National Qualifications 2025

X869/77/11

Spanish
Reading and Translation

MONDAY, 19 MAY

9:00 AM – 10:30 AM

Total marks — 50

SECTION 1 — READING — 30 marks

Attempt ALL questions.

Write your answers clearly, in **English**, in the answer booklet provided. In the answer booklet, you must clearly identify the question number you are attempting.

SECTION 2 — TRANSLATION — 20 marks

Attempt to translate the whole extract.

Write your translation clearly, in **English**, in the answer booklet provided. In the answer booklet, you must clearly identify the section number you are attempting.

You may use a Spanish dictionary.

Use **blue** or **black** ink.

Before leaving the examination room you must give your answer booklet to the Invigilator; if you do not, you may lose all the marks for this paper.

SQA ©

SECTION 1 — READING — 30 marks

Attempt ALL questions

Read the whole article carefully and then answer, in **English**, ALL the questions that follow.

This article discusses a recent report on the ways in which home smart devices gather information, and the potential consequences.

¿Revelan los dispositivos inteligentes información de nuestras casas?

La casa ha sido tradicionalmente el lugar más privado para una familia. Primero entró el móvil, y ahora también, lo han hecho los dispositivos inteligentes, lo que ha cambiado todo. Un informe recién publicado por la Universidad Carlos III de Madrid avisa de los problemas de seguridad y privacidad de ciertos dispositivos inteligentes que tenemos en casa, como los teléfonos, los televisores o los asistentes virtuales. Estos dispositivos pueden tener 'conversaciones' entre ellos y esto hace que den detalles íntimos de cada hogar, sin que los usuarios lo sepan. Antes era imposible obtener esta información.

David Choffnes, uno de los coautores del informe, descubrió que existen una multitud de riesgos posibles asociados con el intercambio de información. Por ejemplo, los dispositivos inteligentes pueden saber nuestra ubicación, la renta que obtenemos, quiénes son nuestros familiares o amigos que pasan por casa, o cuándo estamos o no en casa. Recogen datos de la casa que no tienen nada que ver con su función original. Si el hogar es el lugar más privado, le parece una invasión de la privacidad grave.

Choffnes y su equipo montaron en la universidad una investigación que consistió en 'un laboratorio viviente' con más de cien dispositivos inteligentes. Allí, estudiaron toda la variedad de comportamientos y relaciones que se dan entre los dispositivos inteligentes que se comunican entre sí, desde bombillas y neveras, hasta calefactores y altavoces. Para extender su informe, el equipo investigó además las conexiones que pueden existir entre estos dispositivos y aplicaciones móviles específicas. Juan Tapiador, miembro del equipo de la universidad subraya: "Creo que la gente no tiene ni la más remota idea de que todos los dispositivos inteligentes y aplicaciones conectados a la wifi hablan entre sí de alguna manera. En nuestra investigación, hemos descubierto que la información que contienen los dispositivos les permite deducir muchos detalles de nuestras vidas, y podrían proporcionar una huella digital de nuestra casa, lo que permitiría vigilancias dirigidas".

Es cierto que no todo el mundo entiende los riesgos potenciales identificados en el informe. Los usuarios encuentran difícil reconocer el valor que tiene su información personal porque tienden a malinterpretar el riesgo que implica la recolección de docenas de datos puntuales de una casa. Existen un montón de casos donde se capturan los datos: se anota si pasamos o no por debajo de las luces del pasillo que se encienden solas y cuántas veces pasamos, y el modelo del televisor y las horas que lo vemos.

Vijay Prakash, de la Universidad de Nueva York, y otro coautor del informe, da ejemplos concretos del uso preocupante de nuestra información: "Si una persona malintencionada abusa de la información que flota libremente entre los dispositivos domésticos inteligentes, puede rastrear a un usuario. Además, si las aplicaciones instaladas reconocen nuestros hábitos en línea, podríamos llegar a convertirnos en víctimas de estafadores. Es imprescindible estar atentos a los peligros porque es cierto que esto no pasará solo una vez, sino continuamente".

Prakash continúa: "Mucho de lo que he descrito no es ilegal, pero el entorno tecnológico es un campo de minas y como resultado hay implicaciones bastante graves: muy a menudo el usuario no ha consentido de ninguna manera, y además se obtiene información sensible que está sujeta a la protección de datos".

A un humano toda esta combinación de datos le puede parecer insufrible. Pero para los dispositivos es simplemente su labor cotidiana. Más allá de los riesgos de seguridad posibles, esta información nutre la enorme maquinaria del marketing y la publicidad global. De momento no ocurre, pero igual que recibimos publicidad personalizada en los móviles, la industria ya podría identificar nuestro hogar para personalizar la publicidad acorde a nuestras condiciones económicas. Aún más, hace más fácil monetizar nuestro estilo de vida.

Aunque la mayoría de la información se usa con fines comerciales, es posible que haya otros usos más peligrosos. Esos datos se obtienen cada vez más ilegalmente y pueden convertirse en una herramienta para lanzar ciberataques dañinos. La Unión Europea ha creado varias regulaciones estrictas que deberían proteger a sus ciudadanos de este tipo de riesgo. El problema es que cada día aparecen nuevas amenazas y es muy difícil garantizar que tanto empresas como individuos estén suficientemente protegidos.

Questions **MARKS**

Re-read lines 1–13.

1. Smart devices in our homes have changed everything.

(a) The Carlos III University in Madrid has recently published a report. What warning does it give? **1**

(b) The report states that smart devices have digital conversations between each other. What does it say about this? **1**

2. David Choffnes, one of the co-authors of the report, discovered a range of information sharing between smart devices. What examples are there of this? **4**

Re-read lines 14–24.

3. Choffnes and his team set up an investigation at the university.

(a) What form did the investigation take? **3**

(b) Juan Tapiador, a member of the team, says more about the investigation. What has the team discovered? **2**

Re-read lines 25–30.

4. Not everyone understands the potential risks identified in the report.

(a) What do people find hard to recognise and why? **2**

(b) What examples of data capture does the article highlight in this context? **2**

MARKS

Questions (continued)

Re-read lines 31–36.

5. Vijay Prakash is another co-author of the report.

(a) What does he say about the worrying uses of information gathered? **2**

(b) Why is it essential to be aware of the dangers? **1**

Re-read lines 37–40.

6. Prakash states that although much of what he has described is not illegal, he thinks that this area of technology is a minefield. What are the serious implications of this, in his opinion? **2**

Re-read lines 41–46.

7. Apart from the possible security risks, the article goes on to discuss some other ways in which the information identified by Prakash could be used. What does it say? **3**

Now consider the article as a whole.

8. What is the writer's overall purpose in writing about this subject? Justify your response with close reference to the points made and the language used. **7**

SECTION 2 — TRANSLATION — 20 marks

9. Translate the underlined section into English: (lines 47–52) **20**

Aunque la mayoría . . . suficientemente protegidos.

[END OF QUESTION PAPER]

[OPEN OUT]

DO NOT WRITE ON THIS PAGE

[BLANK PAGE]

DO NOT WRITE ON THIS PAGE

Acknowledgement of copyright

Article – Article is adapted from https://elpais.com/tecnologia/2023-10-30/asi-nos-espian-los-dispositivos-inteligentes-y-revelaninformacion-de-nuestras-casas-la-gente-no-tiene-ni-idea.html?ssm=IG_CM?event_log=oklogin.

SQA has made every effort to trace the owners of copyright of this item and seek permissions. We are happy to discuss permission requirements and incorporate any missing acknowledgement. Please contact question.papers@sqa.org.uk.