M15/3/ITGSX/BP2/SPA/TZ0/XX/M

Diploma Programme
Programme du diplôme
Programa del Diploma

Esquema de calificación

Mayo de 2015

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: Intimidación cibernética entre alumnos en las redes sociales

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 inquietudes o problemáticas de carácter social o ético pueden ser:

- anonimato: poder publicar anónimamente en los sitios de redes sociales y poder generar comportamientos agresivos
- acoso continuado: que tiene como resultado la ridiculización y el sufrimiento de la víctima
- privacidad (utilizar y compartir información personal sin permiso): el uso no ético de información personal de la víctima con la intención de acosarla (si una inquietud o problemática se identifica como privacidad pero se describe como otra —por ejemplo, anonimato—, conceda 1 punto)
- aspectos éticos de la intimidación cibernética (comportamiento incorrecto en Internet)/ciudadanía digital en el uso adecuado de la tecnología: se la considera inaceptable e incluso ilegal en ciertas circunstancias
- autenticidad: disponibilidad pública de información sobre la víctima que puede no ser verdadera; afirmaciones difamatorias.

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

Entre las partes interesadas primarias podrían incluirse las siguientes:

- víctima de intimidación cibernética: la persona agredida por información personal enviada a teléfonos móviles (por ejemplo, mediante SMS) o a redes sociales (Facebook, Ask.fm, etc.)
- "matón" o acosador cibernético: persona que usa dispositivos móviles, computador de escritorio o teléfono móvil para publicar información perjudicial sobre una persona mediante un servicio de telefonía móvil o en redes sociales
- personas que ven la información personal sobre la víctima enviada a una red social
- desarrolladores/empresas de redes sociales/sitios web: diseñan la red social y desarrollar las características entre las que figura el anonimato que utilizan las víctimas y los acosadores
- padres: pueden supervisar las redes sociales/correos electrónicos/SMS con los que se intimida a sus hijos, o que sus hijos utilizan para intimidar
- alumnos/usuarios: lo utilizan para comunicarse y colaborar, estar en contacto con amigos, organizar su vida personal, compartir actualizaciones, imágenes, elementos multimedia, o mensajes con su círculo de amigos (debe tener cierto contexto)

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 las tecnologías informáticas y las redes sociales.

- Entre las respuestas provistas en el artículo se encuentran las siguientes:

Acceso mediante la tecnología informática
- los ejemplos de redes sociales que se dan en el artículo son Facebook y Ask.fm (líneas 4 y 9)
- desde un teléfono móvil o desde un computador portátil a otro usuario (líneas 10 y 11)
- acceso permanente utilizando aplicaciones de teléfonos móviles para publicar directamente en redes sociales (líneas 19 y 20)
- mediante servicios de teléfonos móviles (línea 27)
- las aplicaciones o "apps" son programas informáticos especializados que se descargan a dispositivos móviles, que pueden ejecutarse en Internet, en un computador, en un teléfono móvil o en otros dispositivos electrónicos (nota a pie de página)

Almacenar y compartir información
- el sitio permite que un usuario envíe preguntas anónimas (línea 10)
- cuando se recibe una respuesta, el intercambio de mensajes se publica, para que todos puedan leerlo (líneas 11 y 12)
- recibir un flujo de mensajes desagradables (líneas 12 y 13)
- publicar anónimamente en el colegio (línea 17)
- los mensajes pueden incluir una variedad de información personal, fotos o videos (líneas 20 y 21)

Algunas respuestas con información adicional a la que se da en el artículo pueden ser:

Acceso mediante la tecnología informática
- crear la cuenta y dar la información personal necesaria para hacer esto
- descargar la aplicación o iniciar sesión en el sitio web de la red social
- otras redes sociales (por ejemplo, Twitter, sitios de encuestas por Internet, sitios de juegos interactivos, blogs, etc.)
- utilizar Wi-Fis/accesos a Internet públicos para evitar el seguimiento de direcciones IP
- crear cuentas falsas (sin usar datos personales, o con otras cuentas de correo electrónico)

Almacenar y compartir información
- los usuarios reciben una alerta (por correo electrónico, SMS, etc.) que indica que han recibido información en su teléfono móvil o que se ha publicado información en su red social
- en Ask.fm se permite el anonimato, pero tal vez no en otros sitios
- entre la información personal puede haber fotos y videos que se tomasen sin el conocimiento del usuario
- la información publicada puede verla más gente de la que los usuarios creen
- el usuario puede dejar información que le identifique (como coordenadas en fotos, qué tipo de dispositivo tomó las imágenes, detalles en segundo plano en la foto, etc.) (los usuarios pueden tomar fotos con geoetiquetas activadas y publicarlas)

- buscar amigos en la red social con los que conectarse/utilizar la barra de búsqueda
- utilizar la función de chat, llamadas de voz o mensajes en la red social o el correo electrónico
- etiquetado de fotos o videos

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

*Algunas respuestas pueden ser (esta **no es una lista exhaustiva**):*

- El anonimato es una inquietud o problemática :
  - la red social no tiene un modo de saber quién está ejerciendo la intimidación cibernética
  - poder publicar de forma anónima en redes sociales o utilizar una cuenta falsa (cómo); sin buenas medidas de autentificación o sin buenas políticas en la red social, a menudo basta una dirección de correo electrónico válida, aunque sea falsa (por qué)
- El acoso continuado es una inquietud o problemática:
  - la víctima recibe permanentemente alertas cada vez que se publica información (cómo); la cuenta de la red social o del correo electrónico está configurada para recibir alertas cada vez que alguien publica información, o son automáticas (por qué)
  - es posible que muchas personas envíen información a una cuenta común (cómo); debido a la configuración de privacidad de la cuenta de un usuario, que puede establecerse para amigos o pública y la cantidad de amigos del usuario (por qué)
  - la víctima se siente afectada/ridiculizada/acosada por la naturaleza y frecuencia de los envíos al servicio de telefonía móvil y/o a la red social (cómo); la facilidad de poder divulgar publicaciones hace que las publicaciones hirientes se puedan propagar con rapidez y que lleguen a otras personas que utilicen tecnologías móviles (por qué)
  - no hay forma de pedir a la red social que se borren determinadas publicaciones (cómo); no hay funciones adecuadas incorporadas para denunciar el mal uso de la red social (por qué)
- La privacidad es una inquietud o problemática:
  - el sistema de TI permite que cualquiera pueda ver las publicaciones (cómo); la divulgación de fotos/publicaciones sin que se pida a la persona permiso para que se la etiquete: el uso de etiquetas favorece la rápida divulgación sin que se dé permiso (por qué)
- Los aspectos éticos de la intimidación cibernética son una inquietud o problemática:
  - intimidación cibernética: compartir información personal con la intención de herir o avergonzar a otra persona mediante publicaciones o fotografías/videos etiquetados y a menudo tomados/compartidos si permiso (cómo); el “matón” no tiene que pedir permiso para publicar una fotografía o enviar un correo electrónico con archivos adjuntos; es posible que no se den cuenta de que es una forma de intimidación y que lo hagan “por diversión”, las redes sociales públicas no están completamente supervisadas (por qué)
  - tiene consecuencias jurídicas en ciertas circunstancias: las víctimas pueden demandar al “matón”, para lo cual deben recabar pruebas de la intimidación o del daño a la reputación y llevarlo ante los tribunales (cómo); los “matones” pueden dejar una huella digital, como la dirección IP utilizada

o actividades de conexión a redes escolares; se pueden imprimir como prueba correos electrónicos/publicaciones en la red social (por qué)

- La autenticidad de la persona que publica la información (también relacionado con el anonimato) es una inquietud o problemática:
  - los “matones” pueden crear con facilidad cuentas falsas y esconder su verdadera identidad para crear cuentas desde las que escribir las publicaciones o los mensajes intimidatorios (cómo); esto se debe a que para crear una cuenta se requiere muy poca autentificación para demostrar que el usuario es quien dice ser (a menudo la verificación se hace mediante cuentas de correo electrónico que se pueden crear fácilmente) (por qué)
  - los “matones” utilizan otras cuentas (por ejemplo, cuentas de amigos) para compartir información o publicaciones intimidatorias (cómo); falta de seguridad en las cuentas de amigos si se comparten contraseñas o datos de acceso (por qué)
- La autenticidad de la información es una inquietud o problemática:
  - los “matones” pueden publicar información sobre otras personas aunque no sea verdadera (cómo); falta de procesos de aprobación en la red social para comprobar la fiabilidad del contenido antes de publicarlo (por qué)

Se espera que los alumnos hagan referencia a las partes interesadas y a las tecnologías de la información, datos y procesos. Se espera que los alumnos se refieran a “cómo funciona el sistema de TI” usando la terminología de TI apropiada.

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. La siguiente lista no es exhaustiva. En caso de duda, consulte a su jefe de equipo.

Impacto = resultado/consecuencia/efecto/repercusión

Algunas posibles respuestas son:

Impactos sobre la víctima
Positivos
- formación del carácter: las víctimas aprenden a valerse por sí mismas
- se aprende lo dañina que puede ser la intimidación cibernética y puede disuadir a la víctima de intimidar cibernéticamente a otras personas
- la capacidad de publicar de manera anónima permite libertad de expresión, lo cual es bueno para alumnos tímidos o para personas que vivan en un entorno opresivo
- la intimidación cibernética tiene forma escrita, por lo cual es fácil obtener pruebas de que ha sucedido, ya que las publicaciones y los mensajes se pueden imprimir

Negativos
- sentir que se es victimizado, atormentado, herido, acosado, amenazado, ridiculizado o humillado
- molestia permanente: alertas constantes siempre que se distribuye información
- problemas de salud (como desórdenes vinculados al estrés, temor, inquietud, depresión, indefensión)
- necesidad de cambiar de colegio o de club para evitar el contacto personal con los “matones” cibernéticos
- reticencia a contar a un adulto (como un docente o un padre) que se es víctima de la intimidación cibernética
- descenso en el rendimiento académico, debido a la tensión emocional de recibir intimidación

Impactos sobre quien realiza la intimidación cibernética
Positivos
- sentido de poder sobre la víctima
- reconocimiento personal de los compañeros involucrados en la intimidación cibernética
- menos supervisión por parte de los adultos en actividades por Internet que presenciales
- la intimidación puede realizarse desde sus propias casas, lo cual es cómodo y aporta sensación de seguridad de que no van a descubrirles
- ser capaz de encontrar información personal es un impacto positivo para el “matón”
- una mayor conciencia sobre las implicaciones de sus acciones, que puede conducir a un uso más responsable de la tecnología

Negativos
- si se le descubre, puede enfrentarse al castigo del colegio o a enfrentamientos judiciales con la víctima y sus padres

Impactos sobre las personas que ven las publicaciones
Positivos
- una mayor conciencia y búsqueda de signos de depresión en los amigos; la ayuda evita muchas víctimas mortales
- fuerza a los usuarios a ser cuidadosos y selectivos con sus amigos en línea y a aplicar configuraciones de seguridad más estrictas
- sensación de poder al enterarse de información personal (verídica o no) acerca de la víctima y al juzgar a la víctima

Negativos
- se difunde información sobre la víctima a un público amplio y disperso
- pueden tener poco o ningún conocimiento de si la información es verdadera o no
- pueden optar por no hacer nada por miedo a ser víctimas ellos mismos

Impactos sobre el personal escolar
Positivos
- los colegios han aplicado políticas y sistemas de seguridad que ayudan a prevenir la intimidación cibernética durante el horario escolar
- algunos colegios han desarrollado programas de educación social que abordan la intimidación cibernética
- los colegios pueden supervisar las publicaciones públicas de sus alumnos y ser proactivos para abordar problemas
- la intimidación cibernética tiene forma escrita, por lo cual es más fácil ayudar a los alumnos que quieran denunciar al “matón”

Negativos
- los profesores pueden no ser conscientes de su papel y responsabilidad en los casos de intimidación cibernética
- los colegios pueden carecer de un programa de educación social que contemple los casos de intimidación cibernética
- los sistemas de seguridad para supervisar o hacer un seguimiento de la intimidación cibernética pueden ser caros, además del tiempo que conlleva extraer la información necesaria
- presión adicional sobre el personal para responder a casos de intimidación que sucedan fuera del colegio
- los colegios con un problema de intimidación cibernética pueden ver perjudicada su reputación

Impactos sobre los padres
Positivos
- los padres han aprendido por otros casos a estar al tanto de las aplicaciones y los servicios en línea que sus hijos están utilizando
- una mayor conciencia paterna respecto a las posibles medidas correctivas
- los padres pueden supervisar las cuentas de sus hijos y así protegerlos a distancia

Negativos
- es posible que los padres no sepan cómo abordar la situación cuando su hijo es víctima de intimidación cibernética
- es posible que los padres deban matricular a su hijo en otro colegio para detener la intimidación cibernética
- en algunos países, los padres son los responsables últimos de las acciones de sus hijos menores de edad, y pueden afrontar acciones judiciales si su hijo es un "matón"

Impactos sobre las redes sociales como *Facebook* y Ask.fm
Positivos
- actualizar las políticas para abordar la intimidación cibernética: esto puede fomentar que más estudiantes elijan esa red social por parecer más segura
- una mayor cantidad de usuarios (padres) se unirán a la red social para supervisar a sus hijos o para estar en contacto con ellos

Negativos
- es posible que se tenga que aplicar un sistema de denuncias de casos de intimidación cibernética, lo cual requiere tiempo para que los desarrolladores lo creen y le cuesta a la empresa dinero para emplear a los desarrolladores y para probar las nuevas funciones
- evitar las publicaciones anónimas: esto puede desalentar a determinados usuarios que se hubieran unido por esa función específica
- la reputación de la red social disminuirá si se dan casos repetidos de intimidación cibernética, lo cual conllevará menos usuarios y, en consecuencia, menos ingresos

*Si la evaluación no proporciona ninguna 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	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**.

El problema debe especificarse aquí, pero si no se hace aquí, debe ser uno de los impactos/problemas identificados en el Criterio C.

Algunas posibles respuestas son:

Soluciones para redes sociales que permiten publicaciones anónimas
- las redes sociales deben guardar la información identificatoria para que pueda denunciarse a los "matones" cibernéticos
- los casos de intimidación cibernética requieren de un método sencillo para denunciarlos y emprender acciones
- las políticas deben establecer claramente las penalizaciones por realizar intimidación cibernética
- las redes sociales no deben permitir el anonimato

Soluciones para informar a los padres sobre las acciones que tomar contra la intimidación cibernética
- instalar filtros web en los computadores del hogar para filtrar los sitios web de redes sociales
- guardar todas las pruebas de intimidación cibernética para compartir con los directivos del colegio y la policía
- solicitar asesoramiento y ayuda de organizaciones en línea que se especializan en la intimidación cibernética

Soluciones para colegios que ofrecen programas educativos para evitar la intimidación cibernética
- crear equipos de seguridad para investigar las denuncias de intimidación
- implementar un programa anti-intimidación en el colegio para los alumnos
- desarrollar políticas escolares relacionadas con la intimidación cibernética

Soluciones para colegios que implementen sistemas de seguridad para evitar la intimidación cibernética
- los colegios usan software de red para bloquear sitios web comunes utilizados para la intimidación cibernética (por ejemplo, *Facebook* o Ask.fm)

Soluciones para gobiernos que legislen sobre la intimidación cibernética
- pueden establecerse leyes que definan las condiciones para que los colegios puedan monitorear la intimidación cibernética y denunciarla a la policía
- capacitar a las autoridades policiales sobre los casos denunciados que pueden considerarse intimidación cibernética y qué acciones tomar

Soluciones para la intimidación cibernética
- cancelar la cuenta en la red social para no formar parte de ninguna comunicación relacionada con la intimidación cibernética y para que el "matón" tenga menos acceso a la víctima

No acepte una solución a la intimidación cibernética en general.

*Si la evaluación no proporciona ninguna 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.