DELL Technologies

¿Es más inteligente que su ciberatacante?

Empezar cuestionario

PREGUNTA 1 DE 14

Suplantación de identidad

Recibe un correo electrónico sobre un "pedido de Windows Defender" con una factura de 399,99 $ que parece oficial por una subscripción de 1 año a una cuenta de Microsoft Defender. Indica claramente "Por favor, no responda a este correo electrónico", pero incluye el botón "Ayuda y contacto" y un número de teléfono. No recuerda haber realizado ningún pedido de este tipo.

¿Qué hace?

1

Seleccione la mejor respuesta a continuación

A Hace clic inmediatamente en el botón "Ayuda y contacto", porque no quiere que le hagan el cargo en su tarjeta de crédito.

B Abre el correo electrónico en una ventana de incógnito del navegador web y hace clic en el botón "Ayuda y contacto".

C Comprueba el extracto en línea de su tarjeta de crédito para ver si el cargo aparece y usa el número de teléfono para intentar obtener más información.

D Inspecciona la dirección de correo electrónico y se da cuenta de que parece un intento de suplantación de identidad. Entonces, hace clic en la opción para informar de una suplantación de identidad en su programa de correo electrónico o reenvía el mensaje al departamento de tecnología informática para que lo investiguen. Y, por supuesto, no lo abre.

E Elimina el correo electrónico sin abrirlo.

DELL Technologies

RESPUESTA

Suplantación de identidad

¡BUEN TRABAJO!

Informe del intento de suplantación de identidad

Cuando recibe un correo electrónico sospechoso que le indica que haga clic en algún enlace por cualquier motivo, lo mejor es eliminar el correo electrónico sin abrirlo o hacer clic en la opción de informar la suplantación de identidad en la barra de Outlook para que el equipo de tecnología informática lo investigue.

Si parece una suplantación de identidad, probablemente lo sea.

Siguiente pregunta

DELL Technologies

RESPUESTA

Suplantación de identidad

BUEN TRABAJO, PERO...

Informe del intento de suplantación de identidad

Si llama a un número de teléfono que resulta ser falso, también se pondrá en riesgo. Hay otra opción en esta lista que es más adecuada. **Si parece una suplantación de identidad, probablemente lo sea.**

Siguiente pregunta

DELL Technologies

RESPUESTA

Suplantación de identidad

¡LE HAN HACKEADO!

Informe del intento de suplantación de identidad

Recuerde que, cuando recibe un correo electrónico sospechoso que le indica que haga clic en algún enlace por cualquier motivo, lo mejor es eliminar el correo electrónico sin abrirlo o hacer clic en la opción de informar la suplantación de identidad en la barra de Outlook para que el equipo de tecnología informática lo investigue. **Si parece una suplantación de identidad, probablemente lo sea.**

Siguiente pregunta

DELL Technologies

PREGUNTA 2 DE 14

Suplantación de identidad en redes sociales

Entra en su cuenta de Instagram y ve que Lyle Lovett ha respondido directamente a un comentario que usted le ha hecho en sus publicaciones. Le pide que contacte con él por mensaje directo y le envía un enlace en el que tiene que hacer clic para acceder a contenido muy exclusivo y valioso.

Usted:

2

Seleccione la mejor respuesta a continuación

A No puede creer la suerte que tiene y hace clic inmediatamente en el enlace.

B Copia el enlace y lo abre en una ventana de incógnito.

C Comparte el enlace con sus amigos en redes sociales.

D Pasa el ratón por el enlace y sospecha que podría ser un intento de suplantación de identidad, así que elimina el mensaje y bloquea al remitente.

E Bloquea y denuncia al remitente sin hacer clic en ningún enlace.

DELL Technologies

RESPUESTA

Suplantación de identidad en redes sociales

¡BUEN TRABAJO!

Informe del intento de suplantación de identidad

Cuando recibe un correo electrónico sospechoso que le indica que haga clic en algún enlace por cualquier motivo, lo mejor es eliminar el correo electrónico sin abrirlo o hacer clic en la opción de informar la suplantación de identidad en la barra de Outlook para que el equipo de tecnología informática lo investigue. **Si parece una suplantación de identidad, probablemente lo sea.**

Siguiente pregunta

DELL Technologies

RESPUESTA

Suplantación de identidad en redes sociales

¡LE HAN HACKEADO!

Informe del intento de suplantación de identidad

Recuerde que, cuando recibe un correo electrónico sospechoso que le indica que haga clic en algún enlace por cualquier motivo, lo mejor es eliminar el correo electrónico sin abrirlo o hacer clic en la opción de informar la suplantación de identidad en la barra de Outlook para que el equipo de tecnología informática lo investigue. **Si parece una suplantación de identidad, probablemente lo sea.**

Siguiente pregunta

DELL Technologies

PREGUNTA 3 DE 14

Seguridad de la contraseña

Su departamento de tecnología informática insiste en que cree contraseñas seguras. El motivo es que este tipo de credenciales está entre los objetivos de mayor valor de los atacantes. Entonces...

¿Cómo puede hacer que su contraseña sea más segura?

3

Seleccione la mejor respuesta a continuación

A	Crear contraseñas de 8 caracteres como mínimo (si puede ser, incluso más largas).
B	Usar una combinación de letras, números y caracteres.
C	Evitar reutilizar contraseñas entre cuentas o sitios (lo mejor es que cada una sea única).
D	Todas las opciones anteriores.
E	Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Seguridad de la contraseña

¡BUEN TRABAJO!

Utilice una contraseña segura

Para que una contraseña sea segura, debe ser única y combinar al menos 8 letras, números y caracteres, y quizás también puede usar una frase de contraseña fácil de recordar. ¡No utilice el nombre de su perro! Además, use la autenticación de dos factores, que, junto con la contraseña segura, le dará la protección que necesita.

Siguiente pregunta

DELL Technologies

RESPUESTA

Seguridad de la contraseña

BUEN TRABAJO, PERO...

Utilice una contraseña segura

Una contraseña segura combina todas las medidas de seguridad mencionadas: es única y contiene al menos 8 letras, números y caracteres. ¡No utilice el nombre de su perro! Si desea aumentar la seguridad, use la autenticación de dos factores y frases de contraseña con números y caracteres en lugar de contraseñas.

Siguiente pregunta

DELL Technologies

RESPUESTA

Seguridad de la contraseña

¡LE HAN HACKEADO!

Utilice una contraseña segura

Una contraseña segura es única y combina al menos 8 letras, números y caracteres. Si desea aumentar la seguridad, use la autenticación de dos factores y frases de contraseña con números y caracteres en lugar de contraseñas.

Siguiente pregunta

DELL Technologies

PREGUNTA 4 DE 14

Ingeniería social

Recibe una llamada en su móvil de una persona que dice ser del departamento de tecnología informática para informarle de que su contraseña ha caducado y necesita configurar una nueva. El número de teléfono parece seguro. La persona le pide que le dé su número de empleado, número de seguridad social y fecha de nacimiento para verificar los datos.

¿Qué hace?

4

Seleccione la mejor respuesta a continuación

A Le da la información, porque quiere restablecer la contraseña y seguir con su trabajo.

B Le pide su correo electrónico y número de teléfono de contacto para comprobar su identidad y luego le da la información que le solicitó.

C Cuelga inmediatamente e informa al departamento de tecnología informática.

D Le da su número de empleado y fecha de nacimiento, pero no le da su número de seguridad social.

E Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Ingeniería social

4

¡BUEN TRABAJO!

Cuelgue y contacte con el equipo informático

Algunos atacantes utilizan ingeniería social para conseguir que les facilite información confidencial por teléfono. Aunque pueda comprobar en su sistema que ese empleado existe, no hay ninguna garantía de que esté hablando de verdad con esa persona. **Usted es el único que debe iniciar el proceso para restablecer su contraseña.**

Siguiente pregunta

DELL Technologies

RESPUESTA

Ingeniería social

4

¡LE HAN HACKEADO!

Cuelgue y contacte con el equipo informático

Algunos atacantes utilizan ingeniería social para conseguir que les facilite información confidencial por teléfono. Aunque pueda comprobar en su sistema que ese empleado existe, no hay ninguna garantía de que esté hablando de verdad con esa persona. **Usted es el único que debe iniciar el proceso para restablecer su contraseña.**

Siguiente pregunta

DELL Technologies

PREGUNTA 5 DE 14

Infiltración en su PC

Mientras atiende una llamada, observa un comportamiento extraño en la pantalla, por ejemplo, que el ratón se mueve solo, que hay ventanas de texto o consolas que se abren y cierran, o menús que aparecen y desaparecen.

Entonces:

5

Seleccione la mejor respuesta a continuación

A Supone que es un problema inofensivo del PC y sigue trabajando.

B Lo consulta con su departamento de tecnología informática, pero sigue trabajando.

C Deja de usar el PC, lo apaga inmediatamente y se comunica con el departamento de tecnología informática (desde otro dispositivo) para informar del problema.

DELL Technologies

RESPUESTA

Infiltración en su PC

5

¡BUEN TRABAJO!

Contacte inmediatamente con el equipo informático

El hecho de que el ratón se mueva solo por la pantalla podría indicar un ataque grave con vulneración de datos y, posiblemente, el registro de pulsaciones de teclas. El departamento de tecnología informática debe saberlo lo antes posible para investigar el caso correctamente.

Siguiente pregunta

DELL Technologies

RESPUESTA

Infiltración en su PC

5

¡LE HAN HACKEADO!

Contacte inmediatamente con el equipo informático

Un comportamiento inusual podría indicar que hay un atacante supervisando su PC, quien podría estar extrayendo datos y registrando las pulsaciones de teclas para conocer información importante, como sus contraseñas. La mejor opción es apagar el PC inmediatamente e informar del problema a su departamento de tecnología informática.

Siguiente pregunta

DELL Technologies

PREGUNTA 6 DE 14

Ataque de malware mediante USB

Mientras camina por el aparcamiento de su empresa, ve una bolsa entre dos coches. Ve que contiene cinco unidades USB todavía en el embalaje original, ¡y cada una tiene 500 GB!

¿Qué hace?

6

Seleccione la mejor respuesta a continuación

A Abre una, la inserta en la ranura para USB de su PC y les da las otras cuatro a sus compañeros.

B Se lleva las unidades USB a casa y las utiliza en su ordenador personal.

C Avisa al departamento de tecnología informática y al personal de seguridad del edificio de que se encontró las unidades USB y se las entrega.

D Les regala las unidades USB a sus hijos por Navidad.

E Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Ataque de malware mediante USB

¡BUEN TRABAJO!

Avise al personal de tecnología informática y de seguridad

Este tipo de ataque permite a los atacantes instalar malware en una organización a través de un empleado para insertar archivos payload maliciosos en la red. Nunca inserte una unidad USB ni ningún otro accesorio de origen desconocido en NINGUNO de sus dispositivos. Además, ¡no son un buen regalo!

Siguiente pregunta

DELL Technologies

RESPUESTA

Ataque de malware mediante USB

6

¡LE HAN HACKEADO!

Avise al personal de tecnología informática y de seguridad

Este tipo de ataque permite a los atacantes instalar malware en una organización a través de un empleado para insertar archivos payload maliciosos en la red. Nunca inserte una unidad USB ni ningún otro accesorio de origen desconocido en NINGUNO de sus dispositivos. Además, ¡no son un buen regalo!

Siguiente pregunta

DELL Technologies

PREGUNTA 7 DE 14

Ransomware

Viene un comercial a la oficina para hacer una presentación sobre una tecnología nueva en la que está interesada su empresa. Trae la presentación en una unidad USB y le pide que la inserte en su PC para poder proyectarla mientras habla.

¿Qué hace?

7

Seleccione la mejor respuesta a continuación

A Le hace caso e inserta la unidad USB en su PC.

B Le pregunta si es posible descargar la presentación, ya que hay una política en su empresa que prohíbe usar unidades USB externas, pero, como no se puede descargar, le hace caso e inserta la unidad USB en su PC.

C Le pide que realice la presentación sin proyectarla y no inserta el USB.

D Se asegura de que no haya encontrado la unidad USB en un aparcamiento y luego la inserta en su PC.

E Hace varias copias de la unidad USB y le da una a su gestor.

DELL Technologies

RESPUESTA

Ransomware

7

¡BUEN TRABAJO!

No inserte el USB ni proyecte el contenido

Usted no lo sabía, pero un atacante había sobornado al vendedor con una gran cantidad de dinero y la unidad USB contenía archivos payload de ransomware para bloquear todos sus sistemas. Gracias a que no conectó el USB ni descargó ningún archivo, evitó que el atacante obtuviera acceso. ¡Uf!

Siguiente pregunta

DELL Technologies

RESPUESTA

Ransomware

7

¡LE HAN HACKEADO!

No inserte el USB ni proyecte el contenido

Usted no lo sabía, pero un atacante había sobornado al vendedor con una gran cantidad de dinero, y tanto la unidad USB como el archivo para descargar contenían archivos payload de ransomware para bloquear todos sus sistemas. Evite usar unidades USB externas y descargar archivos de orígenes desconocidos en su PC personal o en los de la empresa.

Siguiente pregunta

DELL Technologies

PREGUNTA 8 DE 14

Autenticación de dos factores

Su banco le ha recomendado utilizar la autenticación de dos factores para iniciar sesión en su sitio. Hay otros sitios web que también utilizan este proceso para garantizar la seguridad de los usuarios.

¿Cuál de estos es un ejemplo de autenticación de dos factores?

8

Seleccione la mejor respuesta a continuación

A Escribe su nombre de usuario y contraseña, y le piden que introduzca su PIN para obtener acceso al sitio web.

B Escribe su nombre de usuario y contraseña, además de resolver un CAPCHA en el que tiene que seleccionar los paneles con señales.

C Escribe su nombre de usuario y contraseña, y el sitio web le envía un mensaje de texto a su móvil con un código de un solo uso que introduce en el cuadro indicado en el sitio web.

D Escribe su nombre de usuario, y el sitio web le pide que introduzca un código de un token seguro que cambia cada minuto y está instalado en su móvil.

E Solo A y C.

F Solo C y D.

G Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Autenticación de dos factores

¡BUEN TRABAJO!

Se necesitan ambos

Con la autenticación de dos factores, se necesita una contraseña y un segundo identificador que sea diferente (como un código enviado por mensaje de texto o un número generado en una aplicación) para identificar y autenticar a los usuarios. Esta capa de seguridad hace que los atacantes lo tengan mucho más difícil para obtener acceso a su información.

Siguiente pregunta

DELL Technologies

RESPUESTA

Autenticación de dos factores

BUEN TRABAJO, PERO...

Se necesitan ambos

¡Está muy cerca! Hay dos ejemplos de autenticación de dos factores aquí. Vuelva a intentarlo y compruebe si reconoce el otro.

Siguiente pregunta

DELL Technologies

RESPUESTA

Autenticación de dos factores

¡LE HAN HACKEADO!

¡Vaya! Se necesitan ambos

Con la autenticación de dos factores, se necesita una contraseña y un segundo identificador que sea diferente (como un código enviado por mensaje de texto o un número generado en una aplicación) para identificar y autenticar a los usuarios. Esta capa de seguridad hace que los atacantes lo tengan mucho más difícil para obtener acceso a su información. Si no la usa, se quedará vulnerable ante los atacantes.

Siguiente pregunta

DELL Technologies

PREGUNTA 9 DE 14

Robos por Bluetooth

Después de conducir hasta una senda para pasar una agradable tarde de senderismo, se da cuenta de que se ha dejado el portátil en la mochila y también el móvil (que no tiene cobertura). Necesita dejar el equipo y el móvil en el vehículo, pero quiere que estén seguros.

¿Qué hace?

9

Seleccione la mejor respuesta a continuación

A Desactiva por completo el wifi.

B Pone el portátil en modo de suspensión.

C Deja el portátil y el móvil en el maletero y lo cierra bien.

D Envuelve el portátil y el móvil en una manta gruesa.

E Apaga por completo el portátil y el móvil, lo que también desactiva el Bluetooth.

DELL Technologies

RESPUESTA

Robos por Bluetooth

¡BUEN TRABAJO!

Apague el portátil y el móvil

Aunque siempre es bueno esconder los dispositivos si los vamos a dejar desatendidos, ahora los ladrones usan escáneres de Bluetooth para localizarlos en vehículos cerrados, y no todos los dispositivos desactivan el Bluetooth en el modo de suspensión. A menudo, los robos se producen en sendas y otro tipo de ubicaciones en las que los propietarios permanecen ausentes durante largos periodos de tiempo. Los ladrones siempre están alertas, así que tome precauciones antes de ir a hacer senderismo.

Siguiente pregunta

DELL Technologies

RESPUESTA

Robos por Bluetooth

¡LE HAN HACKEADO!

Apague el portátil y el móvil

Aunque siempre es bueno esconder los dispositivos si los vamos a dejar desatendidos, ahora los ladrones usan escáneres de Bluetooth para localizarlos en vehículos cerrados, y no todos los dispositivos desactivan el Bluetooth en el modo de suspensión. A menudo, los robos se producen en sendas en las que los propietarios permanecen ausentes durante largos periodos de tiempo. Así que tome precauciones antes de ir a hacer senderismo.

Siguiente pregunta

DELL Technologies

PREGUNTA 10 DE 14

Ataque mediante USB, parte 2

Le invade el espíritu navideño y trae un pequeño árbol de Navidad que funciona por USB para decorar la oficina.

¿Cómo lo enciende?

10

Seleccione la mejor respuesta a continuación

A	Lo conecta a su PC.
B	Lo conecta a un cable de extensión USB que se conecta a su PC.
C	Usa un cargador USB específico para conectar el dispositivo a una toma de corriente normal.
D	No hay manera de encenderlo; se cancela la Navidad.
E	Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Ataque mediante USB, parte 2

10

¡BUEN TRABAJO!

Use un cargador USB específico

Esta variante de ataque mediante USB instala malware en muchos tipos de dispositivos (¡incluso en arbolitos de Navidad!) con la esperanza de que terminen conectados a la red de alguna empresa importante. No conecte nunca ningún dispositivo USB desconocido a su PC, aunque solo sea para cargarlo.

Siguiente pregunta

DELL Technologies

RESPUESTA

Ataque mediante USB, parte 2

10

¡LE HAN HACKEADO!

Use un cargador USB específico

Esta variante de ataque mediante USB instala malware en muchos tipos de dispositivos (¡incluso en arbolitos de Navidad!) con la esperanza de que terminen conectados a la red de alguna empresa importante. No conecte nunca ningún dispositivo USB desconocido a su PC, aunque solo sea para cargarlo.

Siguiente pregunta

DELL Technologies

PREGUNTA 11 DE 14

Ataques de "Evil Maid"

Está en una conferencia sobre ciberseguridad en Shanghái (China) y se aloja en un hotel de cinco estrellas. Antes de salir a cenar, deja su PC en la caja fuerte de la habitación.

¿Su PC está bien protegido contra ataques y robos?

11

Seleccione la mejor respuesta a continuación

A No, porque cualquier dispositivo que se deja desatendido puede sufrir una vulneración.

B Sí, porque cerró bien la caja fuerte donde la dejó.

C Sí, porque también colgó ropa en el armario para que no se viera la caja fuerte.

D Sí, porque es un hotel muy bueno.

E Sí, porque no es un PC muy bueno.

DELL Technologies

RESPUESTA

Ataques de "Evil Maid"

11

¡BUEN TRABAJO!

No, cualquier dispositivo puede sufrir una vulneración

Cualquier dispositivo que se deja desatendido puede abrirse y quedar expuesto a través de lo que se conoce como un ataque de "Evil Maid" (criada malvada). En este ataque, un atacante obtiene acceso abriendo él mismo el PC e insertando malware. Cualquier dispositivo que no tenga con usted podrá ser atacado. Recuerde también que no debe dejar a ningún desconocido al cuidado de su dispositivo, especialmente si se trata de una "criada malvada".

Siguiente pregunta

DELL Technologies

RESPUESTA

Ataques de "Evil Maid"

11

¡LE HAN HACKEADO!

No, cualquier dispositivo puede sufrir una vulneración

Cualquier dispositivo que se deja desatendido puede abrirse y quedar expuesto a través de lo que se conoce como un ataque de "Evil Maid" (criada malvada). En este ataque, un atacante obtiene acceso abriendo él mismo el PC e insertando malware. Para protegerlos de verdad, todos los dispositivos deben estar con usted. No deje nunca a un desconocido al cuidado de sus dispositivos, especialmente si se trata de una "criada malvada".

Siguiente pregunta

DELL Technologies

PREGUNTA 12 DE 14

Spyware

Recibe un mensaje de texto de un número que le resulta familiar donde le dicen que su hija ha tenido un accidente y se la han llevado al hospital. Incluye un enlace para ponerse en contacto inmediatamente con el remitente.

Usted:

12

Seleccione la mejor respuesta a continuación

A	Hace clic inmediatamente en el enlace, porque está preocupado por su hija.
B	Busca el número, descubre que pertenece a la zona donde se encontraba su hija y hace clic en el enlace.
C	No hace clic en el enlace, sino que llama a su hija para asegurarse de que está bien.
D	Ninguna de las opciones anteriores.

DELL Technologies

RESPUESTA

Spyware

12

¡BUEN TRABAJO!

No haga clic en el enlace

Este tipo de ataque es un intento de instalar spyware en su móvil. El spyware podría poner en riesgo el móvil y ese riesgo podría extenderse a la red de su empresa. Usted se dio cuenta de que el mensaje no parecía muy real y utilizó otra forma de comprobar que su hija estaba bien. ¡Bien hecho!

Siguiente pregunta

DELL Technologies

RESPUESTA

Spyware

12

¡LE HAN HACKEADO!

No haga clic en el enlace

Este tipo de ataque es un intento de instalar spyware en su móvil. El spyware podría poner en riesgo el móvil y ese riesgo podría extenderse a la red de su empresa. Al hacear clic en el enlace, se introducen archivos payload de spyware en su dispositivo. Simplemente, no se crea los mensajes de desconocidos, aunque sean muy convincentes.

Siguiente pregunta

DELL Technologies

PREGUNTA 13 DE 14

Seguridad de puntos finales

Los agentes de amenazas (podríamos llamarles incluso hackers con intenciones maliciosas) están dirigiendo sus ataques a los puntos finales.

Los puntos finales se definen como:

13

Seleccione la mejor respuesta a continuación

A	Sobremesas.
B	Sobremesas y portátiles.
C	Sobremesas, portátiles y servidores.
D	Sobremesas, portátiles, servidores, la cloud y más.
E	Sobremesas, portátiles, servidores, la cloud y el último destino de mi GPS.

DELL Technologies

RESPUESTA

Seguridad de puntos finales

13

¡BUEN TRABAJO!

Cualquier dispositivo conectado de forma remota

Un punto final es cualquier dispositivo conectado de forma remota a una red. La seguridad de los puntos finales es fundamental para proteger los dispositivos y los datos de su organización, así que asegúrese de estar siempre un paso por delante de los atacantes.

Siguiente pregunta

DELL Technologies

RESPUESTA

Seguridad de puntos finales

BUEN TRABAJO, PERO...

Cualquier dispositivo conectado de forma remota

Un punto final es cualquier dispositivo conectado de forma remota a una red. La seguridad de los puntos finales es fundamental para proteger los dispositivos y los datos de su organización, así que asegúrese de estar siempre un paso por delante de los atacantes.

Siguiente pregunta

DELL Technologies

RESPUESTA

Seguridad de puntos finales

13

¡LE HAN HACKEADO!

Cualquier dispositivo conectado de forma remota

Un punto final es cualquier dispositivo conectado de forma remota a una red. La seguridad de los puntos finales es fundamental para proteger los dispositivos y los datos de su organización, así que asegúrese de estar siempre un paso por delante de los atacantes.

Siguiente pregunta

DELL Technologies

PREGUNTA 14 DE 14

Seguridad de puntos finales, parte 2

Los hackers con intenciones maliciosas tienen como objetivo puntos finales como sobremesas, portátiles, móviles, impresoras inalámbricas, servidores y cualquier otro dispositivo que se conecte a una red.

¿Qué pasos debería seguir para prevenir un ataque?

14

Seleccione la mejor respuesta a continuación

A	Asegurarme de cerrar y bloquear mi dispositivo cuando no lo esté usando.
B	Actualizar mi dispositivo y aplicar los parches necesarios con frecuencia.
C	Tener buenos hábitos de uso del correo electrónico: informar de correos electrónicos sospechosos.
D	No conectar nunca un dispositivo desconocido a mi punto final.
E	Todas las opciones anteriores.

DELL Technologies

RESPUESTA

Seguridad de puntos finales, parte 2

¡BUEN TRABAJO!

Todas las opciones anteriores

Se nota que ha aprendido consejos de ciberseguridad y los está poniendo en práctica. La seguridad de los puntos finales es fundamental para proteger los dispositivos y los datos de su organización, así que asegúrese de estar siempre un paso por delante de los atacantes.

Siguiente pregunta

DELL Technologies

RESPUESTA

Seguridad de puntos finales, parte 2

BUEN TRABAJO, PERO...

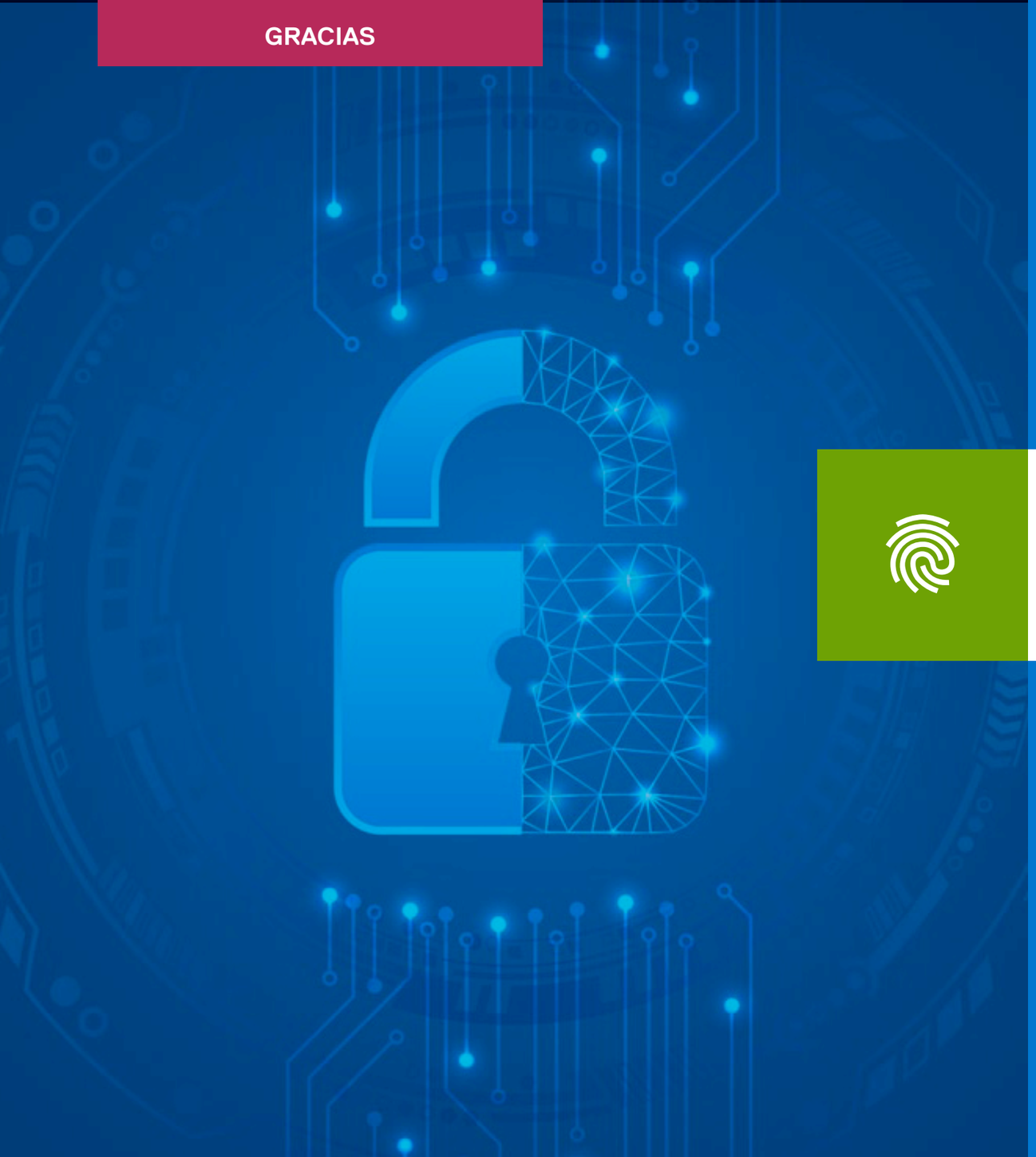
¡Aún hay más!

Hay más de una medida que debe tomar para proteger sus dispositivos. La seguridad de los puntos finales es fundamental para proteger los dispositivos y los datos de su organización, así que asegúrese de estar siempre un paso por delante de los atacantes.

Siguiente pregunta

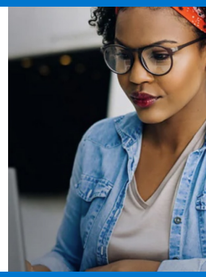
DELL Technologies

GRACIAS



Más información:

Visite **Dell.com/Endpoint-Security**



DELL Technologies