N16/3/ITGSX/BP2/SPA/TZ0/XX/M

Diploma Programme
Programme du diplôme
Programa del Diploma

Esquema de calificación

Noviembre de 2016

Tecnología de la información en una sociedad global

Nivel superior y nivel medio

Prueba 2

15 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: Política y gobierno

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.

Algunas posibles inquietudes o problemáticas de carácter social o ético son:

- vigilancia: el uso de la tecnología significa que la policía está bajo constante vigilancia de sus superiores
- privacidad: el uso de cámaras en los dispositivos puede significar que no solo se observa a los delincuentes. También se capta la vida cotidiana de los agentes de policía
- privacidad: ¿los datos relativos a la información personal de las víctimas y la información sobre el delito se almacenan de forma segura en la base de datos central?
- privacidad: delincuentes conocidos porque cometieran un delito en el pasado; que se encuentren en la zona no significa que sigan realizando dicha actividad delictiva
- privacidad: víctimas de delitos: Centro de barrio
- confiabilidad: excesiva confianza en la tecnología. La policía puede no ser capaz de llevar a cabo su trabajo con eficacia si la tecnología falla
- confiabilidad: Centro de barrio. Se permite a los ciudadanos proporcionar actualizaciones sobre delitos que conozcan, lo que conlleva un potencial de información falsa o exagerada, etc
- integridad de los datos: los cambios no autorizados a los datos sobre la delincuencia podrían significar que no se puede confiar en dichos datos
- seguridad: acceder a una base de datos central desde una variedad de dispositivos; podrían sufrir un ataque de *hacking* (piratería informática); pérdida del dispositivo
- seguridad: el uso de apps de terceros para el almacenamiento de datos u otros fines (Google Maps) plantea posibles riesgos de seguridad
- políticas y normas: no tener políticas adecuadas sobre el uso de dispositivos podría causar problemas para el departamento de policía sobre cómo se utilizan los dispositivos móviles
- brecha digital: impacto en el trabajo si los policías no están familiarizados con el uso de sistemas de TI; impacto en los ciudadanos que no estén familiarizados con el uso de apps y no sepan cómo dar información actualizada, denunciar delitos y recibir alertas, lo cual reduciría la eficacia del sistema.

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

Algunas posibles partes interesadas primarias son:
- agentes de policía: usan la app para obtener información acerca de los delitos en un área o para denunciar un delito
- ciudadanos/testigos: utilizan la herramienta de generación de mapas de delitos para alertar a la policía con información sobre delitos; la utilizan para ver qué tan segura es su zona
- administradores del departamento de policía: utilizan la app de la policía para determinar dónde ubicar a los agentes
- delincuentes: usan la app para decidir dónde cometer el próximo delito
- desarrolladores de la app: desarrollan la app de la policía y son responsables de corregir los errores y comprobar la seguridad de los datos
- víctimas: cuyos datos se registran en el dispositivo inteligente en la escena del delito.

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: uso de teléfonos inteligentes y tabletas para denunciar un delito o actualizar información sobre un delito en el servidor de la nube en la sede de la policía de Londres.

Las respuestas proporcionadas en el artículo son las siguientes:
- la función Denuncia de delitos permite a un agente denunciar un delito
- los mapas digitales proporcionan información sobre delitos en un área determinada
- hacer clic en cada punto permite que un policía actualice la información de un delito o que ingrese los detalles de un delito
- se pueden usar cámaras de dispositivos para reunir pruebas de video en tiempo real
- la creación de una base de datos única de la policía permite a los agentes ingresar información
- autorizar los dispositivos forma parte de la configuración, debido a su compatibilidad multiplataforma
- almacenamiento en servidores de terceros
- procesamiento/análisis de datos por fecha, hora, zona y tipo de delito. Los datos se visualizan en una serie de gráficos
- reproducción de videos y grabaciones
- compartir información por etiquetas: enviar a un compañero
- compartir video.

Algunas posibles respuestas con información adicional a la del artículo son:

Configuración:
- descarga de la app
- registrarse con la app de la policía, para lo cual se debe incluir el nombre de usuario y contraseña o información personal o número de teléfono móvil para la verificación
- servicios de localización activados
- iniciar sesión en la app de la policía
- el uso de herramientas como el configurador de Apple para crear una "imagen" del dispositivo (más probable que descargar la app) de modo que incluya la configuración, datos de seguridad, etc
- nombre de usuario y contraseña para acceder al STT.

Entrada:
- la entrada de datos se hace mediante foto, voz, texto, lápiz informático y botones del dispositivo
- la entrada usa la pantalla táctil, la cámara del teléfono o el micrófono
- se usan servicios de localización como el GPS para identificar el área.

Conectividad:
- el teléfono inteligente se conecta a la red inalámbrica o de banda ancha móvil (mediante enlace de radio) (3G, 4G, Wi-Fi)
- se usa un cliente/servidor: el teléfono es el cliente, la jefatura de policía ofrece los servicios en la nube
- los datos deben encriptarse durante la transmisión/desencriptarse en el servidor.

Procesamiento:
- la app identifica la ubicación de los agentes de policía mediante GPS o torres de telefonía celular (triangulación) e identifica a cada agente en el mapa
- ver otros delitos denunciados en la zona
- seleccionar iconos de delitos para leer más información acerca de ellos
- si el delito ya se ha denunciado: leer la información sobre el delito y tomar nota de las advertencias, por ejemplo, si es un delincuente peligroso. Hacer clic en el delito y escribir información adicional, número de identificación de la policía y usar la cámara para captar pruebas (video/foto del delito)
- si el delito es nuevo, ingresar la información requerida en los campos obligatorios, por ejemplo, seleccionar el tipo de delito, los detalles del delito, subir foto/video capturado usando el teléfono inteligente o la tableta
- a cada delito se le asignará un identificador único para identificarlo y evitar que se mezclen los detalles de delitos similares en la misma zona
- los detalles del delito se envían usando el botón de envío
- uso de retransmisión (*streaming*) en tiempo real para las pruebas en video
- uso de dudas y criterios de búsqueda al analizar los datos.

Almacenamiento:
- la base de datos de la policía almacena cada nuevo registro de delito usando un identificador único para identificarlo
- almacenamiento local de datos para reproducirlos, modificarlos, o por si se pierde la conexión.

Salida:
- el mensaje de confirmación del delito denunciado se muestra en la pantalla junto con orientación sobre cómo proceder con el delito (por ejemplo, pedir refuerzos)
- salida de audio: sonidos de advertencia
- gráficos y visualizaciones.

(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 inquietud o problemática y partes específicas, o la totalidad, del sistema de TI significa que el alumno debe incluir cómo y por qué la inquietud o problemática ha surgido a partir de la utilización del sistema de TI. La mención de la inquietud o problemática identificada en el criterio A puede ser implícita.

Algunas posibles respuestas son:

Vigilancia:
- los servicios de localización incorporados podrían significar que se puede rastrear a la policía cuando está en servicio (cómo); debido a falta de políticas (por qué).

Privacidad:
- el uso de cámaras en los dispositivos puede significar que los agentes de policía pueden grabar las actividades de los ciudadanos sin razón válida o mientras recogen pruebas de un delito (cómo). La vida cotidiana de los ciudadanos puede grabarse y guardarse en la base de datos de la policía (cómo). Las fotografías o los videos que se realizan durante el servicio pueden tomarse desde cierta distancia y que en ellos aparezca no solo el delito, sino también personas inocentes (por qué). Las cámaras de las tabletas o teléfonos no tienen zoom o ajustes complejos (por qué)
- el acceso no autorizado a datos sobre delitos (cómo); debido a falta de políticas o de configuración de seguridad de la base de datos podría significar que otros accedan a las imágenes de video (por qué)
- la privacidad de personas con antecedentes: es posible que las personas con antecedentes policiales o que hayan cometido un delito en el pasado sean objetivos de la policía o sufran acoso (cómo); ya que el dispositivo identifica a delincuentes conocidos en la zona (por qué)
- las apps de terceros para almacenar o crear mapas de datos, como los documentos de Google (cómo); puede significar que quienquiera que tenga acceso podría ver datos confidenciales (por qué)

Confiabilidad:
- depender demasiado de la tecnología podría hacer que, si falla, resulte difícil para los agentes de policía hacer su trabajo:
  - por ejemplo, poca batería de los teléfonos (cómo); las apps del teléfono, por ejemplo la grabadora de video, usan la batería rápidamente, o los modelos de teléfonos más viejos tienen menor duración de la batería (por qué)
  - si un teléfono queda dañado al detener a un delincuente podría significar que la policía no tenga acceso a los datos sobre delitos mientras realizan su trabajo, lo cual podría ponerlos en peligro al acercarse a la escena de un delito (cómo); la carcasa del teléfono inteligente puede no ser muy resistente, o podría mojarse o ser pisada (por qué)
  - la pérdida de la señal Wi-Fi (cómo); no todas las áreas de una ciudad tienen la misma cobertura, por ejemplo si el agente que tiene el dispositivo se desplaza bajo tierra, o si algún edificio se interpone (por qué)
  - puede que los mapas no estén actualizados o que las actualizaciones no sean precisas, lo cual puede hacer que la localización de la escena del delito no sea correcta, que se envíe apoyo a una ubicación errónea, o que se den instrucciones erróneas a los agentes (por qué).

Integridad de los datos:
- modificación no autorizada o accidental de la información por parte de agentes de policía (cómo); si las propiedades de los campos no están establecidas correctamente, o si hay un acceso no autorizado debido a una configuración de seguridad deficiente en el teléfono, en el servidor o en la transmisión podría significar que los datos no sean correctos (por qué)
- actualización, por parte de los ciudadanos, de delitos que conozcan (cómo); la información puede ser falsa, errónea, obsoleta o tener la intención de despistar a la policía (por qué).

Seguridad:
- acceder a una base de datos central desde una variedad de dispositivos: podrían sufrir un ataque de *hacking* (piratería informática) mediante la interceptación de los datos en la transmisión (cómo); interceptación y desencriptado de los datos en la transmisión debido a la falta de un encriptado fuerte (por qué)
- ataques de *hacking* (piratería informática) a la base de datos de la policía en la nube (cómo); podrían estar causados por penetraciones al cortafuegos (*firewall*) o por la falta de actualización del software del servidor (por qué)
- ataques de *hacking* (piratería informática) al teléfono/tableta (cómo); los expertos en seguridad tienen que realizar comprobaciones de seguridad en los distintos sistemas operativos, lo que podría significar que algunos dispositivos son menos seguros que otros (puesto que los *hackers* o piratas informáticos encuentran fallos de seguridad continuamente), puede haber virus en el teléfono/tableta (por qué)
- problemas de seguridad debido a la pérdida de dispositivos: los móviles/tabletas pueden perderse fácilmente cuando los policías están de servicio (cómo); los dispositivos pequeños podrían caerse de los bolsillos de los uniformes, los códigos de acceso fáciles y los detalles de usuario guardados en la app podrían significar que los delincuentes podrían obtener acceso a la base de datos de la policía fácilmente si los encuentran (por qué)
- el control del acceso no lo gestiona la policía, sino el administrador externo (cómo); ya que el almacenamiento de datos y los mapas de Google los administran terceros.

Falta de políticas y normas:
- no tener políticas adecuadas sobre el uso de dispositivos podría causar problemas para el departamento de policía sobre cómo los agentes utilizan los dispositivos móviles, por ejemplo, podrían infringir la privacidad de los ciudadanos o revelar información confidencial acerca de las operaciones de la policía (cómo); los administradores de la policía pueden no ser conscientes de los posibles problemas que podrían surgir debido a que trabajan en oficinas (por qué).

Se espera que los alumnos hagan referencia a las partes interesadas, las tecnologías de la información, los datos y los procesos pertinentes. Se espera que los alumnos expliquen "cómo funciona el sistema de TI" utilizando una 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.

Algunos posibles impactos positivos para los agentes de policía son:
- información actualizada en tiempo real, de modo que estarán más preparados cuando se aproximen a un delito y podrán estar más seguros en las calles
- saber dónde se encuentran los agentes de refuerzo para ayudar a combatir los delitos
- procesamiento más rápido de los delitos (menos tiempo al no tener que volver a la comisaría)
- mejores estadísticas de delincuencia podrían conducir a más promociones/aumentos de sueldo/bonificaciones
- más oportunidades laborales para desarrollar la tecnología de TI
- la participación activa de los ciudadanos acerca a la comunidad la labor de la policía.

Algunos posibles impactos negativos para los agentes de policía son:
- depender de la app en exceso, por ejemplo, el dispositivo podría quedarse sin batería, o sin cobertura de red, o tardar en conectarse; eso puede hacer su trabajo más difícil y más peligroso
- no todos los policías experimentados están familiarizados con las nuevas tecnologías, así que tendrán que recibir capacitación
- la pérdida o daños del dispositivo pueden ser costoso si es necesario reemplazarlo o repararlo
- si se han manipulado los datos, la policía puede denunciar incorrectamente un delito o suponer erróneamente que un área es segura
- vigilancia: el uso de la tecnología significa que la policía está bajo vigilancia constante de sus superiores
- privacidad: el uso de cámaras en los dispositivos puede significar que no solo se observa a los delincuentes. Se capta la vida cotidiana de los agentes de policía
- falta de políticas y normas: puede hacer que el trabajo de los agentes sea más difícil, por ejemplo, que la información no sea admisible en un juicio, o que algunas acciones inapropiadas de los agentes de policía proporcionasen escapatorias para los delincuentes.

Algunos posibles impactos positivos para los ciudadanos/testigos/víctimas son:
- calles más seguras: se puede disuadir a los delincuentes menores. La policía está mejor equipada para resolver delitos
- reunir más pruebas para los juicios, lo que puede significar procesamientos con más éxito
- se puede tomar decisiones bien fundamentadas sobre si desplazarse a un área determinada.

Algunos posibles impactos negativos para los ciudadanos/testigos/víctimas son:
- se puede invadir la privacidad de ciudadanos inocentes debido al aumento de la vigilancia mediante los dispositivos de la policía
- los ciudadanos que viven en zonas de cobertura deficiente de Wi-Fi o de la red móvil pueden no estar tan protegidos
- el valor del precio de la vivienda puede caer en las zonas donde se detecta una tendencia de aumento de los delitos si esta información se comparte con la población
- si los delincuentes logran interceptar la base de datos sobre delitos y usan dichos datos, las zonas podrían pasar a ser menos seguras
- el acceso no autorizado a los datos sobre la delincuencia que luego se comparten con la población podría poner en riesgo a ciudadanos a los que falsamente se vinculase con un delito
- integridad de los datos: los cambios no autorizados a los datos sobre la delincuencia podrían significar que no se puede confiar en ellos y que ciudadanos inocentes pueden ser acusados de delitos
- la falta de políticas por parte del departamento de policía podría conducir a un mal uso, lo que podría afectar negativamente a los ciudadanos
- el servidor lo mantiene un tercero, por lo que puede ser difícil averiguar quién tiene acceso a los datos, además de los agentes de policía.

Algunos posibles impactos positivos para el departamento de policía/los administradores/los desarrolladores de la app son:
- supervisión más fácil de los agentes de policía (dado que se les puede rastrear)
- ahorro de personal, dado que los agentes pueden ser más eficientes
- reducción de costos debido a que se requieren menos policías para hacer el mismo trabajo
- mayores oportunidades de empleo
- mayor eficacia en lo que se refiere al tiempo, el costo y el esfuerzo
- mayor eficacia en lo que se refiere la exactitud de los datos obtenidos y a presentarlos a varias partes interesadas
- la asistencia técnica la presta un tercero, así que no es necesario invertir en tecnología en la nube: se ahorra en costos.

Algunos posibles impactos negativos para el departamento de policía son:
- aumento de los costos de proporcionar la solución de TI: dispositivos, desarrollo de apps
- más difícil para el departamento técnico dar asistencia técnica y administrar una solución multiplataforma; puede haber más problemas de seguridad a los que hacer frente
- puede que haya agentes de policía buenos y experimentados que no sean tan eficientes como deberían debido a la falta de conocimientos técnicos
- la necesidad de capacitación y los costos que implica
- muchos pueden considerar que utilizar esta tecnología es difícil/incómodo
- si se filtran los datos de los que se encarga un tercero, la reputación de la policía quedará en entredicho
- un fallo tecnológico puede conllevar interrupciones y atrasos; dependencia excesiva en la tecnología y pérdida de intuición
- la pérdida o el robo de dispositivos: puede haber un uso indebido de estos si caen en malas manos
- pérdida de puestos de trabajo ya que se necesitan menos policías para patrullar pero más para mantener la tecnología.

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**.

Algunas posibles respuestas son:

Soluciones a los problemas de la vigilancia:
- políticas sobre quién tiene acceso a la información sobre la ubicación de los agentes de policía y sus movimientos y cómo se utiliza esta información
- los agentes de policía pueden desactivar los servicios de seguimiento de GPS/ubicación cuando quieran.

Soluciones a los problemas de seguridad/privacidad/integridad de los datos:
- los datos sobre la delincuencia se encriptan durante la transmisión y en el servidor central en la nube
- acceso restringido a la información almacenada en el servidor central, es decir, los empleados solo pueden ver la información necesaria
- autenticación para los empleados de la policía que tengan permiso para acceder a la base de datos
- se pueden establecer políticas
- mantener pistas/registros de auditoría para mostrar quién accede a los datos y cuándo
- métodos de autenticación como utilizar una contraseña segura/biometría/dirección MAC/dirección IP en el inicio de sesión
- capacitación en seguridad para los empleados
- los datos que hay en el servidor no se comparten con otras partes/se mantienen en el servidor en la sede de la policía.

Soluciones al problema de la confiabilidad del servidor de la nube:
- redundancia integrada en el sistema: tener un servidor de reserva por si el servidor principal falla (ahora esto forma parte de los proveedores de servicios en la nube, pero hay que explicar que ha habido ocasiones en las que estos grandes sistemas de reserva no funcionaron)
- políticas del departamento de policía: incluir procedimientos/programación de carga alternativa para hacer frente a los problemas técnicos
- políticas del departamento de policía para manejar problemas imprevistos, por ejemplo, agentes que no han hecho copias de seguridad o que no pueden enviar datos debido a problemas técnicos.

Soluciones al problema de la confiabilidad de los dispositivos de la policía y el acceso al servidor en la nube:
- disponibilidad de otros dispositivos, por ejemplo, un dispositivo de repuesto en el coche patrulla
- otras formas de acceder a la red pública para conectarse al servidor de la policía (puntos de acceso Wi-Fi)
- guardar temporalmente el delito en el dispositivo hasta que se restablezca la red
- software de seguimiento de dispositivo por si se pierde el teléfono; software que permita bloquearlo, borrarlo, ubicarlo en un mapa o incluso ver la cara del usuario con la cámara del dispositivo
- políticas del departamento de policía respecto al robo/pérdida/dispositivos dañados, que incluyan procedimientos y la forma de abordar los problemas técnicos.

Soluciones al problema de la falta de políticas sobre el uso apropiado de la tecnología:

- se deben elaborar políticas que incluyan en qué casos, cómo, dónde y cuándo se debe utilizar la tecnología. Esto lo deben desarrollar los administradores de la policía y se debe compartir con todos los departamentos de policía del país.

*Si la evaluación no proporciona ninguna información adicional a la que se da del artículo, se 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.