PREGUNTAS FRECUENTES Y RESPUESTAS (ACTUALIZADO 27 DE ABRIL DEL 2021)

El sitio web de la Universidad pudiera parecer algo diferente a cómo era la última vez que Ud. lo visitó. Actualmente estamos en el trámite de ampliar y actualizar nuestra lista de preguntas y respuestas frecuentes y continuaremos haciéndolo a medida que haya más informatción disponible.

Ud. puede inscribirse aquí para los servicios de monitorización de crédito. **Si ya Ud. se inscribió, no tiene necesidad de hacer nada más para activar su monitorización.**

1. **¿Qué ocurrió?**
   El 24 de diciembre del 2020, el Dispositivo de Transferencia de Archivos (FTA, por sus siglas en inglés) de Accellion fue blanco de un ataque internacional en el que los perpetradores se aprovecharon de un punto vulnerable de esa aplicación y atacaron a más de 100 organizaciones, inclusive universidades, entidades gubernamentales y empresas privadas. En relación con el ataque, se tuvo acceso no autorizado a cierta data de la Universidad. El 29 de marzo del 2021 identificamos parte de esa data que fue publicada en Internet.

   Como la Universidad aprecia la privacidad y la seguridad se están mejorando las medidas de seguridad y protección de su información y sistemas. La Universidad ha descomisionado el FTA de Accellion y está haciendo una transición hacia una solución más segura. La Universidad está cooperando con el FBI y colaborando con expertos externos en ciberseguridad a fin de investigar este asunto y determinar qué ocurrió, qué data fue impactada y a quién pertenece esa data.

2. **¿De quién es la información que fue impactada por la filtración de data de Accellion?**
   En cuanto a la investigación, ya hay pruebas que muestran que una entidad no autorizada logró acceder a archivos que contienen información personal perteneciente a miembros de la comunidad de la Universidad, inclusive empleados y sus dependientes, retirados y beneficiarios, donantes y estudiantes actuales o eventuales.

   La Universidad está ocupada en identificar a los miembros de la comunidad cuya información personal y de contacto se haya visto impactada. Estas investigaciones toman tiempo, y estamos trabajando expresamente para proporcionar información precisa lo antes posible. Dentro de los próximos 45 o 60 días esperamos poder enviar notificaciones individuales adecuadas a esas personas cuya información personal haya sido impactada y cuyos detalles de contacto actuales estén disponibles para la Universidad.

3. **¿Qué clase de información ha sido impactada?**
   La información impactada pudiera incluir nombres completos, direcciones, números de teléfono, números de Seguridad Social, información sobre licencia de conducción, pasaporte y financiera, incluso números de cuentas y rutas bancarias, información relacionada con la salud y beneficios, información sobre discapacidades y fecha de nacimiento, así como otra información personal.

   La Universidad está ocupada en identificar a los miembros de la comunidad cuya información personal y de contacto haya sido impactada. Estas investigaciones toman tiempo, y estamos trabajando expresamente para proporcionar información precisa lo antes posible. Dentro de los próximos 45 o 60 días, esperamos poder enviar notificaciones individuales adecuadas a esas personas cuya información personal haya sido impactada y cuyos detalles de contacto actuales estén disponibles para la Universidad.

4. **¿Necesito hacer algo?**
   La Universidad está ofreciendo servicios gratuitos de monitorización y protección contra robo de identidad mediante Experian IdentityWorks; haga clic aquí para inscribirse.

Pedimos a los miembros de la comunidad universitaria que se mantengan alertas contra amenazas de robo o fraudes de identidad. Además de eso, siempre viene bien estar atento a la suplantación de identidad (*phishing*) en *emails* y llamadas telefónicas de alguien que se haga pasar por un conocido suyo o finja ser de una empresa con la que Ud. tenga negocios, y le pide a Ud. información sensitiva, tal como contraseñas, números de Seguro Social o información sobre cuentas financieras. Ud. deberá reportar sospechas de *phishing* o intentos de ingeniería social a communications@ucop.edu.

También queremos recomendarle que use autentificación multifactorial en sus cuentas en línea cuando se las ofrezcan.

INFORMACIÓN SOBRE CÓMO OBTENER UN INFORME DE CRÉDITO GRATIS
Los residentes de EE.UU. tienen derecho, de acuerdo con las leyes estadounidenses, a recibir cada año un informe de crédito gratis de cada uno de los tres principales burós de crédito. Para pedir sus informes de crédito gratuitos, visite www.annualcreditreport.com o llame libre de cargos al (877) 726-1014.

INFORMACIÓN SOBRE COMO IMPLEMENTAR UN ALERTA DE FRAUDE O UNA SUSPENSIÓN POR SEGURIDAD
Ud. puede contactar a los tres principales burós de crédito en las direcciones que aparecen a continuación y pedirles gratuitamente un alerta en su archivo de crédito si Ud. sospechara que pudiera ser víctima de un fraude. El alerta de fraude no afecta su capacidad para obtener crédito o un préstamo. En vez de eso, le avisa a las empresas que su información personal pudiera hallarse comprometida y les exige a las empresas que verifiquen la identidad suya antes de emitir un crédito. Aunque esto pudiera causar alguna demora breve. Si el que está solicitando crédito es Ud., esto pudiera protegerle de alguien que esté usando su nombre para pedir crédito.

Además del alerta de fraude, Ud. pudiera considerar una congelación gratis de su informe de crédito por razones de seguridad. La congelación por seguridad le prohíbe a la agencia de crédito reportar ninguna información del informe de crédito del consumidor sin una autorización por escrito. No obstante, por favor tenga presente que poner una congelación por razones de seguridad en su informe de crédito pudiera demorar, interferir o impedir la aprobación oportuna de cualquier solicitud de nuevos préstamos, créditos, hipotecas, empleos, viviendas u otros servicios que Ud. haga. Una agencia reportadora de crédito no puede cobrarle a Ud. por poner, suspender temporalmente o quitar permanentemente una congelación por seguridad.

Para poner un alerta de fraude en su informe de crédito, Ud. deberá contactar a uno de los tres burós de crédito abajo listados y los otros dos automáticamente añadirán el alerta de fraude. Para poner una congelación por seguridad en su informe de crédito, Ud. tendrá que contactar a los tres burós de crédito abajo listados.

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 (800) 680-7289 www.transunion.com

Para pedir una congelación por seguridad, Ud. tendrá que aportar la siguiente información:
1. Su nombre completo (incluso inicial, así como Jr., Sr., II, III, etc.);
2. Número de Seguridad Social;
3. Fecha de nacimiento;
4. Si Ud. se ha mudado en los últimos cinco (5) años, las direcciones dónde Ud. haya residido durante esos cinco años anteriores;
5. Prueba de su dirección actual, tal como cuentas de servicios públicos o teléfono; y

6. Una fotocopia legible de un carné de identificación expedido por el gobierno (licencia estatal de conductor o tarjeta de ID, identificación militar, etc.).

Ud. también podrá contactar a la Comisión Federal de Comercio de EE.UU. (FTC, por sus siglas en inglés) para pedir más información sobre alertas de fraude, congelaciones por seguridad y cómo protegerse a sí mismo del robo de identidad. Se puede contactar a la FTC en el 400 7th St. SW, Washington, D.C. 20024; teléfono (877) 382-4357; o www.consumer.gov/idtheft.
Ud. puede obtener información de la FTC y de las agencias que emiten reportes crediticios arriba mencionadas acerca de cómo pedir un alerta de fraude y/o una congelación de crédito en su informe de crédito.

5. ¿Cómo puedo averiguar si mi información ha sido expuesta?
En los próximos 45 o 60 días, esperamos poder enviarles notificaciones individuales adecuadas a las personas cuya información personal haya sido impactada y cuyos detalles de contacto actuales estén disponibles para la Universidad. Estas investigaciones toman tiempo y estamos trabajando expresamente, a la vez que tomamos cuidados para proporcionar información precisa lo más rápido que podamos.

6. ¿Está la Universidad proporcionando algún tipo de monitorización de crédito?
Sí. Porque proteger a los miembros de la comunidad de la UC es una alta prioridad. La Universidad rápidamente concertó una monitorización de crédito y servicios de protección contra robo de indentidad gratuitos para toda la comunidad de la Universidad mediante Experian IdentityWorks; haga clic aquí para inscribirse. La Universidad también notificó a la comunidad por *email* y publicó un aviso en sus sitios web. Ciertos campus también presentaron talleres interactivos.

7. ¿Cómo me inscribo en Experian IdentityWorks?
La Universidad ha dispuesto gratuitamente servicios de monitorización de crédito y de protección contra el robo de identidad para toda la comunidad de la Universidad mediante ExperianIdentityWorks; haga clic aquí para la inscripción de adultos y aquí para la inscripción de menores.

8. ¿Qué hago si recibo una confirmación de Experian de que se halló información mía en Internet?
Si Ud. ha recibido un aviso de Experian, eso prueba que el servicio de monitorización está funcionando. El portal de Experian para sus miembros ofrece información acerca de lo que Ud. puede hacer para protegerse a sí mismo.

Experian aconseja a las personas que den varios pasos, según el tipo de información expuesta.

a) Mi dirección de *email* está comprometida; ¿qué debo hacer entonces?
- Considere cambiar la contraseña de su *email* y de otras cuentas que usen su dirección de *email* como nombre de usuario. Use una contraseña fuerte y evite reusar contraseñas en múltiples sitios.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con sus cuentas bancarias y de crédito por si hubiera transacciones extrañas.

b) Mi número de teléfono está comprometido; ¿qué debo hacer entonces?
- Vigile las llamadas sospechosas y contacte a su proveedor de telefonía si estas aumentan notablemente.
- Añada su nombre a la lista nacional de Do Not Call.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.

- Como precaución, ojo con sus cuentas bancarias y de crédito por si hubiera transacciones extrañas.

c) Mi licencia de conductor está comprometida; ¿qué debo hacer entonces?
- Contacte a su Departamento de Vehículos Motorizados (DMV, por sus siglas en inglés) local.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con sus cuentas bancarias y/o de crédito por si hubiera transacciones extrañas.

d) Mi carné médico está comprometido; ¿qué debo hacer entonces?
- Contacte a su proveedor de atención médica para reportar cualquier actividad y verificar que no se haya iniciado ninguna reclamación fraudulenta.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con sus cuentas de seguro médico, así como sus cuentas bancarias y/o de crédito por si hubiera transacciones extrañas.

e) Mi tarjeta de débito, crédito o de compras al detalle está comprometida; ¿qué debo hacer entonces?
- Revise minuciosamente el historial de transacciones de la cuenta por si hubiera cargos extraños.
- Si Ud. detecta cargos extraños u otras actividades sospechosas, contacte a su institución financiera para cancelar su tarjeta y/o reportarla robada.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con las otras cuentas bancarias y de crédito por si hubiera transacciones extrañas.

f) Mi pasaporte está comprometido; ¿qué debo hacer entonces?
- Contacte a la oficina de Pasaportes de EE.UU. (o a su embajada o consulado respectivo, si su pasaporte fuera de otro país).
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.

g) Mi cuenta bancaria está comprometida; ¿qué debo hacer entonces?
- Revise minuciosamente el historial de transacciones de la cuenta por si hubiera cargos extraños.
- Si Ud. detecta cargos extraños u otra actividad sospechosa, contacte a su institución financiera y cierre su cuenta bancaria y/o de tarjeta.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con otras cuentas bancarias y/o de tarjeta por si hubiera transacciones extrañas.

h) Mi número de Cuenta Bancaria Internacional (IBAN, por sus siglas en inglés) está comprometido; ¿qué debo hacer entonces?
- Revise el historial de transacciones de la cuenta por si hubiera cargos extraños.
- Si Ud. detecta cargos extraños u otra actividad sospechosa, contacte a su institución financiera y cierre su cuenta bancaria y/o de tarjeta.
- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con otras cuentas bancarias y/o de tarjeta por si hubiera transacciones extrañas.

i) Mi número de ID nacional está comprometido; ¿qué debo hacer entonces?

- Revise sus informes de crédito en los tres burós (Experian, Equifax y Transunion) por si hubiera nuevas actividades.
- Como precaución, ojo con sus cuentas bancarias y/o de tarjeta por si hubiera transacciones extrañas.

j) He recibido el nombre de una empresa infiltrada en mi notificación de Vigilancia de Internet por Experian.

Esa es potencialmente la compañía o sitio web donde se originó el compromiso en Internet. Los *hackers*, cuando comparten data robada en la web oscura, a veces dan el nombre de la compañía o sitio web infiltrado de donde se extrajo la información. En situaciones como esta Ud. pudiera ver una referencia a la UC.

Si Ud. no reconoce el nombre de la compañía infiltrada como el de una con la que Ud. tenga una relación, pudiera ser el de una tercera parte u organización conectada por interfaz a una compañía con la que Ud. tenga negocios. Un ejemplo hipotético pudiera ser el que su información haya quedado expuesta durante la infiltración de un procesador de pagos asociado con una aerolínea comercial a la que Ud. le haya comprado boletos.

k) Se ha detectado una nueva indagación; ¿qué debo hacer entonces?

Si Ud. reconoce o autorizó esta actividad, no hace falta hacer nada. De lo contrario, aquí hay más información que pudiera ayudar.

Si Ud. sigue convencido de que Ud. no autorizó esa actividad, he aquí los pasos que Ud. debe dar:
- Contacte al acreedor – esto pudiera aclarar lo que está sucediendo.
- Revise su informe de crédito por si hubiera una nueva actividad.
- Dispute la información de la cuenta en su informe de crédito.

l) Se ha detectado una nueva cuenta o cambio; ¿qué debo hacer entonces?

Si Ud. reconoce o autorizó esa actividad, no hace falta hacer nada. De lo contrario, aquí hay más información que pudiera ayudarle.

Si Ud. sigue convencido de que Ud. no autorizó esa actividad, hay pasos que Ud. debe dar.
- Contacte al acreedor – esto pudiera aclarar lo que está sucediendo.
- Revise su informe de crédito respecto a la nueva actividad.
- Dispute la información de la cuenta en su informe de crédito.

m) No reconozco el nombre de una compañía en mi informe de crédito.

Si Ud. no está seguro de si Ud. inició la actividad que aparece en su alerta, he aquí alguna información que pudiera ayudarle:

¿Solicitó Ud. recientemente un crédito o la apertura de una nueva cuenta? He aquí algunas compañías cuyos nombres Ud. pudiera encontrar en su alerta, que tal vez no le resulten conocidos a primera vista:
- JPMCB (alias JP Morgan Chase Bank)
- CBNA (alias Citibank)
- CapOne (alias CapitalOne)
- FNBO (alias First National Bank of Omaha)
- TBH (alias The Home Depot)
- Synchrony Bank – Proveedor de crédito y préstamos que típicamente trabaja con grandes detallistas.
- Credco – Esta es una agencia externa que reporta. A menudo las compañías hipotecarias, instituciones financieras, y concesionarios contactan a ese tipo de agencias reportadoras para obtener una puntuación de tres burós.

- Ally – El Banco Ally es un proveedor de crédito y préstamos que típicamente trabaja con grandes detallistas de varios sectores, tales como financiamiento de autos, patrocinadores de valores agregados y finanzas corporativas.

n) Solicité un crédito, pero no he recibido un alerta

La mayoría de los prestamistas reportan actividad en una cuenta dentro de 30 días, pero algunos pueden tardar hasta 90 días. También hay algunos acredores más pequeños que solo reportan a una de las tres agencias nacionales que reportan a los consumidores - Equifax, Experian y TransUnion. Si su acreedor no reporta a las tres, entonces Ud. no recibirá un alerta de las tres por la misma actividad.

o) ¿Por qué recibí más de un alerta por la misma solicitud de préstamo?

He aquí algunas razones comunes de que Ud. recibirá múltiples alertas por la misma solicitud de préstamo:

- Si se aprobó el préstamo y el prestamista abrió una cuenta a nombre suyo, Ud. recibirá un alerta por el informe de crédito inicial para procesar su solicitud y también otro alerta por la apertura de la cuenta.
- Si el prestamista reportó su cuenta a los tres principales burós de crédito - Experian, Equifax y TransUnion – Ud. pudiera recibir un alerta de cada buró.

p) Mi número de Seguridad Social está comprometido, ¿qué debo hacer entonces?

Ud. puede llamar a Experian al (888) 397 3742. Pedimos a los miembros de la comunidad de la Universidad que se mantengan atentos contra las amenazas de robo de identidad y/o fraude. Además de eso, siempre viene bien estar al tanto de *emails* de *phishing* y/o llamadas telefónicas de alguien que lo trate a Ud. como si lo conociera o pretende ser de una compañía con la que Ud. tal vez tenga negocios, y le pìde información sensitiva, tal como contraseñas, número de Seguridad Social o información sobre cuentas financieras. Ud. puede reportar sospechas de *phishing* o intentos de ingeniería social a communications@ucop.edu. También le recomendamos que use autentificación multifactorial en sus cuentas en línea cuando se lo ofrezcan.

INFORMACIÓN SOBRE COMO OBTENER UN INFORME DE CRÉDITO GRATIS

Los residentes de EE.UU. tienen derecho de acuerdo con las leyes estadounidenses a un informe de crédito gratuito anual de cada uno de los tres principales burós de crédito. Para pedir sus informes gratuitos de crédito, visite www.annualcreditreport.com o llame sin cargos al (877) 726-1014.

INFORMACIÓN SOBRE COMO IMPLEMENTAR UN ALERTA DE FRAUDE O UNA SUSPENSIÓN POR SEGURIDAD

Ud. puede contactar a los tres principales burós de crédito en las direcciones que aparecen a continuación y pedirles que pongan un alerta en su archivo de crédito si Ud. sospecha que pudiera ser víctima de un fraude. El alerta de fraude no afecta su capacidad para obtener crédito o un préstamo. En vez de eso, le avisa a las empresas que su información personal pudiera hallarse comprometida y les exige a las empresas que verifiquen la identidad de Ud. antes de emitir un crédito. Aunque esto pudiera causar alguna demora breve. Si el que está solicitando crédito es Ud., esto pudiera protegerle de alguien que esté usando su nombre para pedir crédito.

Además del alerta de fraude, Ud. pudiera considerar una congelación gratis de su informe de crédito por razones de seguridad. La congelación por seguridad le prohíbe a la agencia de crédito reportar ninguna información del informe de crédito del consumidor sin una autorización por escrito. No obstante, por favor tenga presente que poner una congelación por razones de seguridad en su informe de crédito pudiera demorar, interferir o impedir la aprobación oportuna de cualquier solicitud de nuevos préstamos, créditos, hipotecas, empleos, viviendas u otros servicios que Ud. haga. Una

agencia reportadora de crédito no puede cobrarle a Ud. por poner, suspender temporalmente o quitar permanentemente una congelación por seguridad.

Para poner un alerta de fraude en su informe de crédito, Ud. deberá contactar a uno de los tres burós de crédito abajo listados y los otros dos automáticamente añadirán el alerta de fraude. Para poner una congelación por seguridad en su informe de crédito, Ud. tendrá que contactar a los tres burós de crédito abajo listados.

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 (800) 680-7289 www.transunion.com

Para pedir una congelación por seguridad, Ud. tendrá que aportar la siguiente información:
1. Su nombre completo (incluso inicial, así como Jr., Sr., II, III, etc.);
2. Número de Seguridad Social;
3. Fecha de nacimiento;
4. Si Ud. se ha mudado en los últimos cinco (5) años, las direcciones dónde Ud. haya residido durante esos cinco años anteriores;
5. Prueba de su dirección actual, tal como cuentas de servicios públicos o teléfono; y
6. Una fotocopia legible de un carné de identificación expedido por el gobierno (licencia estatal de conductor o tarjeta de ID, identificación militar, etc.).

Ud. también podrá contactar a la Comisión Federal de Comercio de EE.UU. (FTC, por sus siglas en inglés) para pedir más información sobre alertas de fraude, congelaciones por seguridad y cómo protegerse a sí mismo del robo de identidad. Se puede contactar a la FTC en el 400 7th St. SW, Washington, D.C. 20024; teléfono (877) 382-4357; o www.consumer.gov/idtheft.
Ud. puede obtener información de la FTC y de las agencias que emiten reportes crediticios arriba mencionadas acerca de cómo pedir un alerta de fraude y/o una congelación de crédito en su informe de crédito.

9. ¿Puedo recibir monitorización de crédito si no soy un residente documentado?
Para recibir servicios de crédito, Ud. deberá ser mayor de 18 años, tener crédito establecido en los EE.UU., tener un número de Seguridad Social a nombre suyo y tener una dirección docimiciliaria en EE.UU. que aparezca en su archivo de crédito.

10. ¿Debo notificar a la Universidad acerca de cualquier data mía que haya sido afectada, además de proceder con Experian y emprender una acción directa?
No es necesario notificar a la Universidad acerca de la data afectada a causa del caso de Accellion. La Universidad está trabajando para identificar a los miembros de la comunidad cuya información personal y de contacto hayan sido impactadas. Estas investigaciones toman tiempo y estamos trabajando expresamente, a la vez que tomamos medidas para proporcionar información precisa lo más rápido que podamos. Dentro de los próximos 45 – 60 días, esperamos tener la información que necesitemos para enviar notificaciones individuales a aquellos cuya información de contacto actual esté disponible para la Universidad.

11. ¿Puedo checar mis informes de crédito?
Sí. Las agencias de monitorización de crédito recomiendan que usted revise su informe de crédito al menos una vez al año, o más a menudo, como parte de sus prácticas de administración de finanzas. Algunos individuos prefieren checar sus puntuationes crediticias mensualmente o incluso

semanalmente. Ud. puede checar su puntuación crediticia tan a menudo como quiera sin que eso afecte su puntuación.

12. **¿Tengo que pagar por el informe de crédito?**
    Ud. puede pedir sus informes de crédito gratuitamente a los tres burós de crédito una vez al año. Ud. puede hacerlo en línea en www.annualcreditreport.com o por teléfono al 1-877-322-8228.

13. **¿Qué hace Ud. para mejor asegurar que las redes de la Universidad respondan a esta situación?**
    Cuando descubrimos el asunto, sacamos de línea el Accellion FTA y tapamos la vulnerabilidad. Hay pruebas de que otros sistemas de la Universidad fueron impactados. Estamos en el trámite de hacer una transición a un nuevo sistema para transferir data con mejores controles de seguridad, desplegando una monitorización adicional del sistema a través de nuestra red, efectuando un chequeo de seguridad en ciertos sistemas y mejorando los controles, procesos y procedimientos de seguridad.

14. **Se ha resuelto la situación?**
    Sí. Cuando descubrimos el asunto, sacamos de línea el sistema y tapamos la vulnerabilidad de Accellion. No hay evidencia de que otros sistemas de la Universidad hayan sido impactados. Estamos en el proceso de transición a un nuevo sistema para transferir archivos. Estamos en el proceso de transición a un sistema de monitorización adicional con mejores controles de seguridad, desplegando una monitorización de sistema adicional en toda nuestra red, efectuando chequeos de salud de la seguridad de ciertos sistemas y mejorando los controles, procesos y procedimientos de seguridad

15. **¿Han notificado Uds. a las autoridades apropiadas?**
    Sí. La Universidad ha reportado el asunto a las autoridades policiales federales de los EE.UU.

16. **¿Qué es la autentificación multifactorial?**
    La autentificación es el proceso de determinar si alguien o algo es, en efecto, quién o qué, el/lo que se declara a sí mismo.La autentificación multifactorial (MFA) es un sistema de seguridad que requiere más de un método de autentificación de categorías independientes de credenciales para verificar la identidad para conectarse (*login*) u otra transacción. La autentificación multifactorial combina dos más credenciales independientes: que el usuario conoce (contraseñas), que el usuario tiene (*token* de seguridad) y que el usuario es quien dice ser (verificación biométrica).

17. **¿Qué debo hacer si tengo más preguntas?**
    Las preguntas acerca de este incidente pueden remitirse a communications@ucop.edu.