicaciones para las partes interesadas. A los alumnos que han brindado una buena conclusión se les aplica el mejor ajuste aquí. Solo una parte interesada, máximo de* ***[4]*** *si incluye análisis y evaluaciones, por ejemplo, los impactos solo en el alumno. Si el número de impactos es significativo pero está desequilibrado para un 6, entonces es mejor para un 4 o un 5 dependiendo de la cantidad de análisis y evaluación.*

[6]: *se recomienda al menos dos impactos negativos y dos positivos para cada parte interesada a fin de proporcionar un análisis equilibrado en la banda de puntuación superior. La calidad del análisis es la consideración más importante.*

[7–8]: *se necesita una conclusión respaldada por una referencia directa a los impactos descritos. La evaluación debe centrarse en el impacto general en todas las partes interesadas mencionadas al analizar el equilibrio entre los impactos positivos y negativos.*

Los impactos positivos pueden incluir:

Para el empleado
- comodidad: no es necesario llevar tarjetas de identificación, recordar códigos PIN o contraseñas, *etc.*
- velocidad: la autorización es muy rápida, no es necesario detenerse y esperar
- menos riesgo potencial que el uso de la biometría: si el chip se ve comprometido, entonces puede ser reprogramado o reemplazado, a diferencia de la biométrica que no se puede cambiar
- podría usar el RFID único con otros sistemas y aplicaciones informáticas externos a la empresa, por ejemplo, domótica o llaves sin contacto para vehículos.

Para la empresa
- permite un control detallado de quién está autorizado para hacer qué (por ejemplo, los empleados pueden tener acceso a algunas áreas de la empresa y se les niega el acceso a otras)
- registros fáciles de mantener de quién hace qué, cuándo y dónde para auditorías, control de costos, *etc.*
- el chip se puede usar potencialmente para una creciente variedad de propósitos en el futuro
- la eliminación de contraseñas/PIN elimina los problemas causados por los empleados que usan contraseñas débiles /las escriben para recordarlas/puede que su PIN sea visto por otros empleados mientras los ingresan/empleados que comparten contraseñas; aumentando potencialmente la seguridad de la empresa
- una vez insertado puede necesitar menos soporte de TI que las contraseñas que a menudo se olvidan y el personal de TI debe cambiarlas.

Los impactos negativos pueden incluir:

Para el empleado
- algunos empleados pueden ser particularmente opuestos/temerosos del proceso de implantación o tener objeciones culturales/religiosas/médicas/sanitarias al mismo
- amenaza física para la seguridad si una persona extrae el chip de la mano o ataca físicamente a una persona y la obliga a usar su mano
- el empleado puede perder su trabajo si se niega a implantar el chip/falta de autonomía o de elección para el empleadouna vez implantado, el chip siempre está ahí y siempre "activo". Los empleados pueden tener poco control sobre la forma en que los datos en el chip, o los registros sobre el uso del chip (en la base de datos), son utilizados por la empresa y/o terceros
- la compañía puede monitorizar al empleado en tiempo real para localizarlo, así como utilizar los registros para el mismo propósito, por ejemplo, controlando la frecuencia con la que el empleado ha entrado en el baño o en la sala de café. Este es un problema de privacidad/vigilancia
- los datos en el chip pueden ser comprometidos por un tercero malintencionado. Sin querer, el empleado puede permitir que un tercero sea identificado falsamente como el empleado o podría entrar a zonas delicadas. ¿Quién será responsable de esta infracción?
- extracción y/o desactivación (borrado de datos si se usan más allá de la identificación única) al terminar el empleo - procedimiento traumático e invasivo
- si el RFID se usa fuera de la empresa (por ejemplo, para uso personal), la desactivación podría ser un problema
- vida útil de la tecnología - la obsolescencia puede requerir más chips, lo que puede dar lugar a problemas potenciales si la información personal en el chip no está actualizada y necesita actualizarse. Esto es difícil, ya que el chip RFID tendría que ser extraído.
- datos incorrectos en el chip podrían tener consecuencias para el acceso al sistema e implicaciones médicas/financieras y también médicas si el chip necesita ser reemplazado.

Para la empresa

- el chip de un empleado puede estar comprometido (por ejemplo, clonado o los datos de este pueden ser analizados por un tercero malintencionado), la seguridad de la empresa puede estar en riesgo
- la compañía tendría que ofrecer asistencia continua para garantizar que los permisos se mantuvieran actualizados y que los datos fueran confiables
- si el empleado resultó víctima de fraude a través del uso del chip, ¿sería la empresa responsable de las consecuencias?
- obligar a tener un chip implantado puede disuadir a los empleados de unirse a la empresa y causar que algunos dejen su trabajo
- la reputación/publicidad de la empresa puede verse afectada debido a la posible vigilancia de los empleados/publicidad negativa
- puede haber problemas cuando un empleado es despedido o renuncia. Aunque se cerraría su cuenta en la base de datos, también existe el problema de extraerle el dispositivo RFID de la mano
- el costo de implantar el chip y otros costos asociados con la producción de chips médicos viables puede ser grande. Y también, mucho más que una etiqueta de identificación normal
- las complicaciones debidas a los implantes supondrían costos para la compañía (médica y hospitalaria) y, también, para sus compañías de seguros
- problemas de interferencia con el metal y la eficacia limitante del agua, en particular con los chips de baja y alta frecuencia de rango vida útil de la tecnología - inversión continua y actualización, especialmente si el empleado necesita nuevos chips para operar con equipos más modernos.

Nivel	***Descriptor de nivel***
0	*La respuesta no alcanza ninguno de los niveles especificados por los descriptores que figuran a continuación.*
1–2	*El impacto de las cuestiones sociales o éticas sobre las partes interesadas se describe, pero no se evalúa. Se copia directamente material del artículo o se hacen referencias implícitas a él.*
3–5	*El impacto de las cuestiones sociales o éticas sobre las partes interesadas se analiza parcialmente, con algunos comentarios de evaluación. La respuesta contiene referencias explícitas parcialmente desarrolladas a la información que aparece en el artículo. Hay cierto uso de terminología de TISG adecuada.*
6–8	*El impacto de las cuestiones sociales o éticas sobre las partes interesadas se analiza y se evalúa completamente. En toda la respuesta se hacen adecuadamente referencias explícitas y bien desarrolladas a la información que aparece en el artículo. Se usa terminología de TISG adecuada.*

Criterio D — Una solución a un problema planteado en el artículo **[8]**

4. Evalúe **una** posible solución que aborde al menos **un** problema identificado en el **Criterio C**.

[1]*: se identifica la solución.*

[2]*: se describe la solución (qué, quién, dónde) y el enlace al artículo puede ser implícito, lo que podría ser una descripción general, por ejemplo, descripción de política general similar a la que se encuentra en un libro de texto.*

[3]*: la solución se aplica al problema directamente y no de manera general (una descripción, especialmente de la encriptación, típica de un libro de texto implicaría la pérdida de esta puntuación) cómo y por qué resuelve el problema (primera evaluación positiva). La solución debe ser factible y se puede aplicar al problema, incluso si no es de "buena calidad".*

[4–5]*: se requiere al menos otra evaluación positiva y al menos una evaluación negativa. Mejor ajuste si la descripción es limitada.*

[6]*: una calificación completa por las fortalezas y debilidades requiere un equilibrio de al menos dos evaluaciones positivas y negativas.*

[7–8]*: párrafo final que hace referencia directamente a las evaluaciones. Los alumnos pueden proponer desarrollos futuros como parte de la conclusión en lugar de una discusión de evaluaciones; se aplica el mejor ajuste.*

Las respuestas pueden incluir, entre otras, las soluciones que se enumeran a continuación. El examinador debe usar su juicio y su conocimiento para determinar si una solución se aplica al problema y es factible. En caso de duda el examinador debe consultar al jefe de equipo.

Soluciones técnicas

Encriptación

Por favor, tenga en cuenta que muchos alumnos tienden a escribir soluciones para la encriptación: la encriptación de los datos en el chip y/o en la base de datos - necesita explicar cómo se encripta y cómo se utiliza para resolver el problema o de lo contrario pierde puntos por falta de descripción y la incapacidad de explicar cómo se aplica para resolver el problema.

- los datos personales que se están transfiriendo se encriptan para evitar la interceptación de paquetes de datos durante la transmisión. Dentro de la base de datos hay una clave para la desencriptación autorizada
- el RFID sólo contiene un identificador único que está vinculado con la base de datos. Los datos personales están securizados en la base de datos.

Integridad de los datos

- datos incorrectos en el chip - implementación de procesos de validación y verificación de datos en la base de datos y al almacenar datos en el chip
    - si el chip de un empleado está en peligro (por ejemplo, clonado o los datos han sido robados por un tercero malintencionado), la seguridad de la empresa puede estar en peligro.
    - encriptación de los datos en el chip y/o en la base de datos
    - la seguridad puede ser un rango de medidas similares y conectadas tales como cortafuegos, escáneres de virus, encriptación, contraseñas, etc.
- limitar la cantidad de datos almacenados en el chip/base de datos a los datos necesarios para conceder los permisos, minimizando así el impacto negativo de cualquier brecha de la seguridad
    - implementar la autenticación de dos factores (por ejemplo, el chip más un PIN, una aplicación, un mensaje de texto o una contraseña de correo electrónico) o una autenticación biométrica adicional (por ejemplo, chip y escáner de retina)
- sustituir el chip por una autenticación biométrica que tenga muchos de los beneficios del chip sin los aspectos negativos de las cuestiones médicas o éticas - la evaluación debe ser una comparación con el chip; de lo contrario, es sólo una descripción de la nueva tecnología y no se aplica al problema de la tecnología del chip

- la empresa tendría que ofrecer un soporte informático continuo para garantizar que los permisos se mantuvieran actualizados y los datos fueran fiables
    - la compañía formula una estrategia de revisión/actualización regular para asegurar que los datos se mantengan actualizados y exactos
- los datos sobre los permisos (acceso a las puertas, etc.) se almacenan en la base de datos, no en el chip RFID, por lo que los datos pueden actualizarse fácilmente
    - si el empleado se convierte en víctima de fraude a través del uso del chip, ¿será la empresa responsable de las consecuencias?

<u>Soluciones relacionadas con políticas y procedimientos</u>

- se podrían establecer políticas (a nivel de empresa o incluso nacional) para controlar las circunstancias en las que se podrían recopilar, almacenar y utilizar los datos. Estas políticas deben ser revisadas y actualizadas periódicamente. Los empleados deben estar de acuerdo explícitamente con esas políticas dando su consentimiento para participar.
- algunos empleados pueden ser particularmente opuestos/temerosos del proceso de implantación o tener objeciones culturales/religiosas al mismo
    - a dichos empleados se les podría permitir usar el chip fuera del cuerpo en lugar de tenerlo implantado
- una vez implantado, el chip siempre está ahí y siempre “activo”. Los empleados pueden tener poco control sobre la forma en que los datos en el chip son utilizados por la empresa y o terceros
    - podría ser posible que los empleados protejan el chip (por ejemplo, usando un guante especialmente diseñado u otro parche blindado) para evitar que se lea fuera de las situaciones elegidas por ellos
    - se puede usar un guante especial para evitar el acceso no deseado, desconocido o accidental a la información del implante RFID
- los datos en el chip pueden estar comprometidos por un tercero malicioso
- encriptación de los datos en el chip o en la base de datos

- limitar la cantidad de datos almacenados en el chip/base de datos a solo los datos necesarios para otorgar permisos, minimizando así el impacto negativo de cualquier brecha de seguridad.

Si la evaluación no proporciona información adicional a la del artículo, al alumno se le otorgará un máximo de ***[2]****.*

Nivel	***Descriptor de nivel***
0	*La respuesta no alcanza ninguno de los niveles especificados por los descriptores que figuran a continuación.*
1–2	*Se propone y se describe* ***una*** *solución factible al menos a* ***un*** *problema.* *No se da ningún comentario de evaluación. Se copia directamente material del artículo o se hacen referencias implícitas a él.*
3–5	*Se propone y se evalúa parcialmente* ***una*** *solución factible al menos a* ***un*** *problema. La respuesta contiene referencias explícitas parcialmente desarrolladas a la información que aparece en el artículo. Hay cierto uso de terminología de TISG adecuada.*
6–8	*Se propone y se evalúa completamente* ***una*** *solución factible al menos a* ***un*** *problema; se abordan los puntos fuertes y los potenciales puntos débiles de dicha solución. También pueden haberse identificado áreas de futuro desarrollo. En toda la respuesta se hacen adecuadamente referencias explícitas y totalmente desarrolladas a la información que aparece en el artículo. Se usa terminología de TISG adecuada.*