JFStrategy

Estudio

Percepción sobre **seguridad digital** en México

2020-2021

Estudio de percepción

Seguridad digital en México 2020-2021

Agradecemos la valiosa colaboración de todas las personas que hicieron posible la publicación de este estudio, con especial reconocimiento a quienes aportaron su tiempo, saber y perspectiva para responder el cuestionario, materia prima de esta investigación.

Los resultados del estudio expresan la opinión de los encuestados y pueden o no reflejar el punto de vista de los investigadores.

Colaboradores:

Juan Francisco Serrano
Dirección

Víctor Hugo O'Farrill
Coordinación y promoción

Eduardo Zimbrón
Diseño de investigación y análisis

Contenido

INTRODUCCIÓN **3**

CONCLUSIONES **4**

OBJETIVOS DEL ESTUDIO **7**

METODOLOGÍA **7**

RESULTADOS **9**

¿QUÉ SE ENTIENDE POR SEGURIDAD EN MEDIOS DIGITALES? 9
PRINCIPALES AMENAZAS IDENTIFICADAS EN MEDIOS DIGITALES 10
Amenazas en Internet *11*
Amenazas en redes sociales *12*
Amenazas en comercio electrónico *13*
Amenazas en banca electrónica *15*
Amenazas en correo electrónico *16*
Amenazas en apps móviles *17*
SITIOS O *APPS* DE COMPRAS O SERVICIOS EN LÍNEA CONSIDERADAS CONFIABLES Y SEGURAS 18
SITIOS O *APPS* DE COMPRAS O SERVICIOS EN LÍNEA CONSIDERADAS NO CONFIABLES O INSEGURAS 20
*Principales razones y comentarios de por qué los sitios mencionados se consideran **no** confiables o inseguros* *21*
RECURSOS DE APOYO IDENTIFICADOS QUE AYUDAN A INCREMENTAR LA SEGURIDAD EN LA COMUNICACIÓN O TRANSACCIONES EN LÍNEA 24
SEGURIDAD EN LOS SERVICIOS DE ALMACENAMIENTO EN LA NUBE 26
Otros servicios de almacenamiento en nube mencionados *28*
Razones por las cuales los servicios de almacenamiento en la nube son percibidos como seguros o inseguros *29*
Opiniones que apoyan la percepción de seguridad de los sitios mencionados 29
Opiniones que apoyan la percepción de inseguridad de los sitios mencionados 32
Opiniones generales o mixtas acerca de los sitios mencionados 34
ACCIONES CONCRETAS COMPARTIDAS POR LOS ENTREVISTADOS 35
PRINCIPALES RETOS PARA LAS EMPRESAS Y ORGANIZACIONES 37
SITUACIÓN DE MÉXICO FRENTE A OTROS PAÍSES EN MATERIA DE SEGURIDAD EN MEDIOS DIGITALES 40
Razones por las que se tiene esa percepción *40*
PRINCIPALES RETOS QUE ENFRENTA MÉXICO COMO PAÍS EN MATERIA DE SEGURIDAD EN MEDIOS DIGITALES 43

GLOSARIO DE TÉRMINOS **45**

ARTÍCULOS DE INTERÉS **50**

LA IMPORTANCIA (CASI SIEMPRE COMENTADA PERO RARA VEZ EJECUTADA) DE LOS PROCESOS EN LA SEGURIDAD DE LA INFORMACIÓN. 51
EL PAPEL DEL USUARIO EN LA SEGURIDAD DE LA CIUDADANÍA DIGITAL 53
CULTURA DE RIESGOS A TRAVÉS DEL LIDERAZGO 55
¿POR QUÉ ES RELEVANTE LA SEGURIDAD EN UN SITIO WEB? 56

ANEXOS **59**

ANEXO 1. LISTA DE PARTICIPANTES EN LA ENCUESTA 60
ANEXO 2. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN INTERNET EN GENERAL 64
ANEXO 3. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN REDES SOCIALES 66
ANEXO 4. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN COMERCIO ELECTRÓNICO 68
ANEXO 5. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN BANCA ELECTRÓNICA 69
ANEXO 6. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN CORREO ELECTRÓNICO 71
ANEXO 7. RESPUESTAS MÁS RELEVANTES SOBRE LAS AMENAZAS PERCIBIDAS EN *APPS* MÓVILES 72

ANEXO 8. RELACIÓN DE SITIOS/*APPS* PERCIBIDOS COMO SEGUROS O INSEGUROS, QUE TUVIERON SÓLO 1 MENCIÓN 74
ANEXO 9. RELACIÓN DE *SOFTWARE* O RECURSOS DE APOYO QUE AYUDAN A INCREMENTAR LA SEGURIDAD, QUE TUVIERON SÓLO 1 MENCIÓN.... 76
ANEXO 10. ACCIONES CONCRETAS APLICADAS QUE FUERON COMPARTIDAS POR LOS ENTREVISTADOS..... 77
ANEXO 11. RAZONES MÁS RELEVANTES DE POR QUÉ SE CONSIDERA QUE MÉXICO SE ENCUENTRA MEJOR, IGUAL O PEOR QUE OTROS PAÍSES. 80
ANEXO 12. LISTA DE LOS RETOS MÁS RELEVANTES DE MÉXICO, TAL COMO FUERON MENCIONADOS POR LOS ENTREVISTADOS 85

Introducción

La vida personal y empresarial se ha vuelto cada vez más digital. La tecnología y los medios digitales han transformado casi cualquier actividad humana. Esa apertura a medios digitales conlleva un riesgo: la seguridad.

La seguridad en los medios digitales incluye, generalmente, tres modalidades:

Evitar la extracción (robo) o intrusión (modificación) de información.
Asegurar que la información esté disponible cuando se requiere.
Salvaguardar la integridad de la información.

Ante la necesidad de contar con información específica de México acerca de la percepción que se tiene sobre la seguridad en medios digitales, Joint Future Strategy, en coordinación con otras organizaciones interesadas en la comprensión y difusión del tema, encabeza este estudio enfocado a evaluar el grado de conocimiento y la percepción que existe al respecto, recopilando la opinión de expertos en la materia, usuarios y ejecutivos importantes de diversas empresas y organizaciones.

JFStrategy ha llevado a cabo investigaciones similares en años anteriores, centradas en la seguridad informática. Para lograr un mayor contexto, este estudio intenta obtener datos sobre medios digitales en general, precisamente por el auge y la prevalencia de actividades digitales en México y en el mundo.

Para facilitar la clasificación, los medios digitales se han divido en grandes rubros:

Internet
Redes sociales
Comercio electrónico
Banca electrónica
Correo electrónico
Apps móviles

En los últimos meses de 2019 y principios de 2020, se llevaron a cabo las encuestas entre usuarios, especialistas y empresarios para producir el **Estudio de seguridad en medios digitales en México 2020**, con el propósito de dar visibilidad al tema y servir como base de futuras comparaciones.

Conclusiones

1. La mayoría de los entrevistados señaló que los grandes retos de México en la materia de seguridad digital son:

    a. Voluntad / certeza jurídica
    b. Culturización / difusión
    c. Mayor capacitación/ educación sobre el tema

    La primera parte de estos tres rubros, se percibe como tarea del gobierno. En los dos segundos, la opinión generalizada es que gobierno, instituciones, iniciativa privada y los usuarios comparten responsabilidades.

2. Resulta paradójico que la capacitación haya sido mencionada sólo por 5 entrevistados entre las acciones de seguridad digital que han realizado, o están llevando a cabo, en sus organizaciones, siendo la falta de cultura digital uno de los factores que más vulneran los entornos transaccionales y de manejo de información a través de medios digitales (y uno de los rezagos de mayor peso percibidos por los propios entrevistados).

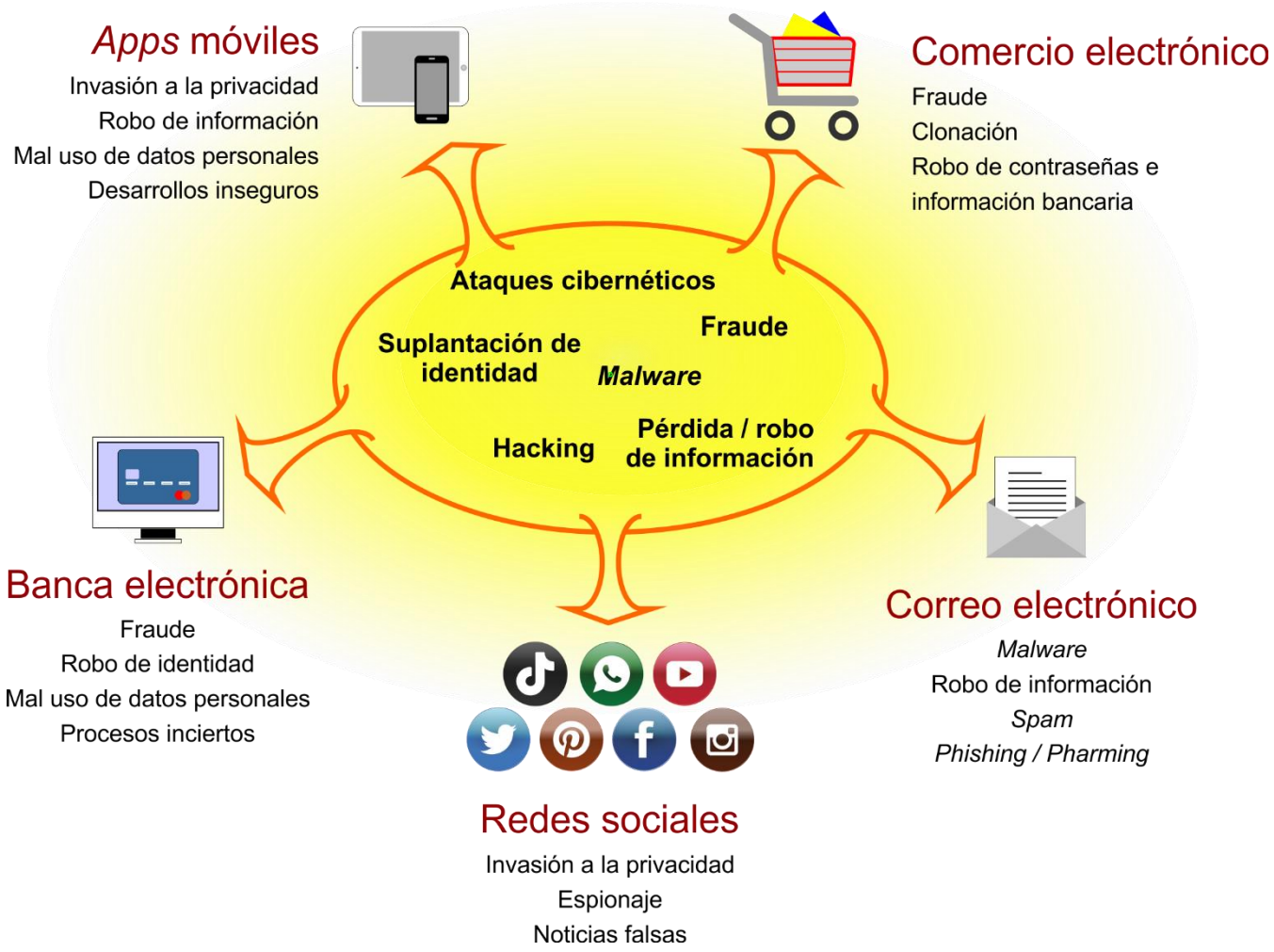
3. Entre los factores de riesgo y las soluciones que permiten minimizar los riesgos, el tema de procesos tuvo menciones muy escasas.

4. La situación de México frente a otros países es considerada como "peor" por un 43% de los entrevistados; sólo un 10% piensa que es mejor. Las principales razones de la percepción negativa giran alrededor de la deficiente inversión en tecnología de seguridad, la poca conciencia sobre el tema por parte de la población, la escasa educación general y la limitada difusión. Quienes perciben que hay un rezago tecnológico en México mencionan que es provocado, entre otras causas, por una inversión reducida, huecos legales y poca atención gubernamental; no hay un compromiso regulatorio y generalmente existe una postura laxa o reactiva.

5. La gran mayoría de los recursos de apoyo identificados para incrementar la seguridad digital transaccional está relacionada con insumos tecnológicos, así como con las plataformas e infraestructura de proveedores de servicios en línea. Sólo un pequeño número de entrevistados mencionó acciones que corresponden al usuario (como contraseñas seguras o ampliar su propia cultura sobre el tema). En general, en todo el estudio, se puede apreciar que existe una percepción de que la seguridad es más una responsabilidad que recae en el proveedor de servicios o productos que en el usuario.

6. Los encuestados muestran un alto nivel de conciencia sobre las amenazas del mundo digital. Sus respuestas mencionan una gama de posibilidades que pueden vulnerar sus empresas y su persona. Hay suficiente consenso como para decir que, en general, perciben que tienen a la mano diversas medidas para minimizar las amenazas propias de la existencia digital.

7. Por lo común, independientemente del medio digital al que se refieran, las amenazas que más preocupan a los entrevistados son ataques cibernéticos/*malware*, posibilidades de fraude, suplantación de identidad, *hacking* y pérdida/robo de información. Sin embargo, hay algunas amenazas que se asocian de manera más específica a un canal determinado, como puede observarse en el siguiente esquema:



8. Hay un número considerable de respuestas que muestran preocupación por la invasión de la privacidad, aun sin que necesariamente se genere un detrimento económico.

9. Se observa un segmento que está preocupado por la prevalencia de las noticias e información falsas como un asunto de seguridad, tanto porque pueden provocar acciones "desinformadas" como por generar confusión en el proceso de decisión. Conllevan una sobresaturación de mensajes que dificulta distinguir lo importante de lo trivial.

10. Se puede concluir que el mundo digital es percibido como riesgoso, con impactos de amplio espectro. Entre las acciones necesarias para disminuir riesgos manifestadas por los entrevistados, se requiere:

    a. Incrementar la voluntad de atender el problema en el nivel gubernamental y en el organizacional.
    b. Incentivar una mayor cultura de seguridad digital, a través de difusión permanente y del fortalecimiento tanto de la capacitación como de los programas educativos.
    c. Mayor inversión en infraestructura y actualización continua de los sistemas.
    d. Cumplir con mayor cabalidad con los estándares internacionales y las recomendaciones del sector financiero.
    e. Construir políticas que den certeza jurídica a empresarios, proveedores e inversionistas.
    f. Extender las medidas de seguridad (infraestructura, educación, procesos) a todos los sectores y a la población en general.
    g. Fomentar la innovación en materia de seguridad digital en el país.
    h. Lograr una mayor colaboración intersectorial.

11. Existen opiniones divergentes respecto de la seguridad en el uso de banca electrónica. Por un lado, hay quienes perciben que es uno de los canales digitales más seguros y confiables (entre otras razones, por el cuidado y la fuerte inversión destinada a este rubro por parte de los bancos), mientras que otros entrevistados desconfían de la infraestructura tecnológica y los procesos de este mecanismo al considerarlos vulnerables. En general, el temor a ser víctimas de fraude por esta vía es alto.

12. El espionaje es una amenaza percibida en diversos canales digitales, aunque con matices diferentes. En las redes sociales, se habla de la posibilidad de que sujetos no autorizados tengan acceso a información personal confidencial, que podría ser mal utilizada por el crimen o como elemento para atacar o desprestigiar a las personas. En cuanto al uso de *apps*, se menciona el almacenamiento que los proveedores hacen de la información del usuario (personal y de rutas de navegación) y las facilidades de geolocalización, acceso a cámara y micrófono de los dispositivos como las acciones que permiten el registro de hábitos y comportamiento, vigilancia cibernética, hostigamiento comercial y mal uso de datos personales.

Objetivos del estudio

- Conocer la percepción de ejecutivos de distintos niveles acerca del estado que guarda la seguridad en medios digitales dentro de su empresa y en México en general con respecto a otros países.
- Recabar la opinión sobre los niveles de seguridad en diversos sitios de Internet, *apps* y plataformas que ofrecen servicios o compras en línea.
- Identificar los principales retos percibidos que enfrentan las personas y organizaciones en materia de seguridad en medios digitales.
- Conocer la percepción general (puntos fuertes y deficiencias) acerca de la cultura de seguridad en medios digitales en México.

Metodología

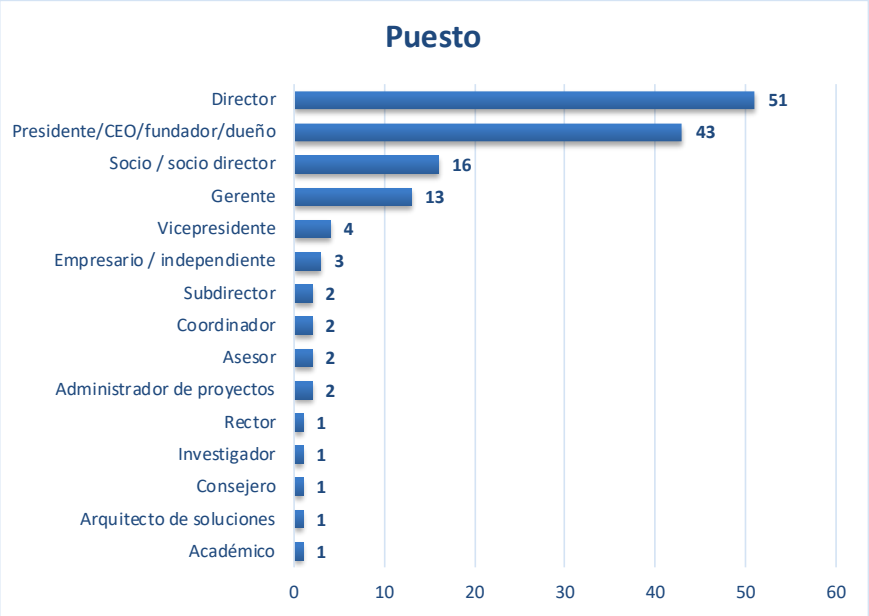
Método de investigación

Se utilizó la encuesta *online* como método de investigación, aplicando un cuestionario estructurado como instrumento de medición.

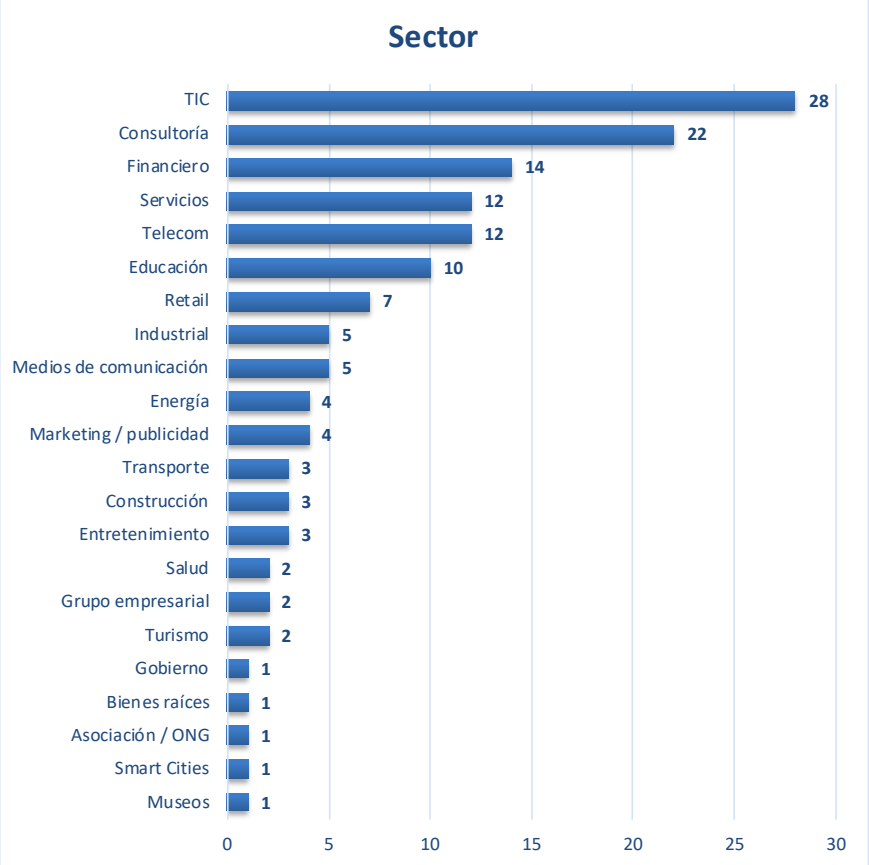
Sobre una base de datos depurada de directivos y ejecutivos de alto nivel de distintos sectores, se extendió una invitación a participar en el estudio. De este ejercicio, se obtuvo un total de 143 encuestas efectivas.

La mayoría de las preguntas del cuestionario fueron intencionalmente diseñadas para que los encuestados dieran respuestas abiertas, con el propósito de recabar con precisión lo que pensaban o percibían sobre los temas de investigación, sin inducir sus afirmaciones ni limitar sus alcances. Para efectos de graficación y comprensión, las respuestas fueron codificadas y agrupadas por analistas especializados bajo términos equivalentes.

Perfil de los entrevistados



(respuestas totales: 143)



(respuestas totales: 143)

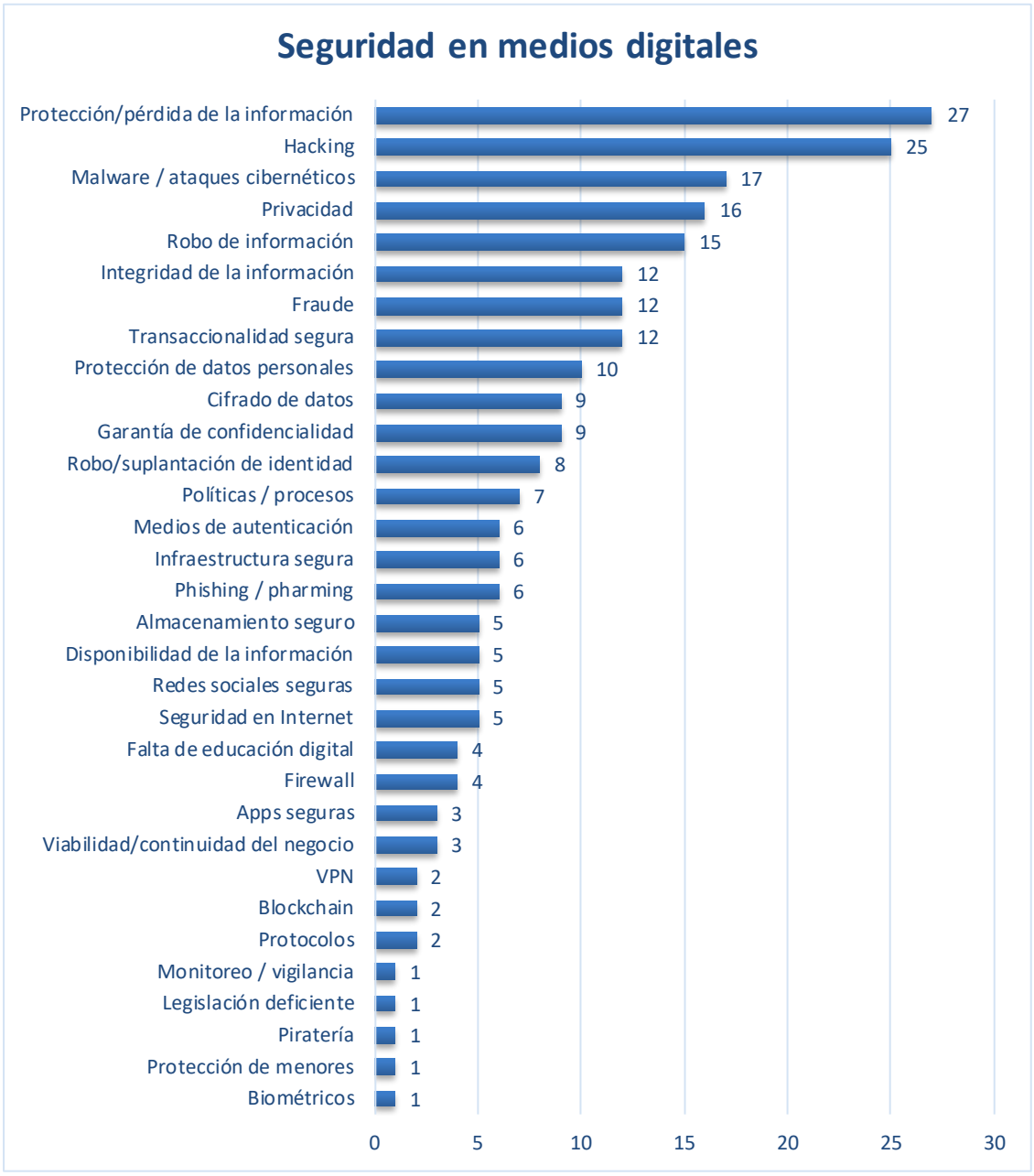
La lista de participantes se desglosa en el Anexo 1

Resultados

¿Qué se entiende por seguridad en medios digitales?

Pregunta: Ante el término “seguridad en medios digitales”, ¿qué le viene a la mente?

La pregunta se planteó de forma abierta y, posteriormente, las respuestas fueron codificadas en categorías, como se muestra en la gráfica:



La pregunta se realizó en forma abierta con el propósito de que los entrevistados expresaran de manera espontánea los conceptos que asocian al término de "seguridad en medios digitales" y no limitar sus respuestas con ideas predeterminadas.

Los conceptos que más se asocian con el tema giran alrededor de la necesidad de que la información empresarial **permanezca íntegra y no se pierda**, esté **disponible** siempre que los usuarios la requieran y que **personas no autorizadas no tengan acceso** a ella (robo de información / confidencialidad).

Asimismo, la seguridad en medios digitales se relaciona con la protección ante posibles **actividades delictivas**, como ataques cibernéticos y *malware*, fraude (mencionado tal cual como fraude o en términos de robo, *phishing*, *pharming*, suplantación de identidad, ingeniería social) y con **cuestiones técnicas** asociadas, como antivirus, cifrado de datos, medios de autenticación, infraestructura, *firewalls*, VPN, *blockchain* y protocolos, entre otros.

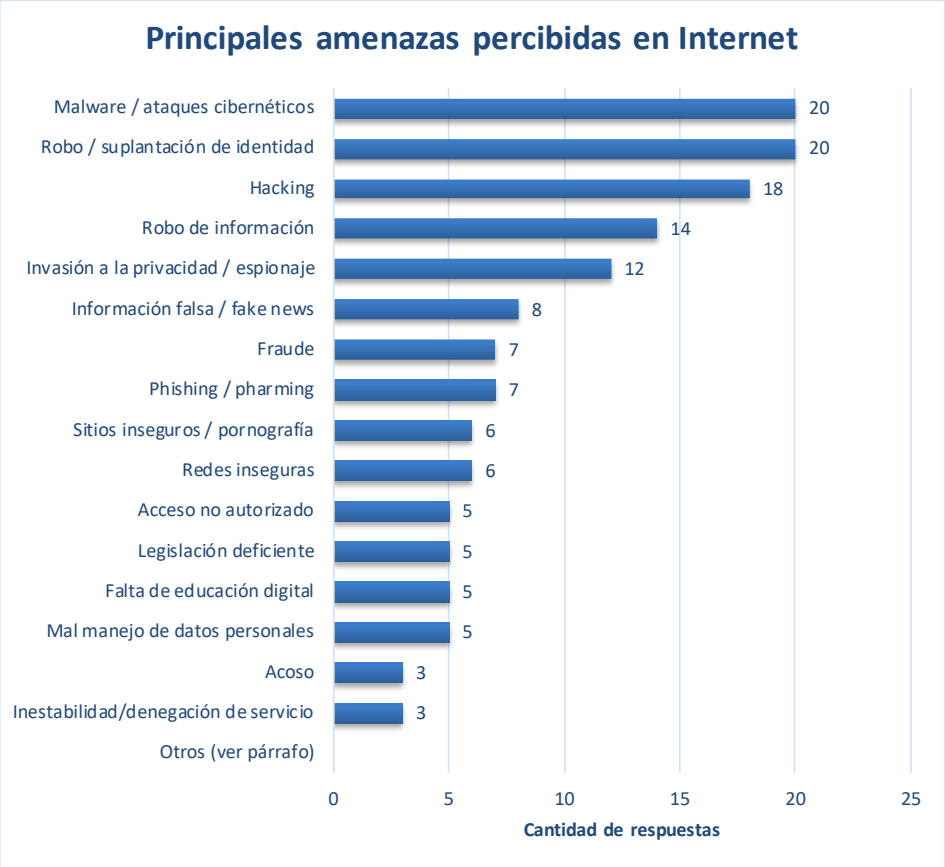
Principales amenazas identificadas en medios digitales

Pregunta: En general, y sin mencionar marcas, empresas u organizaciones, ¿cuáles son las principales amenazas que percibe en los siguientes rubros?

- Internet en general
- Redes sociales
- Compras en línea
- Banca electrónica
- Correo electrónico
- *Apps* para *smartphones*

Describa el riesgo de manera genérica.

Amenazas en Internet



*Las **amenazas percibidas en el rubro "Otros"** son las siguientes: delincuencia organizada,* pharming*, vulnerabilidad de menores, transaccionalidad insegura, sistemas intrusivos, clonación, concentración de servicios en pocos proveedores, políticas/procesos ausentes o deficientes, riesgos en la integridad de la información, arquitectura de sistemas vulnerable, protocolos en conflicto, medios de autenticación deficientes. Dos de los entrevistados mencionaron "Ninguna", indicando que no perciben que existan amenazas en el Internet en general. Ver las respuestas más relevantes enlistadas en el Anexo 2.*

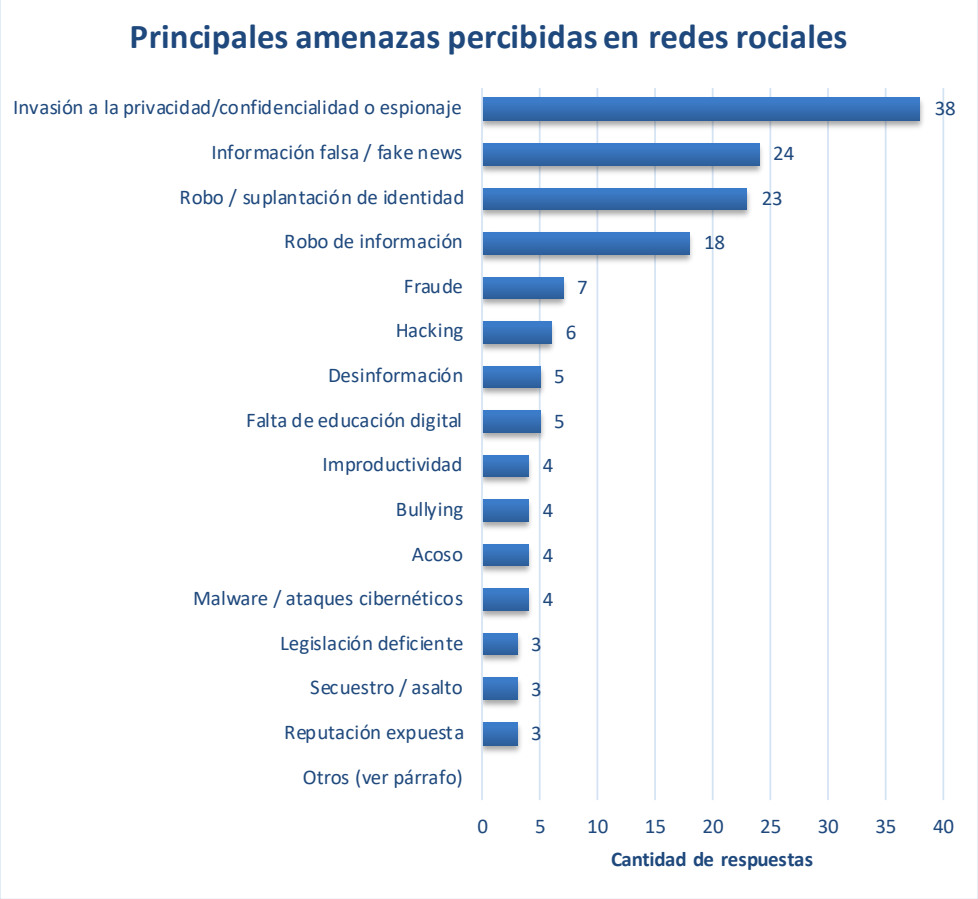
Los ataques cibernéticos, incluyendo diversos tipos de *malware*, la suplantación de identidad, el hackeo de los sistemas y el robo de información, son sin duda las amenazas mencionadas con mayor recurrencia. La posibilidad de ser víctima de algún tipo de fraude, a través de este canal, es también una preocupación evidente. Estas amenazas suelen ser comunes a todos los medios digitales.

De manera particular dentro del concepto de Internet en general, se observa la mención de conceptos específicos, como son el caso del **espionaje**, la difusión de **noticias falsas**, el acceso a la **pornografía** y otros sitios no confiables.

El espionaje se liga a la intromisión de personas en la información personal confidencial, así como al hecho de que algunas empresas tienen acceso a patrones de comportamiento, hábitos y características personales de la gente, a través de *cookies*, pixeles de rastreo u otros mecanismos de recolección oculta de información.

Hubo diversos comentarios que mostraban preocupación por la información sensible, como los datos bancarios y la información personal.

Amenazas en redes sociales



*Las **Amenazas percibidas en el rubro "Otros"** son las siguientes: pornografía, vulnerabilidad de menores, ingeniería social,* phishing*, conspiración,* deepfakes*,* pharming*,* grooming*, depresión, bots. Ver las respuestas más relevantes enlistadas en el Anexo 3*.

La mayoría de las menciones giraron alrededor de la *invasión a la privacidad / espionaje*. El hecho de que las personas compartan información personal a través de las redes sociales a las que se suscriben (de manera intencional o sin saberlo) es considerado como una

vulnerabilidad importante. Hay quien piensa que muchas actividades criminales se facilitan por estos medios.

En segundo lugar, se indicó la exposición a información falsa o *fake news* (16.78% de los entrevistados) como otro de los temores o amenazas en el rubro de redes sociales. El concepto de *fake news* fue asociado al de *Desinformación*, que no sólo se refiere a la información falsa distribuida intencionalmente para hacer creer a las personas supuestas verdades y la consecuente aparición de cámaras de eco sociales, sino también al efecto que se da por una sobresaturación de mensajes que dificulta distinguir lo importante de lo trivial.

En tercer lugar, se menciona el robo/suplantación de identidad, seguida del robo de información.

Resalta el hecho de que conceptos como *bullying* o acoso fueron mencionados por sólo 4 personas cada uno (2.8% de los entrevistados).

Amenazas en comercio electrónico

Nota: 2 entrevistados mencionaron no percibir amenaza alguna en este rubro

*Las **amenazas percibidas en el rubro "Otros"** son las siguientes: productos de mala calidad, predominancia de monopolios, banca móvil insegura, piratería.*
Ver las respuestas más relevantes enlistadas en el Anexo 4.

Como se ha podido observar, cada canal digital tiene aspectos particulares y vulnerabilidades vinculadas a su uso y propósito.

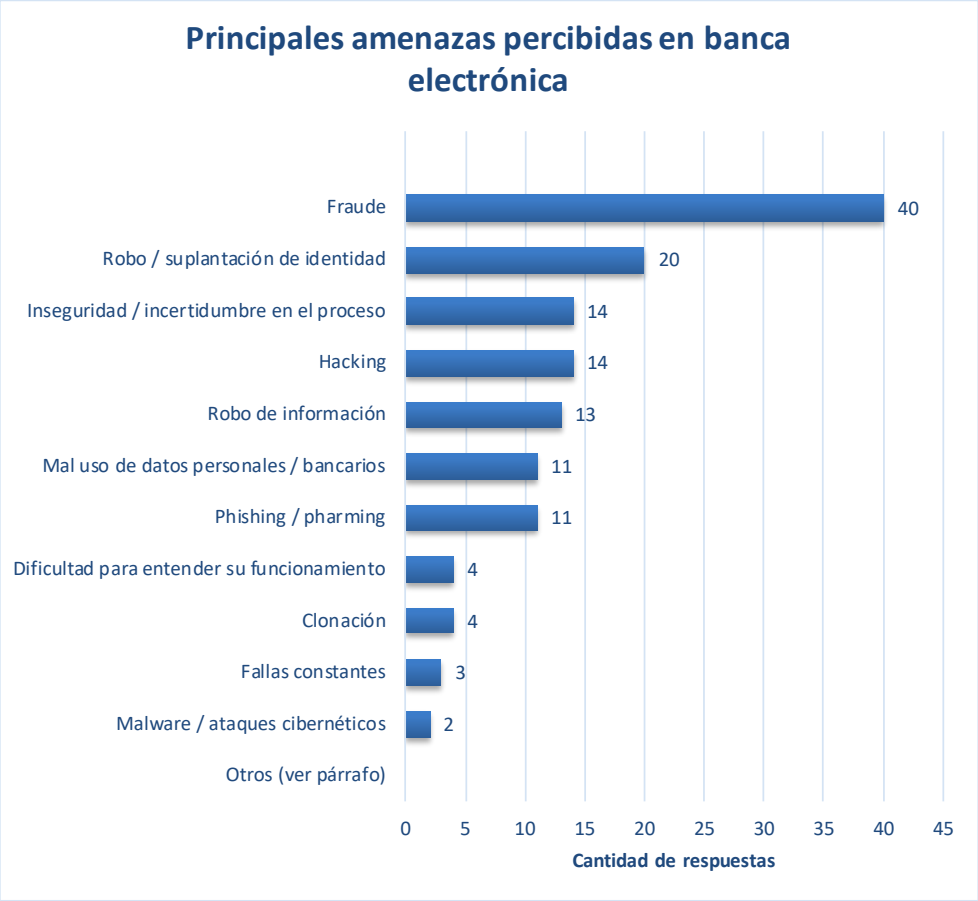
Fraude es la amenaza identificada por un mayor número de entrevistados (32.87%) con relación al comercio electrónico; de acuerdo con las respuestas proporcionadas, podría efectuarse al momento de hacer transacciones, principalmente en sitios de ventas *online* desconocidos. Hubo quien mencionó que las implementaciones actuales no son a prueba de los programadores internos y pueden guardar muchos elementos sensibles.

El robo de información abarca principalmente la posibilidad de que un tercero pueda tener acceso a información bancaria privada o a las credenciales y contraseñas del comprador.

La clonación de tarjetas de crédito o débito, si bien se trata también de una actividad fraudulenta (mencionada por el 15.38% de los entrevistados), se ha codificado separada del concepto fraude, porque así fue mencionada por los entrevistados y tiene un significado concreto.

Es notable que 7 de los entrevistados consideran (concretamente las empresas que hacen comercio electrónico) una amenaza el hecho de que los consumidores no confíen en este canal de venta y no se atrevan a usarlo.

Amenazas en banca electrónica



Nota: 9 entrevistados mencionaron no percibir amenaza alguna en este rubro
*Las **amenazas percibidas en el rubro "Otros"** son las siguientes:* ransomware*, desconfianza del usuario para usar estas plataformas, legislación deficiente, acceso no autorizado, invasión a la privacidad/espionaje. Ver las respuestas más relevantes enlistadas en el Anexo 5*.

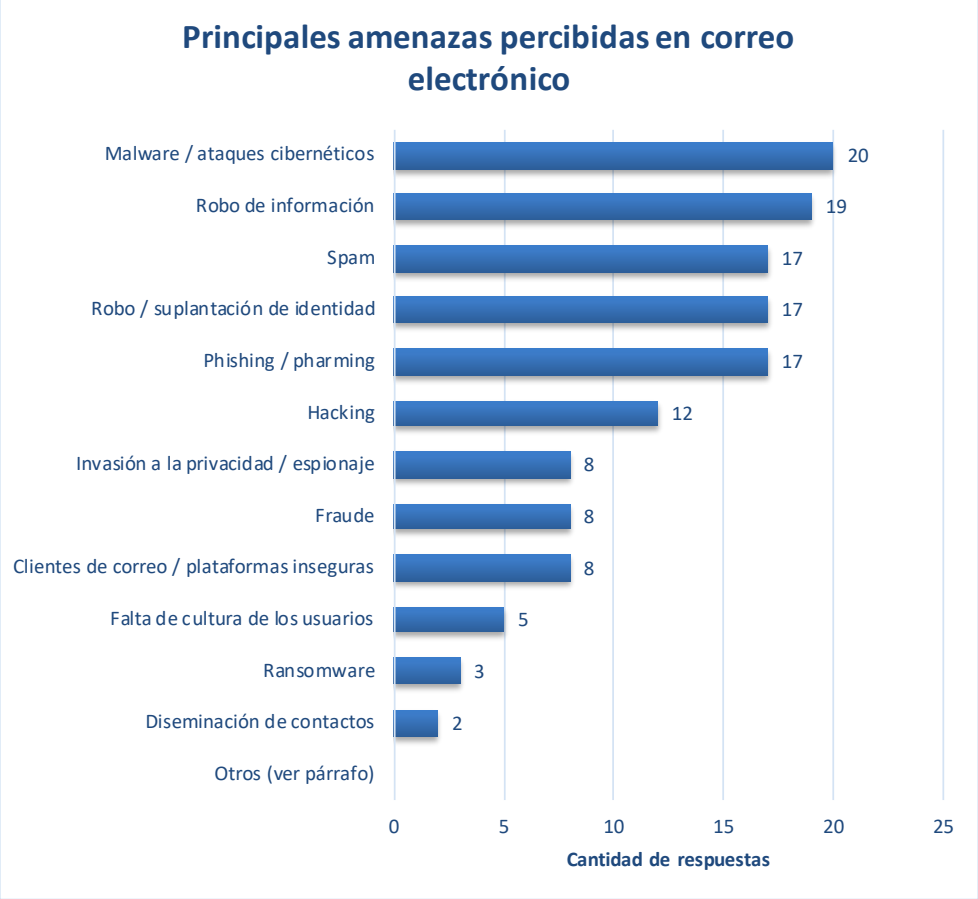
De manera similar a la percepción que se tiene en el rubro de comercio electrónico, la posibilidad de fraude por el uso de la banca electrónica es la amenaza mencionada con mayor frecuencia (27.97% de los entrevistados). Sin embargo, llama la atención que este es uno de los canales considerados más seguros como consecuencia de la gran inversión que realizan los bancos en infraestructura y medidas de seguridad. Las personas que efectúan transacciones por esta vía, en general, tienen confianza en el medio, según se aprecia en diversos comentarios a lo largo de este estudio. Se observa que 9 personas mencionaron que no perciben ninguna amenaza en el uso de las bancas digitales. En contraposición, hay quienes creen que la seguridad bancaria en medios digitales es vulnerable, desconfían de la efectividad de la tecnología y los procesos; además de los riesgos patrimoniales, opinan que aún hay

servicios deficientes, transacciones fallidas y un manejo dudoso de la información de los clientes.

La suplantación de identidad también es calificada como un riesgo por 20 personas. Aunque no necesariamente se lleve a cabo por la utilización de este medio, sino por otros mecanismos (*phishing*, *pharming* u otro tipo de técnicas y complicidades), se piensa que la banca electrónica podría ser "la puerta" para llegar al dinero de la gente y las empresas.

A pesar de que no hay una transmisión o intercambio de datos personales por medio de la banca en línea, el mal uso de esta información es percibido como una posible amenaza a través de estas plataformas.

Amenazas en correo electrónico



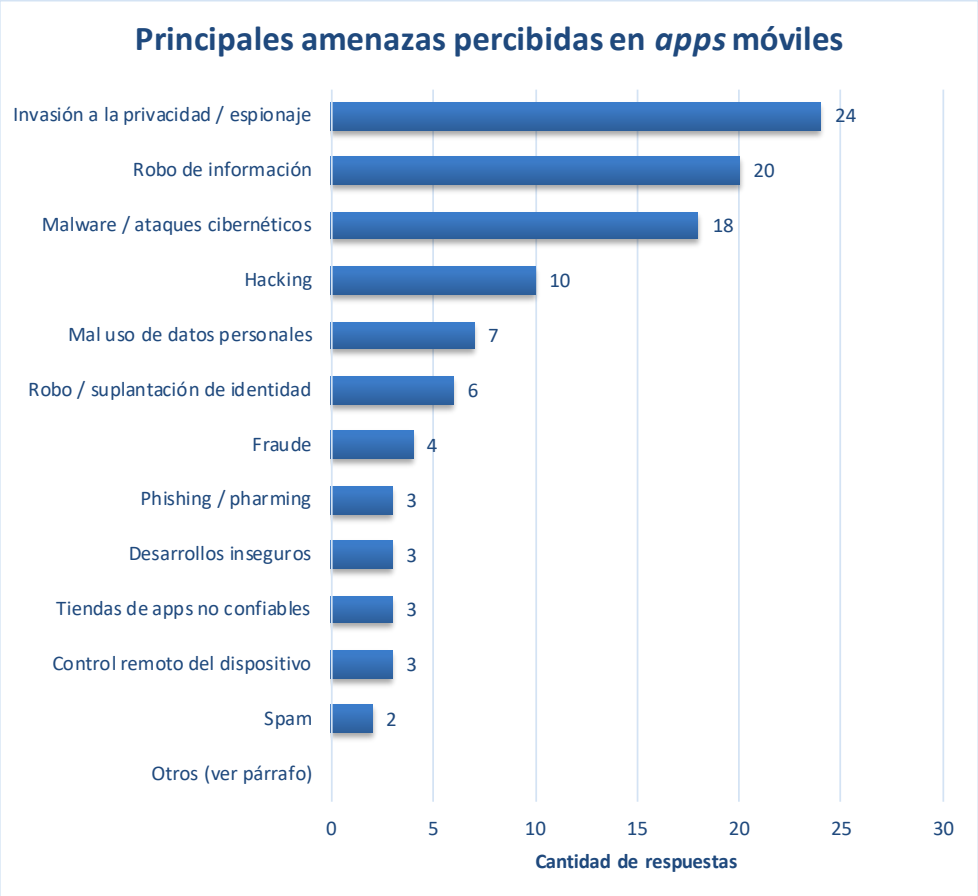
*Nota: 8 entrevistados mencionaron no percibir amenaza alguna en este rubro. Las **amenazas percibidas en el rubro "Otros"** son las siguientes: anonimato del remitente, fuga de información, información falsa, ingeniería social. Ver las respuestas más relevantes enlistadas en el Anexo 6.*

La distribución de *malware* o ataques cibernéticos, así como el robo de información, son las amenazas más mencionadas en relación al uso del correo electrónico. Se refiere principalmente a la diseminación de virus y *links* maliciosos, así como a los ataques a equipos informáticos. *Ransomware* bien podría estar incluido en esta categoría para algunos; sin embargo, se decidió incluirlo como un rubro aparte debido a las personas (3) que lo nombraron de manera específica.

En la tercera posición, y con la misma proporción de respuestas (11.9%), las amenazas percibidas por medio de correo electrónico son *spam*, suplantación de identidad y *phishing*.

Llama la atención que 8 personas señalan que no existe ningún riesgo en el uso del correo electrónico.

Amenazas en *apps* móviles



Nota: 6 entrevistados mencionaron no percibir amenaza alguna en este rubro
*Las **amenazas percibidas en el rubro "Otros"** son las siguientes:* clickbait*, clonación,* pharming*, desconfianza del usuario para usarlas, legislación deficiente. Ver las respuestas más relevantes enlistadas en el Anexo 7.*

La amenaza más citada en relación con el uso de *apps* móviles es la invasión a la privacidad/espionaje; contempla aspectos como el acceso a datos confidenciales, almacenamiento de información personal sin consentimiento, registro de hábitos y comportamientos, vigilancia cibernética, acceso a la geolocalización, cámara y micrófono del dispositivo, entre otros. Estas acciones inciden en otras amenazas percibidas: el mal uso de datos personales, hostigamiento comercial, venta de información, etcétera.

El uso de *apps* se asocia con la amenaza del robo de información. Por lo común, un gran número de entrevistados siente temor de que el proveedor de la *app* (en *apps* poco conocidas o de reputación dudosa) capte y utilice la información del usuario (a través de los datos que se capturan al abrir una cuenta, principalmente), o que el proveedor no tenga implementados mecanismos de seguridad adecuados y la información pueda ser captada por terceros.

También las *apps* para *smartphones* o tabletas son percibidas como posibles diseminadoras de código malicioso, según lo comentado por 12.6% de los entrevistados.

Sitios o *apps* de compras o servicios en línea consideradas confiables y seguras

Pregunta: Mencione hasta 5 sitios o *apps* de compras o servicios en línea que considera confiables y seguras.

Sitio/App	Menciones
Amazon	115
Mercado Libre	33
eBay	24
BBVA/BBVA móvil	23
Uber	20
App store	19
PayPal	18
American Express	13
Netflix	13
Liverpool	11
Bancanet/Citi Banamex	10
Bancas electrónicas en general	9

Sitio/App	Menciones
*Link*edIn	5
Uber Eats	4
AirBnB	4
Waze	4
Cornershop	4
WhatsApp	4
Líneas aéreas en general	3
Interjet	3
Domino's	3
Cinemex	3
Santander	3
Google	3

Apple	9	Starbucks	3
Expedia	9	Skype	2
Aeroméxico	7	Facebook	2
Costco	7	Sanborns	2
Spotify	7	Cabify	2
Best Buy	7	Segunda Mano	2
Walmart	6	Privalia	2
Palacio de Hierro	6	Tiendas departamentales en general	2
iTunes	6	Rappi	2
Linio	6	Open Table	2
Booking. com	6	Apple Music	2
Despegar.com	5	CFE Contigo	2
Banorte	5	Play Store	2
Cinépolis	5	Uniqlo	2

Se enlistan los sitios/apps que tuvieron sólo 1 mención en el Anexo 8.

Indudablemente, Amazon es la marca mejor percibida en cuestión de seguridad; fue mencionada por un 80.42% de los entrevistados y a una distancia de más de 3 veces respecto del sitio que ocupa la segunda posición en menciones que es Mercado Libre (23.08).

Las primeras 3 posiciones corresponden a tiendas virtuales, probablemente entre las más utilizadas en el país (Amazon, Mercado Libre y eBay). Entre las primeras 12, se observa la presencia de 4 instituciones financieras (PayPal, BBVA, American Express, Citi Banamex y 1 mención relacionada con los servicios de banca electrónica en general.

Los sitios y *apps* de las líneas aéreas tienen una buena percepción, en general, como plataformas seguras.

Destaca el hecho de que Apple, en diversas aplicaciones, es una marca bien percibida. Tal fue el caso de las menciones de App Store (ocupando la quinta posición), Apple, iTunes y Apple Music.

Sitios o *apps* de compras o servicios en línea consideradas No confiables o inseguras

Pregunta: Mencione hasta 5 sitios o *apps* de compras o servicios en línea que NO considera confiables y seguras.

Sitio/App	Menciones
Mercado Libre	31
Facebook	17
Instagram	10
Alibaba	7
eBay	6
Citi Banamex / Bancanet móvil	6
Uber	5
Liverpool	5
Snapchat	4
Palacio de Hierro	4
CFE	4
Rappi	4
Walmart	4
Tinder	4
Ticket Master	4
Sitios de juegos en general	3
Costco	3
Telmex	3
Cursos en Línea	3
Sitios de compras establecidos en China	3
Despegar.com	3

Sitio/App	Menciones
WhatsApp	3
Google	3
Privalia	3
Amazon	3
BBVA	3
Banorte	3
Muchos sitios gubernamentales	3
Redes sociales en general	2
Aeroméxico	2
Cinépolis	2
Target.com	2
IDMexico	2
Play Store	2
Sitios para adultos	2
Gobierno de la CDMX	2
Sitios que no tengan certificado o protocolo seguro	2
Aliexpress	2
Youporn	2
IZZI	2
Algunos de Hoteles	2

Se enlistan los sitios/apps que tuvieron sólo 1 mención en el Anexo 8.

Resulta notoria la referencia de diferentes redes, y del concepto redes sociales en general, entre los sitios o *apps* que se consideran inseguros o poco confiables.

El sitio con mayor número de menciones negativas resultó ser Mercado libre (31 entrevistados creen que es inseguro), mientras 33 personas lo catalogaron como un sitio seguro. A diferencia de otros sitios o aplicaciones, llama la atención que el número de opiniones en uno u otro sentido es casi la misma. Otras tiendas virtuales, como eBay y Amazon, también son percibidas como inseguras sólo por algunos entrevistados (6 y 3 respectivamente); una

proporción significativamente menor a las menciones que las califican como sitios seguros y confiables. Otras tiendas fueron percibidas como inseguras por una pequeña fracción de los encuestados; por ejemplo, Alibaba (7).

Algunas bancas mencionadas como seguras y confiables (BBVA, Citi Banamex y Banorte), también se calificaron en sentido contrario por otros entrevistados, aunque en menor proporción.

Las tiendas en línea de las dos principales tiendas departamentales en México (Liverpool y Palacio de Hierro) fueron citadas en ambas percepciones, si bien ambas tuvieron una mayor frecuencia de menciones como sitios seguros y confiables.

Principales razones y comentarios de por qué los sitios mencionados se consideran **no** confiables o inseguros

(Listado en orden alfabético)

1. Desconfianza en terceras partes, ya que en ocasiones las empresas pequeñas no tienen los procesos para asegurar la entrega de productos ni la protección de los datos.
2. Dudas sobre el adecuado almacenamiento de información personal y sobre las transacciones financieras.
3. El producto no es parecido al visto *online*.
4. En general, cualquier aplicación o sitio se vuelven no confiables o inseguros desde el momento en que registran la ubicación del usuario y generan registros que pueden ser utilizados para muchos fines, inclusive para delinquir.
5. En general, porque los envíos tardan demasiado en llegar y el servicio al cliente es en algunas bastante malo.
6. Errores básicos que me llevan a desconfiar de todo el sitio.
7. Es muy fácil ser engañado y comprar algo que no es lo que quieres, que viene defectuoso o que tiene un sobre precio importante. Intentan resolverlo, pero hay personas muy ingeniosas que siempre logran engañar a alguien. Participan tantos "vendedores" que es imposible asegurar que todos tienen buenas intenciones. Cabe mencionar que compro mucho en una de las principales plataformas multi vendedor, pero hay que saber hacerlo.

8. Fallas de seguridad en el manejo de sesión. Manejo de errores. Correos de seguimiento de terceros que nada tienen que ver con mi compra (pareciera robo o venta de datos personales).
9. Falta de confianza en el desarrollo de la marca y servicios.
10. Falta de control.
11. Han tenido problemas de seguridad o los métodos de autenticación no se perciben robustos.
12. He comprobado que no hacen un buen uso de la información personal.
13. He tenido experiencias negativas con anterioridad.
14. He tenido malas experiencias con ellos de fuga de información y cargos no existentes.
15. He tenido problemas con compras o inclusive con compras no hechas por mí.
16. Historial de ataques previos, *data breaches*.
17. Interfaz muy pobre, poco responsiva, falla. No usa buena tecnología de encriptación.
18. La navegación no es amigable y la información es confusa.
19. La página de Internet de la tienda no carga bien... si eso hace en la página, no quiero saber en temas de seguridad. Y las páginas patito, no, o sea, no puedo.
20. La tienda me ha hecho cargos a tarjetas sin tener la mercancía que compré en inventario y al final no la he recibido. Los reclamos son muy complicados. En general, con los otros sitios que menciono, el excesivo uso de *cookies* me genera desconfianza.
21. Las compras van a análisis de fraude del banco, eso complica todo.
22. Los sitios de pornografía y las aplicaciones de citas tienen muy mala fama y hay mayor riesgo de ser hackeado o de que le roben a uno información.
23. Mala reputación o bajas calificaciones de clientes anteriores
24. Me clonaron mi tarjeta después de una compra *online*. Me llegan muchos correos fraudulentos de ese banco y no soy cliente.
25. Me da la impresión de que el manejo de información no es el apropiado. Además de que he recibido cargos de ese sitio de manera incorrecta.
26. Me han metido cargos que no son, en esa *app* hay problemas de seguridad personal serios.
27. Mi única experiencia negativa es que se bloqueen mucho y cueste trabajo desbloquearlas.

28. No conozco sus métodos de procesamiento de pago o no sé qué información puedan estar tomando de mi celular.
29. No considero que muchas empresas tengan sistemas de seguridad efectivos para cuidar la información.
30. No cuentan con suficiente verificación
31. No es consistente ni confiable su funcionamiento.
32. No están bien desarrolladas y no proporcionan información de cómo navegar dentro de las mismas.
33. No están reguladas, no existe seguridad en el manejo de datos, no son empresas (marcas) reconocidas.
34. No garantizan la confidencialidad en el manejo de la información, riesgo de robo de identidad.
35. No son claras las garantías que ofrece la marca, la cual depende de vendedores y compradores con distintos grados de compromiso y ética.
36. No tienen una infraestructura de seguridad robusta.
37. Pocas medidas de seguridad y validación; otras han sido víctimas de hackeo y brechas de seguridad.
38. Por experiencias negativas en lo que respecta a mecanismos de seguridad que han derivado en robo de información, clonación de cuentas, fraude.
39. Por fallas que se han venido experimentando en ellas, lo que demuestra que no cuentan con la suficiente seguridad en su desarrollo.
40. Por falta de elementos de seguridad.
41. Porque sin tener certeza al 100%, he recibido cargos no reconocidos a mi tarjeta después de realizar compras en este tipo de establecimientos.
42. Porque yo, o alguien conocido, he experimentado problemas con ellas con los medios de pago.
43. Por su funcionamiento en general, performance, no dan confianza en que no roben información, o bien, que no cumplan con lo contratado.
44. Porque anexan mucha publicidad no deseada y exploran datos de los usuarios, además de que tienen historial negativo de clonación de tarjetas.
45. Porque no te llega lo que compras, pero sí te lo cargan a la TDC . Porque al visitarlas te llueven correos *spam*.

46. Porque no tienen certificados de seguridad o piden información que no deseo compartir.
47. Porque siento que hay pocos filtros de seguridad.
48. Porque suelen enviar información no encriptada.
49. Se ha probado que hacen un mal uso de datos personales y metadatos
50. Se han documentado casos de vulnerabilidades de seguridad en ellas.
51. Solicitan demasiada información, que podría ser usada por terceros.
52. Solicitud de información en exceso y posterior acoso electrónico con publicidad y promociones.
53. Solicitan, generalmente, datos personales de registro, incluyendo datos bancarios.
54. Son fáciles de hackear.
55. Su construcción no aparenta ser robusta.
56. Su enfoque no proporciona alguna garantía para el comprador.
57. Temor/sospecha de clonación.
58. Tengo indicios de que el *password* de mi cuenta fue hackeado.
59. Tienen muchos errores, desde el acceso, hasta la calidad de la conexión.
60. Toman datos y los asocian para después usarlos para *spam* y fraudes.
61. Venden datos de usuarios; no hay control.

Recursos de apoyo identificados que ayudan a incrementar la seguridad en la comunicación o transacciones en línea

Pregunta: ¿Cuál *software* o recursos de apoyo conoce para incrementar la seguridad en la comunicación o transacciones en línea? Mencione hasta 5

Sitio/App	Menciones
PayPal	18
Protocolos seguros SSL / https	15
Symantec/Norton	15
Conexiones VPN	15
Cifrado / Encriptación	13
Firewall	13

Sitio/App	Menciones
Avast	2
Verified by Visa	2
Cisco	2
Sophos	2
Aplicaciones bancarias	2
Antispyware	2

Autenticación de dos vías / múltiple	9
Token	9
Biometría	8
Antivirus	8
McAfee	7
Verisign	6
Certificados de seguridad	6
Kaspersky	6
American Express	4
Contraseñas seguras	4
Filtrado de contenidos	3
BitDefender	3
Checkpoint	2

Gmail	2
Google Safe Search	2
Mercado Pago	2
Block chain	2
Nessus	2
Nikto	2
Cultura del usuario	2
Sistema Operativo iOS	2
Cybersource	2
Tarjeta digital	2
Detección de Intrusos	2
Trustee	2

Se enlistan las aplicaciones o recursos de apoyo que tuvieron sólo 1 mención en el Anexo 9.

La encuesta muestra dos grupos de respuestas: se habla de conceptos genéricos y se mencionan marcas o empresas que apoyan la seguridad en la comunicación digital. Las menciones mayoritarias en el primer grupo se refieren a conceptos como el uso de protocolos seguros, conexiones VPN, cifrado y encriptación de datos, *firewalls*, sistemas de autenticación en capas, token, tecnología biométrica, antivirus y certificados de seguridad, entre otros. En el segundo grupo, se citan nombres y marcas (en orden de cantidad de menciones) como PayPal, Symantec/Norton, McAfee, Verisign y Kaspersky, entre otros.

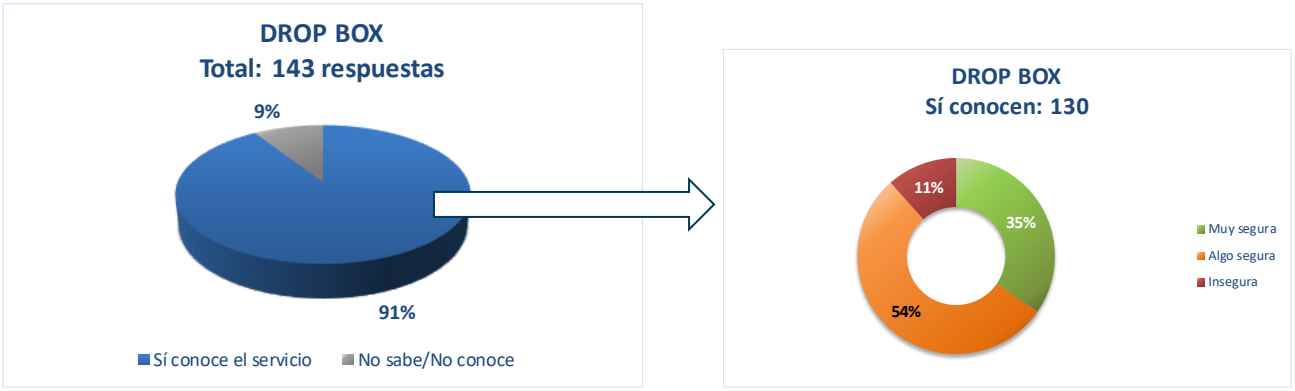
Si bien la mayoría de las opciones mencionadas efectivamente son herramientas o recursos que ayudan a incrementar la seguridad (como aditamentos que se agregan a la infraestructura de telecomunicaciones o a los equipos locales), algunos entrevistados mencionan otras que son propiamente plataformas o aplicaciones transaccionales o de servicios. Esto podría deberse a que dichas plataformas son percibidas como seguras en sí mismas, teniendo PayPal, como se observa en la gráfica, una posición relevante en este sentido.

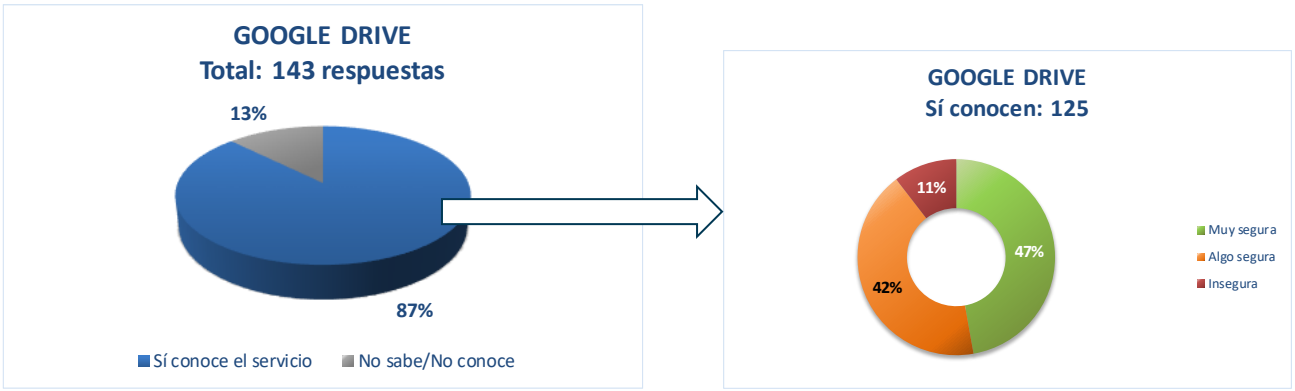
Ocho personas mencionaron no encontrar ningún recurso que apoye el incremento de la seguridad en este sentido.

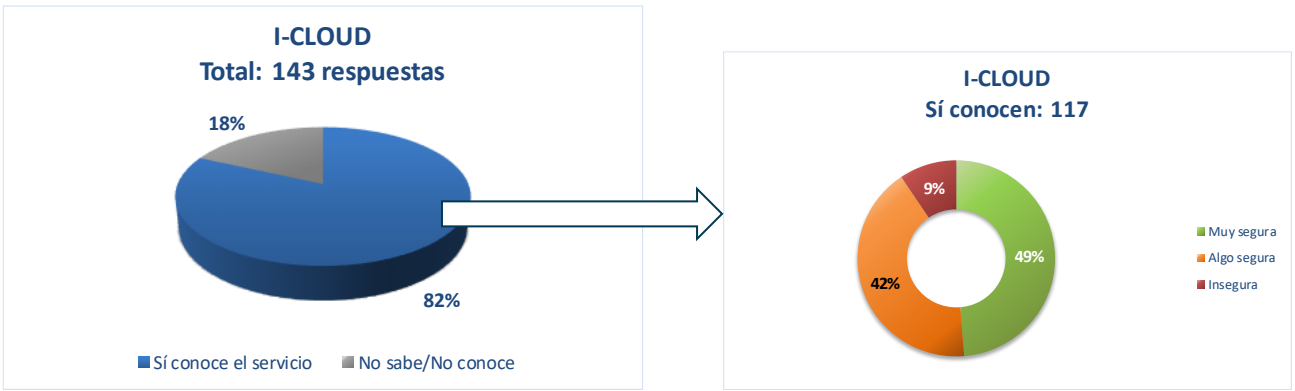
Seguridad en los servicios de almacenamiento en la nube

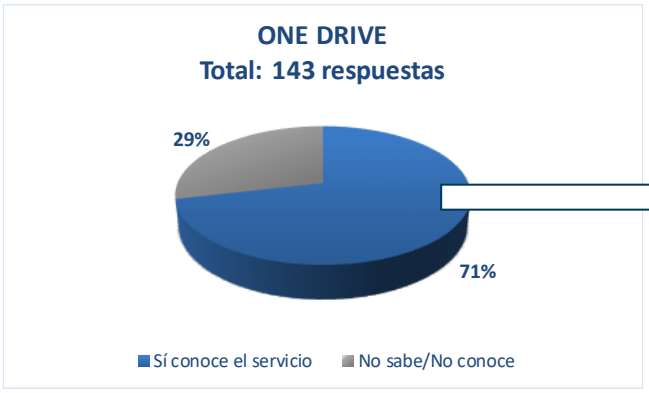
Pregunta: ¿Considera que la información de su empresa u organización está (o estaría) segura en servicios de almacenamiento en nube? Por favor, indique cuáles y qué tanto.

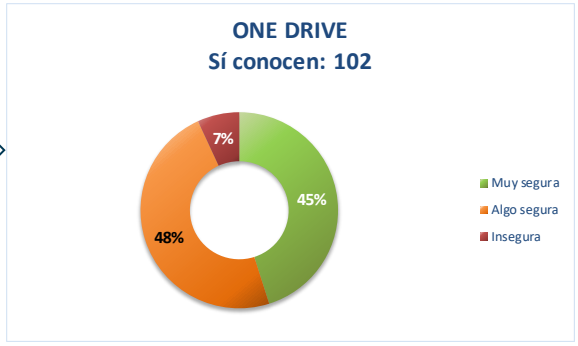
Se presentan a continuación las gráficas de las respuestas:



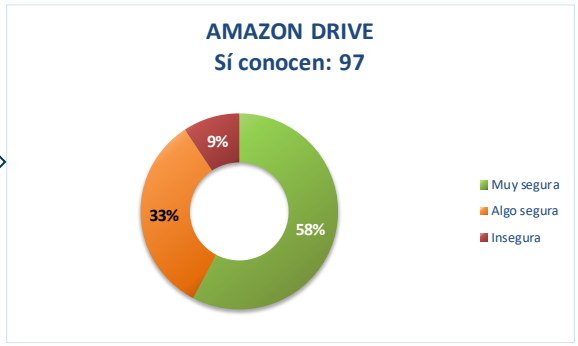


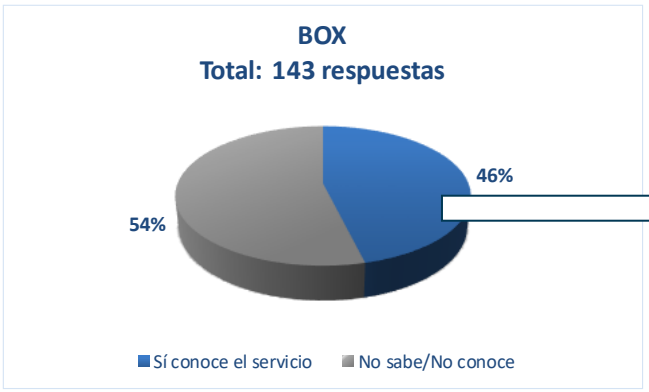


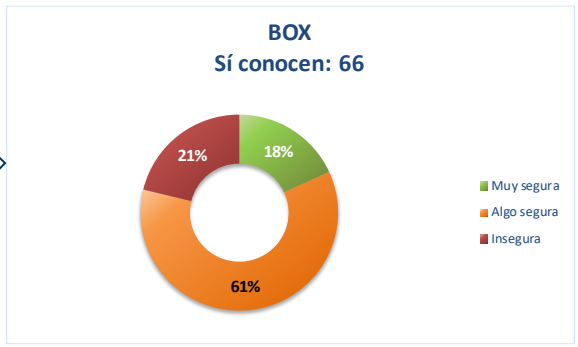

ONE DRIVE
Total: 143 respuestas
29%
71%
Sí conoce el servicio
No sabe/No conoce

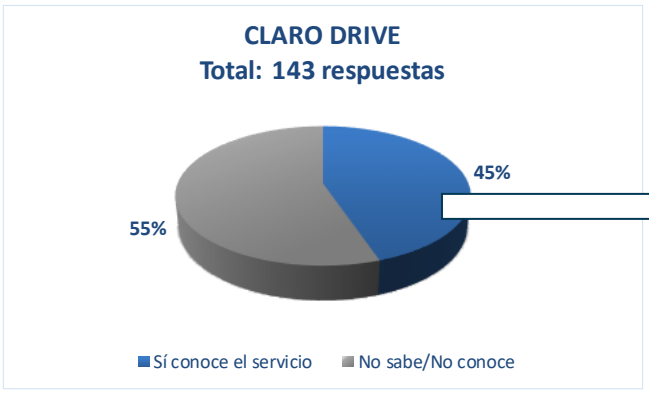

ONE DRIVE
Sí conocen: 102
7%
45%
48%
Muy segura
Algo segura
Insegura

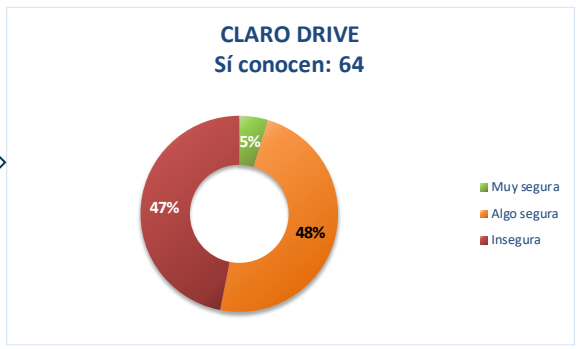

AMAZON DRIVE
Total: 143 respuestas
32%
68%
Sí conoce el servicio
No sabe/No conoce


AMAZON DRIVE
Sí conocen: 97
9%
33%
58%
Muy segura
Algo segura
Insegura


BOX
Total: 143 respuestas
46%
54%
Sí conoce el servicio
No sabe/No conoce


BOX
Sí conocen: 66
21%
18%
61%
Muy segura
Algo segura
Insegura


CLARO DRIVE
Total: 143 respuestas
45%
55%
Sí conoce el servicio
No sabe/No conoce


CLARO DRIVE
Sí conocen: 64
5%
47%
48%
Muy segura
Algo segura
Insegura

En las respuestas se advierte que Drop Box es la plataforma de almacenamiento en la nube más conocida (91% de los entrevistados). Claro Drive y Box son las menos conocidas (45% y 46% de los entrevistados, respectivamente).

La mayoría de las personas que opinaron y conocen las plataformas coinciden en que OneDrive tiene un sistema de almacenamiento seguro en la nube (93% de las 102 menciones), mientras que Claro Drive es percibido como el sistema más inseguro por el 47% de las 64 menciones correspondientes.

La plataforma considerada como MUY SEGURA por la mayor proporción de respondentes es Amazon Drive, con un 58% de las 97 menciones.

Otros servicios de almacenamiento en nube mencionados

Otros medios mencionados como MUY SEGUROS

Servicio	Menciones
Azure	2
pCloud	2
Amazon Web Services	1
Carbonite	1
Gator	1
Godaddy	1
Huawei Drive	1
KIO Networks	1
Livedrive	1
Mantenerse desconectado de cualquier red	1
ownCloud	1
Zoho	1

Otros medios mencionados como ALGO SEGUROS

Servicio	Menciones
Mega	2
Adrive	1
Disco externo	1
Exchange	1

Host Gator	1
Hubic	1
IBM	1
mega.nz	1
pCloud	1
Servicios administrados en nubes privadas	1
SpiderOak	1
Stratosphere	1
Tresorit	1
Via Networks	1

Otros medios mencionados como INSEGUROS

Servicio	Menciones
MediaFire	1
Rackspace	1
Slack	1
Tresorit	1
Yo no pondría información de mi empresa en la nube	1
Zoho	1

Razones por las cuales los servicios de almacenamiento en la nube son percibidos como seguros o inseguros

Opiniones que apoyan la percepción de seguridad de los sitios mencionados
(Listado en orden alfabético)

1. A nuestro parecer, cuentan con el API y con los sistemas de seguridad adecuados para el nivel de información que manejamos.
2. Almacenamiento en la nube es una realidad que ha ido acabando con los servidores en sitio.
3. Apple es la única empresa que me da confianza en cuanto a la privacidad.
4. Con las demás plataformas no ha sucedido nada, pero en las conversaciones con amigos "expertos" suelen recomendar los servidores de Amazon.
5. Con las que conozco y he usado nunca he tenido problemas.

6. Considero más confiables los servicios de organizaciones como Microsoft y Google, sobre todo cuando se tiene contratado directamente por la empresa, que permiten configurar controles adicionales como el doble factor de autenticación, y no tanto las gratuitas.
7. Considero que estas empresas deben tener lo último en seguridad, ya que es su *core business*. Es más difícil mantenerse al día "en casa".
8. Contamos con servicios en la nube con IBM. Por el momento no hemos tenido problemas.
9. Creo que el almacenamiento en la nube es una gran herramienta hoy en día.
10. Creo que los protocolos de seguridad de estas grandes empresas son más efectivos/ completos que las soluciones locales.
11. Drop Box, Google Drive, I-Cloud son servicios que conozco y he utilizado por años sin ningún problema. Entiendo que Amazon Drive es un servicio muy sólido y con excelente prestigio. Utilizo Box para algunas cosas pero no me gusta cómo funciona cuando he cambiado de equipo, genera archivos duplicados que provocan confusiones.
12. Dropbox y Box están protegidos por varios elementos, como doble autenticación, además de que existe un área de seguridad que se encarga de vigilar que no haya accesos malignos.
13. El que el servicio sea proporcionado por una empresa de gran tamaño da mayor confianza en la seguridad.
14. En general, se me hacen seguros
15. En general, estos sitios cuentan con una mayor eficiencia en recursos tecnológicos.
16. En la empresa utilizamos servidores de Google para nuestros servicios, yo en lo personal uso One Drive, y sabemos que Amazon es muy seguro.
17. Entiendo que Dropbox tiene un costo y garantiza el respaldo de nuestra información.
18. Entiendo que son muy seguros y no conozco casos de hackeo o que se haya caído la red/nube.
19. Es una solución bastante atractiva a nivel financiero, ya que no se tienen que hacer grandes desembolsos. Se puede crecer conforme se necesite, no se requiere gran conocimiento técnico, ahorro en espacio y energía. Acceso a la información desde cualquier parte; siempre y cuando se tenga acceso a Internet.
20. Estamos migrando a nivel mundial todo a Azure, así que definitivamente es una garantía ya muy evaluada en el grupo; aquí el tema de seguridad se toma muy en serio.
21. Existe confianza en los servicios de pago.
22. Existen formas de administrar la información para tener respaldos, conocer quién entró a la herramienta, qué vieron, modificaron o borraron.
23. He usado esas tecnologías que califiqué como seguras por muchos años y nunca he tenido problemas, confío en ellas.

24. Incluye el sistema pCloud Crypto que encripta los datos en la terminal de acceso del usuario, por lo que cualquier cosa que viaja por Internet y es almacenada en los servidores va encriptada de origen.
25. La información está encriptada por lo que la consideramos segura.
26. La mejor alternativa de seguridad es contratar un servicio de servidor dedicado al almacenaje en la nube.
27. Las grandes empresas enfocadas en prestar ese servicio cuentan con los recursos especializados para garantizar la seguridad.
28. Las nubes son seguras, los esquemas de acceso fijados por los usuarios pueden ser inseguros.
29. Los GAFAS tienen mejor infraestructura y seguridad de información que cualquier empresa. El día de hoy está más segura la información en la nube que en su propio *data center*.
30. Los principales proveedores de servicio en la nube, como Amazon y Microsoft, tienen múltiples herramientas de seguridad, la responsabilidad recae en la administración y manejo que les da el usuario final.
31. Los proveedores de servicios en la nube han ido mejorando sus plataformas e incrementando la seguridad en las mismas. Esto se debe sumar a procesos personales de uso de contraseñas, cambios y herramientas adicionales, para garantizar verdadera seguridad.
32. Los usamos todos y no hemos tenido ninguna amenaza o pérdida de información.
33. Mejores opciones son servicios de AWS/GCP, aunque no son infalibles. Es un tema de lo crítico que es la información vs. el costo de la seguridad. Por ahora, OK con Google Drive y G-Suite para mi empresa.
34. Mientras se mantengan con 2FA, no es tan factible robar la información por la forma en que se almacena el contenido.
35. Muy a favor, es el futuro.
36. No he tenido problemas.
37. Optimización de espacios en memoria en los dispositivos, servidores, fácil uso de recuperación de archivos.
38. Sé que Google maneja mucha información y por lo tanto sus parámetros y medidas de seguridad son confiables.
39. Seguros y profesionales los que conozco.
40. Sí considero que son servicios seguros por estar respaldados por empresas muy importantes en el mundo de la tecnología.
41. Son empresas que tienen años mejorando la calidad y seguridad de esta clase de servicios.
42. Son más seguros.

43. Son muy prácticos, seguros y económicos.
44. Son muy seguras en la medida que uno como usuario resguarde las claves y las sesiones no permanezcan abiertas en equipos públicos.
45. Son necesarios por la inseguridad que vivimos actualmente, pues en cualquier momento podemos ser víctimas de la delincuencia y nos roban nuestra herramienta de trabajo con toda nuestra información.
46. Soy usuario de todas las que marqué y no hemos tenido problemas. Tampoco he sabido de terceros que los hayan tenido.
47. Soy usuario de todos los servicios que indiqué y los considero seguros porque invierten mucho dinero y recursos. Por supuesto, siempre hay un riesgo de que sean vulnerados y estoy consciente de ello.
48. Todas esas cuentan con estándares de seguridad adecuados.
49. Todos esos servicios de almacenamientos están respaldados por empresas globales que en principio hacen inversiones importantes en tecnología y en seguridad de la misma.
50. Todos los productos mencionados pertenecen a compañías que gozan de buena reputación y capital suficiente para garantizar seguridad a sus usuarios.
51. Usamos OneDrive y funciona muy bien.

Opiniones que apoyan la percepción de inseguridad de los sitios mencionados
(Listado en orden alfabético)

1. A pesar de invertir grandes cantidades de dinero en seguridad, dichas empresas son objeto de constantes ataques, ya que representan un “premio” importante.
2. A pesar de que los principales sitios son relativamente seguros, existe el riesgo de que pudieran ser hackeados o infectados.
3. Algunos de los servicios de almacenamiento en la nube tienen poca seguridad y políticas de uso que ceden privacidad. Otros han sido hackeados y datos personales han sido robados y utilizados para fraudes o bien vendidos en línea. Otros han entregado datos a gobiernos para espiar a sus ciudadanos. Las compañías generalmente ocultan a sus clientes que han sido atacadas y no son castigadas por hacerlo. Sólo Europa está penalizando estos comportamientos.
4. Considero que no hay nada 100% seguro. Siempre hay riesgos de que se pueda filtrar información.
5. Creo que cualquiera es susceptible de pérdida de información.
6. Creo que en la nube nada es 100% seguro.

7. Cuentan con elementos de seguridad pero no hay garantía de que tu información no sea vulnerada.
8. El hecho de que la información esté en manos de alguna empresa que ofrece el servicio, da la impresión de que siempre existe el riesgo de que puedan tener acceso a ella, en algún momento, sin el consentimiento y conocimiento del dueño de la información.
9. En el caso One Drive no me gusta Microsoft.
10. Es tendencia, pero no se sabe qué tan segura será el día que se necesite.
11. Google Drive está ligado a una cuenta de Gmail, y si el acceso a esa cuenta es hackeado (sucede con regularidad), también tienen acceso al Drive. En mi experiencia, en Dropbox la descarga de respaldos grandes es poco eficiente.
12. Google es menos seguro al igual que las otras. De hecho, me parece que es muy probable que analicen mi información y la usen para fines comerciales, aunque tal vez de manera anónima.
13. Google/Facebook usan la información de los clientes para monetizar los servicios.
14. He tenido malas experiencias con Dropbox.
15. Las tecnologías que no he utilizado me parece que invierten menos en seguridad y que no guardan la información de manera leal y confiable.
16. Los proveedores del servicio no se responsabilizan finalmente por la seguridad de la información.
17. Los que son muy públicos no tienen buenas medidas de seguridad.
18. Los servicios de almacenamiento previamente mencionados son de los más populares y se han convertido en el blanco ideal de organizaciones criminales.
19. Los servicios públicos aún no se perciben como altamente confiables.
20. Me hace dudar la mala reputación de ciertas empresas y ver cómo se doblegan ante el gobierno.
21. Me parece que aún existe escepticismo en el almacenamiento de datos sensibles en la nube por tratarse de un recurso con acceso generalizado. Las empresas que lo hacen deberían promocionar sus garantías de seguridad.
22. Ningún servicio de nube es seguro
23. No almaceno nada en la nube, que yo sepa.
24. No confío ciegamente en ninguno. Y no confío nada en Claro.
25. No considero que algún servicio en la nube tenga garantía de estar segura frente a los hackers.
26. No creo que exista algo completamente seguro.
27. No creo que existan los controles ni los contratos necesarios para que me sintiera cómodo poniendo información de mi empresa en ninguna nube.
28. No en todos los servicios está claro o definido que la información quede encriptada una vez que está almacenada en ellos.

29. No importa que tan segura sea la nube si las redes para alimentarla o para recibir información no lo son.
30. No se explica cuáles son los mecanismos que se usan para resguardar la información y no incluye el factor humano como una debilidad y cómo se ataca.
31. Poca confianza en los servidores, derivado de malas notas políticas.
32. Pocas firmas de almacenamiento en la nube considero que proporcionan una garantía de seguridad real.
33. Se utiliza para almacenamiento de información NO sensible
34. Si los hackers pueden tumbar a organismos bancarios y/o gobiernos, para empresas pequeñas el riesgo es mayor.
35. Son servicios con un buen grado de seguridad, pero no infalibles y pueden ser hackeados.
36. Todos los servicios en la nube mencionados residen o son parte de la red USA, por lo que tienen la posibilidad del acceso de la inteligencia de USA si lo requieren.

Opiniones generales o mixtas acerca de los sitios mencionados
(Listado en orden alfabético)

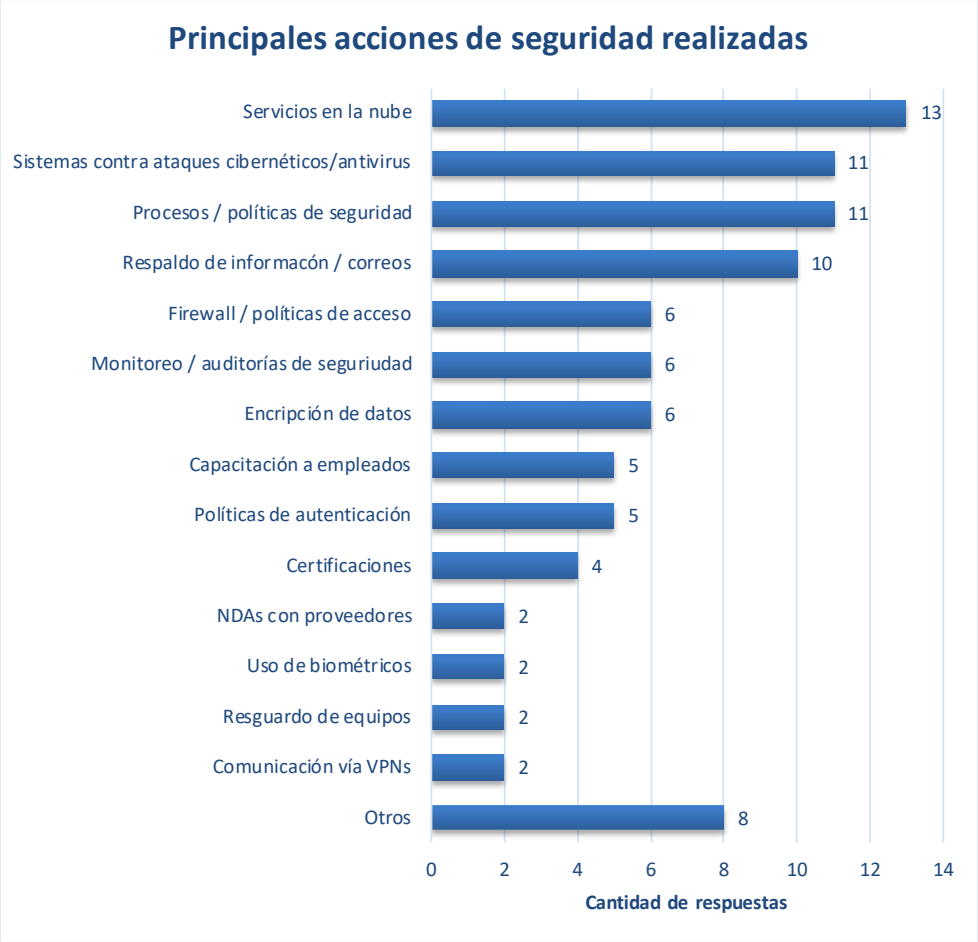
1. Creo que son el futuro, pero algunos han tenido fallas y sí influye el nivel de infraestructura con los que han sido construidos.
2. Dropbox es el que más uso y en realidad desconozco que tan seguro sea. Quiero pensar que lo es. Aunque no envío nunca enlaces invitando a alguien para que tenga acceso a un documento en mi Dropbox. Me genera desconfianza hacerlo.
3. En general, los que marqué algo seguros son *online; cloud storage services* de empresas que le ponen mucho dinero y esfuerzo para que sean seguros. Pero son tan conocidos, que pueden ser blancos para hackers, por eso los considero apenas algo seguros.
4. En nuestra empresa usamos Google Drive, iCloud y Dropbox con buenos resultados. Si no pongo "muy seguro" es porque sabemos que todos los servicios han tenido hackeos y pérdidas de información. Por eso, además de la nube, hacemos respaldos periódicos en discos físicos.
5. La nube es importante pero no esencial
6. La seguridad depende de lo robusto de las redes y centros de datos del proveedor a nivel global.
7. Los servicios grandes y conocidos son blancos de ataques permanentes. Si bien son seguros, lo son porque están en constante defensa de ataques reales. En cuanto sus vulnerabilidades estén expuestas, dejan de ser seguros. Hay servidores en renta,

administrados por expertos y vigilados, pero que no están en el circuito de los que parecen botines para hackers.

8. Los servicios de almacenamiento en la nube seleccionados cuentan con altos estándares de seguridad que, aunque no son impenetrables, normalmente son superiores a los que tradicionalmente implementan las empresas dentro de sus *data centers*; sin embargo, el mal uso por parte de los usuarios finales, al conceder accesos públicos o no protegidos a estos medios de almacenamiento, hace inútiles los mecanismos de seguridad propios del sitio.
9. Ninguno me parece totalmente seguro, pero en general considero difícil el acceso por terceros no autorizados.
10. No depende totalmente del servicio. El servicio debe tener políticas de seguridad disponibles para autenticación, cifrado, etc. Pero depende de que el usuario, o de quien gestiona las políticas de uso en la organización, aplique aquellas que sean adecuadas para el negocio, según su apetito de riesgo.
11. No sólo considerar la tecnología, sino el manejo adecuado de la información por parte de los usuarios y los procesos y controles correspondientes.
12. Para considerar segura la información resguardada, creo que deben manejarse certificados con estándares muy altos y avalados por instituciones confiables.
13. Por el volumen de información que manejan, me parece que algunas empresas proyectan más seguridad que otras.
14. Si no se maneja una política que asegure el buen manejo de los datos, se corren riesgos.
15. Siempre hay riesgos de fuga por parte de los empleados.
16. Siempre será necesario concientizar a los colaboradores del poder de la información, tanto de su buen como de su mal uso. Hoy en día es imposible el no estar conectado en mayor o menor medida, ya queda en manos de los líderes de la organización definir claramente qué información puede estar conectada a la red permanentemente y protegerse legalmente respecto a la aprobación del uso de información y datos personales de parte de clientes y prospectos.

Acciones concretas compartidas por los entrevistados

Pregunta: Sin comprometer ningún secreto estratégico o información confidencial, ¿podría compartir algo que esté haciendo su empresa u organización respecto a seguridad en medios digitales que le parezca relevante? Por favor, intente incluir la mayor cantidad, con una descripción breve.



Ver las respuestas más relevantes enlistadas en el Anexo 10.

Las acciones implementadas que aparecen en el rubro "**Otros**" son las siguientes: *coding* de conducta de empleados, centro de datos seguro, comité de seguridad, soporte de empresas consultoras, DRP/BCP, no utilizar servicios en la nube, BYOD, inteligencia artificial/*machine learning*.

Según los entrevistados en este estudio, la mayoría de las acciones instrumentadas para fortalecer la seguridad en medios digitales son: **servicios** (consultoría de expertos, almacenamiento en la nube o en centros de datos confiables, SOC as a service), **sistemas** (para identificación y prevención de riesgos, monitoreo y auditorías de seguridad constantes), **infraestructura** (robustecimiento de las redes, *firewalls*, redundancia, respaldos en sitio, biométricos) y ***software*** (antivirus, aplicaciones para *coding* de conducta de empleados, VPNs).

Es claro que los servicios proporcionados en la nube, además de su función práctica como proveedores de información centralizada y de aplicaciones, son considerados por diversas

empresas como un medio que añade seguridad a su información, con una infraestructura robusta que, por sus propios mecanismos seguros, garantiza altos niveles de disponibilidad.

Aunque hubo menos menciones de la implementación de herramientas tecnológicas, se compartieron buenas ideas que merecen atención: contar con políticas de seguridad bien establecidas en los niveles organizacional, técnico y de procesos, promover la capacitación periódica de los empleados, tanto de TI como de todas las áreas, promover la certificación en estándares de seguridad nacionales e internacionales (de las empresas y del personal especializado), así como la elaboración y uso metódico de NDAs con los proveedores de la organización.

Principales retos para las empresas y organizaciones

A continuación se presentan los principales retos mencionados. En algunos casos, se han englobado conceptos similares en uno solo.
(Listado en orden alfabético)

Actualización constante y mejoras, dependiendo del costo.
Al transitar a un sistema de gestión propio, será indispensable contar con la seguridad necesaria para evitar intromisiones. Por otro, el acceso seguro y confiable siempre en dispositivos móviles es importante para nosotros.
Alineación a normas internacionales como PCI o ISO, presupuesto para cubrir las funciones y para invertir en herramientas.
Asegurar que toda la información esté segura y se respalde.
Concientizar a todos los colaboradores en materia de seguridad.
Contrarrestar posibles fugas de información y vulnerabilidad de los equipos. Otro gran reto es hacer un estudio constante del recurso humano, ya que la mayoría de las veces por eso se dan las fugas de información.
Cubrir los accesos a portales de bancos y la información financiera.
Cumplir con los requerimientos de seguridad de información que nos exigen clientes del sector financiero.
Dado que se trata de una institución educativa que va desde kinder hasta bachillerato, hay dos grandes temas que nos ocupan además de los tradicionales de cualquier empresa: 1) El no acceso ni distribución a la información personal de estudiantes y sus familias, 2) El no acceso ni distribución de material inapropiado para su edad.
Defensa de ciberataques cada vez mejor realizados. Ingeniería Social. Vulnerabilidad de productos. Concienciación de los usuarios.

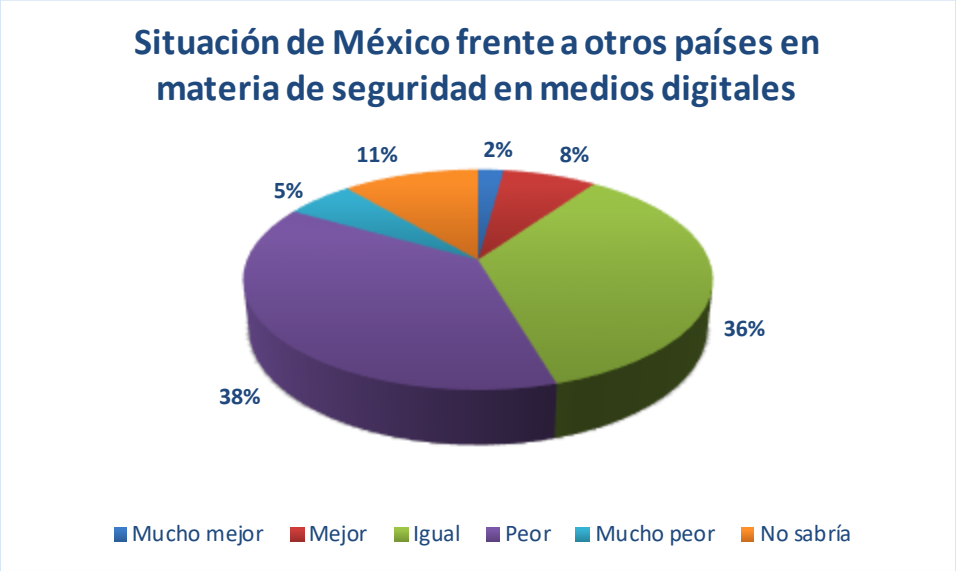
El mayor reto es comprender bien a qué se refiere "seguridad" y cuál debe ser el alcance. Sin ser laxos en temas de importancia, pero tampoco exagerando en otros, cosa que sucede muy a menudo.
En el ramo de la comunicación, el uso de contenido en materia de derechos de autor, ataques a las páginas de medios para hackearlas.
Encontrar un mecanismo para que todo nuestro equipo (12 personas) tengan acceso irrestricto a todos los archivos compartidos en la nube, sin tener el riesgo de borrar información accidentalmente.
Escalar procesos a la nube, seguimos siendo muy *email driven*.
Estar actualizados contra nuevos virus, ataques y amenazas.
Estar en posibilidades de cubrir el costo de todas las variables existentes en cuanto a la detección de vulnerabilidades; las herramientas operan de manera paralela y no integral.
Estar protegidos contra la extorsión, uso no autorizado de cuentas y *apps* bancarias.
Estar siempre al tanto de los riesgos a los cuales podemos enfrentarnos e implementar nuevas formas para proteger nuestra información.
Hacer consciente a la Alta Dirección sobre la necesidad de evitar riesgos.
Implementar *firewalls* suficientemente seguros y eficientes que eviten hackeo. No sufrir lo que le pasó a Mossack Fonseca (empresa panameña que sufrió un robo muy importante de información y desapareció). Continuar con pruebas y escenarios que prueben la seguridad de nuestros datos en la nube.
Inversión en digital.
JAMÁS estar en una noticia de que estaban los datos de nuestros clientes en la nube abierta.
Jurídicamente hablando, el manejo de mucha información confidencial.
La capacitación y concienciación en el uso de nuevas tecnologías.
La percepción del mercado de que la información en la nube no es muy segura, ya que afecta nuestras ventas.
La pérdida de información y la vulnerabilidad de datos personales de los clientes.
Los mayores retos son las leyes gubernamentales que se deben cumplir.
Lidiar con las acciones de los estafadores.
Manejo de información de tarjetas de crédito de clientes, así como documentos personales como pasaportes. Actualmente, no vendemos en línea, pero está previsto y es un reto asegurar que todas las transacciones sean seguras.
Manejo de la información de las personas. Irresponsabilidad de colaboradores.
Mantener al máximo la disponibilidad de servicio.
Mantener la información confidencial.
Mantener seguridad y que todo el personal siga los protocolos.
Mantenerse al ritmo de evolución de las tecnologías digitales. Incorporar nuevos paradigmas de seguridad de datos.
Nuestro reto más grande es mantenernos informados y capacitados a la par de los grandes avances diarios en este campo.
Pérdida de datos críticos para el negocio, robo de información confidencial.
Permanecer protegidos contra ataques cibernéticos.

Presupuesto y recursos humanos.
Protegernos contra la fuga de información.
Seguir evangelizando a todos los empleados de que la seguridad es básica y deben seguirse los procesos correspondientes.
Seguridad informática también tiene que ver con la seguridad personal (robo, secuestro, etc.). Como empresa, quieres ser visto por prospectos y clientes, estar posicionado. Como persona, quieres pasar desapercibido, no atraer la atención, pues las redes están al acceso público de quien elija acceder a esa información. Para buen uso o para "cazarte".
Siendo activistas, y a veces personas non gratas para el sistema, hemos tenido casos de espionaje y acoso.
Tener éxito en el manejo seguro de datos de terceros, así como el resguardo de nuestra información clave y confidencial.
Trump.
Uno de nuestros retos importantes es el poder migrar a la nube nuestra información y tenerla más segura y accesible.
Usabilidad de las plataformas vs. políticas de seguridad.

Situación de México frente a otros países en materia de seguridad en medios digitales

Pregunta: Comparado con otros países, ¿cómo considera que se encuentra México en cuanto a seguridad en medios digitales?

Intencionalmente, no se quiso establecer parámetros de comparación (por ejemplo, contra países específicos), para no influenciar las respuestas, al buscarse el "*top of mind*" dentro de la pregunta.



Razones por las que se tiene esa percepción

Las respuestas fueron codificadas y agrupadas de la siguiente manera:

México se encuentra MUCHO MEJOR	
Hay conciencia/educación/difusión	1
Solidez de la banca en México	1
Se tienen avances significativos	1

México se encuentra MEJOR	
Hay conciencia/educación/difusión	3
Atrasados frente a unos y adelantados frente a otros	2

México se encuentra MEJOR	
Lineamientos/infraestructura de seguridad internacionales	1
Crecimiento y adopción de mejores prácticas	1

México se encuentra IGUAL	
Niveles similares en lo general	10
Lineamientos/infraestructura de seguridad internacionales	9
Lidiamos con los mismos problemas	5
Fácil acceso a la tecnología	4
Se tiene avances significativos	2
Atrasados frente a unos y adelantados frente a otros	2
Tecnología nacional buena	2
Existen facilidades para invertir	2
Mejor en unos aspectos y peor en otros	2
Ningún país es totalmente seguro	1
Empresas grandes bien, PyMEs no tanto	1
Existe una cultura de protección	1
Solidez de la banca en México	1

México se encuentra PEOR	
Falta conciencia/educación/difusión	20
Retrasos legales/regulatorios	9
Rezago tecnológico	8
Poca inversión	5
Altos índices delictivos	5
Escasa atención gubernamental	4
Se menciona en diversas fuentes	2
Altos costos	2
Peor que Estados Unidos	2
Disparidad entre empresa grande y Pymes	1
Atrasados frente a unos y adelantados frente a otros	1

México se encuentra MUCHO PEOR	
Se menciona en diversas fuentes	2
Poca inversión	1
Poco personal capacitado	1
Falta conciencia/educación/difusión	1
Escasa atención gubernamental	1
Peor que Estados Unidos	1

Se pueden consultar las respuestas más relevantes, tal como fueron expresadas por los entrevistados en el Anexo 11.

Sólo un 10% percibe que México como país se encuentra mejor en materia de seguridad en medios digitales frente a otros países en general.

Entre quienes consideran que México se encuentra mejor o igual respecto de otros países, las razones principales para tener esta percepción giran alrededor de que se tienen situaciones similares, tanto en lo que se refiere a la posibilidad de ser víctimas de ataques cibernéticos como a la equidad de la infraestructura y sistemas de seguridad con los que se cuenta. Tienen la impresión de que se aplican estándares y se tiene acceso a infraestructura de nivel internacional. En menor proporción, hay quien considera que los niveles de capacitación y difusión sobre el tema son buenos, hay facilidades para invertir y tienen confianza en los niveles de seguridad de la banca. Comentan que hay organizaciones muy maduras (generalmente, multinacionales), pero que la mayoría de las PyMEs no tiene recursos para invertir en seguridad informática.

Un 43% tiene la percepción de que, en general, México se encuentra peor que otros países, argumentando principalmente poca conciencia sobre el tema por parte de la población, baja educación y difusión insuficiente. Parte de esa falta de concienciación permea desde los tomadores de decisión, quienes prefieren correr riesgos altos para no incurrir en los costos que tiene la implementación de un buen sistema; muchos tienen una visión de corto plazo.

"El tema de seguridad no es entendido a profundidad. Se asume que por adquirir una tecnología en particular el problema está resuelto, cuando la seguridad en informática no es sólo un tema tecnológico, sino de cultura organizacional".

Se percibe que existe un rezago tecnológico provocado, entre otras razones, por una baja inversión, huecos legales y poca atención gubernamental; no hay un compromiso regulatorio y generalmente existe una postura laxa o reactiva. Fue mencionado el caso en el cual miembros del gobierno adquirieron *software* para espiar telefónicamente a diversas personalidades y periodistas, así como las granjas de bots utilizadas para crear tendencias de información política.

Se considera que existe muy poco personal de seguridad bien capacitado y que hay mucho charlatán en el medio.

Principales retos que enfrenta México como país en materia de seguridad en medios digitales

Pregunta: ¿Cuáles considera que son los mayores retos que enfrenta México como país respecto a la seguridad en medios digitales?

*Los **retos mencionados en el rubro "Otros"** son los siguientes: reducir/impedir los robos de identidad, medidas contra agresores internos, desarrollo de programas DRP/BCS, mayor apoyo a las PyMEs y profesionistas independientes, crear comunidades de expertos, incluir la estrategia de seguridad en los objetivos del negocio, responsabilidad compartida, garantizar la privacidad y confidencialidad, sobrepasar el rezago económico del país, incorporación de mejores prácticas de nivel mundial, incorporar el tema en programas educativos. Ver las respuestas más relevantes enlistadas en el Anexo 12.*

El reto de México más citado en esta materia (26.57% de los entrevistados) deriva de la percepción que se tiene acerca de que hace falta una mayor voluntad política y certeza jurídica para que, entre otras cosas, las empresas estén en posibilidades de invertir lo necesario en

seguridad informática. La idea de que a nivel gubernamental no se impulsa la transformación digital es constante. Se considera que no existe una legislación que regule los medios digitales. Además, es necesario establecer alianzas entre instituciones públicas y empresas privadas, capacitar a los usuarios, policías, ministerios públicos y jueces. Se indica también que el Estado no cuenta con una estructura que ataque la corrupción eficientemente ni ofrece garantías de castigo a los delincuentes.

En la misma proporción, más de una cuarta parte de los entrevistados considera que es indispensable culturizar a la población en general y difundir muchos más temas relacionados con la seguridad en medios digitales. Señalan que es apremiante fomentar la conciencia de los usuarios acerca de los riesgos que implica no estar debidamente protegidos ante las amenazas de las técnicas de la ingeniería social, ataques cibernéticos, mal uso de los dispositivos y aplicaciones y fraudes; es decir, crear conciencia del uso y protección de la información empresarial. Asimismo, se indicó que se necesitan acciones para difundir la utilización adecuada de las redes sociales y los beneficios de anticiparse en lugar de corregir, entre otros.

Se percibe la necesidad de fortalecer la educación y la capacitación en todo lo relacionado con la seguridad informática a diferentes niveles. Capacitar al público en general promoviendo una mayor cantidad de cursos sobre el tema, capacitar al personal de las empresas para que sean capaces de seguir los protocolos que mitiguen riesgos, fortalecer los conocimientos de los especialistas en tecnologías de la información en las organizaciones, fomentando la actualización constante, para que los proveedores de soluciones de seguridad cuenten con recursos humanos mejor capacitados.

No se invierte lo suficiente. El crecimiento de las empresas requiere adoptar sistemas de seguridad avanzados, lo cual demanda una inversión fuerte. No es sólo una cuestión de conciencia sobre el tema, sino también de presupuesto, principalmente por parte de las empresas medianas y pequeñas; faltan incentivos. Es indispensable una mayor inversión, tanto en capacitación como en infraestructura, de tal manera que se puedan aterrizar plataformas globales en México, modernizar los sistemas de seguridad en empresas, escuelas y gobierno. Es esencial destinar recursos para investigación y desarrollo en el país, para que las empresas tengan menores costos y mayor acceso a soluciones de seguridad de primer nivel, similar a la que ofrecen los proveedores globales.

Glosario de términos

Anti spyware	*Software* de seguridad informática que detecta, alerta y bloquea los efectos maliciosos de programas instalados en la memoria de los dispositivos, que están observando y enviando información de lo que realiza el usuario.
Antivirus	Programa cuyo objetivo es detectar, detener y eliminar virus informáticos. Estos programas utilizan algoritmos para determinar la intención de un programa, contrastar con bases de datos en donde se han vetado tales programas maliciosos o incluso la ejecución de estos en sistemas controlados y cerrados.
Apps	Son aplicaciones o programas para que las personas realicen actividades diversas en los *smartphones* (teléfonos inteligentes), tabletas y otros dispositivos móviles.
Arquitectura (de TI)	Son todos los componentes (*hardware*, *software* y telecomunicaciones) que intervienen en el funcionamiento específico de un sistema o conjunto de sistemas diseñados para fines informáticos determinados.
BCP	Continuidad de proceso de negocio (por sus siglas en inglés *Business Continuity Process*). La estrategia establecida para poder continuar con la operación de una organización, aunque existan partes que hayan fallado por motivos técnicos.
Biométrico	Método por el cual se identifica a la persona, basado en el reconocimiento de características físicas intransferibles, como lo son la huella digital, el patrón venoso del dedo, la retina ocular o el reconocimiento facial, entre otras.
Blockchain	Es una base de datos estructurada para utilizarse por grandes grupos de personas y cuyas modificaciones de la información son registradas. Los datos están cifrados y almacenados en bloques que son encadenados al bloque previo de información que queda imposibilitado de modificarse al recibir un sello de fecha. Cada nueva información genera un bloque nuevo con vínculo al anterior, de ahí el nombre en inglés que en español se traduce como “cadena de bloques”. De esta manera, queda un registro secuencial inalterable.
Bullying	Es la acción de atacar repetidamente a una persona para mostrar una supuesta superioridad sobre ella o con fines de ensuciar su imagen o prestigio ante terceros. Promueve que otras personas se sumen a esta acción en contra de la víctima para amplificar sus efectos de daño. Puede consistir en ataques verbales o físicos, aunque en el ámbito digital suele realizarse verbalmente y con representaciones gráficas, como la publicación de memes, divulgación de secretos en redes sociales, lenguaje agresivo y denigrante.
BYOD	“Trae tu propio dispositivo” sería la traducción al español de las siglas en inglés *Bring Your Own Device*). Es una práctica mediante la cual una organización permite que los miembros puedan utilizar dispositivos personales propios (por ejemplo, teléfonos inteligentes), implementando medidas para permitir que dichos dispositivos se utilicen para conectarse a la red de la organización y acceder a información o funciones de la organización en cuestión.

Cámara de eco social	Es un mecanismo a través del cual ciertos sitios web van almacenando un historial de nuestros hábitos y preferencias de navegación, asociándolo con características y rasgos personales, de manera tal que cuando regresamos al sitio puedan "decidir" cuál información presentarnos, en qué orden y filtrar el contenido según criterios que definen lo que se considera relevante para nosotros. Esto es posible en todos aquellos sitios web donde el usuario debe firmarse (identificarse) para interactuar, gracias a la creación de perfiles y acceso a través de un identificador único (nombre de usuario y contraseña, por ejemplo). De esta manera, cuando nos firmamos en algún sitio o red social de suscripción, cuando hacemos búsquedas estando previamente autenticados en el explorador (Chrome o Edge, por ejemplo), o cuando entramos a sitios diversos con las credenciales de una de nuestras cuentas habituales, estamos alimentando la base de datos que estos proveedores tienen acerca de nosotros.
Certificado de seguridad	Un elemento de *software* emitido por una autoridad independiente que valida que un ente en Internet (generalmente una *app* o una página) es auténtico, y que está registrado por alguna persona u organización. Hay diversos certificados de seguridad, para diferentes usos.
Cifrado (de datos)	Se refiere al proceso matemático para hacer que un mensaje sea ilegible, excepto para la persona que posee la clave para descifrarlo.
Clickbait	Es una técnica para captar la atención de los lectores o personas que navegan por la web, a través de titulares o promesas espectaculares (ganchos), los cuales en muchas ocasiones llevan a contenidos de mala calidad, noticias falsas o acciones maliciosas como *phishing*.
Clonación	Consiste en la reproducción apócrifa de información u objetos (físicos o digitales) con propósitos fraudulentos, como podrían ser tarjetas de crédito, instrumentos digitales de pago, credenciales de acceso, etcétera.
Cookies	Código en formato de texto que algunos sitios web almacenan en el disco duro del usuario visitante, con el propósito de que el propio sitio web obtenga información acerca del usuario para visitas subsecuentes. Por ejemplo, para identificar si es la primera visita del usuario al sitio o si es un visitante recurrente.
DRP	Plan de recuperación en caso de desastre (por sus siglas en inglés *Disaster Recovery Plan*). Describe pasos específicos para recuperar información y la operación tecnológica de un organismo. Incluye procesos de comunicación, remediación y alternativas de equipo a utilizar. Generalmente, es parte de la estrategia general de un BCP.
Encriptación	El proceso mediante el cual se cifran los datos de tal manera que sólo una persona que cuente con la forma de descifrarlos los podrá entender. Se utiliza para que la información esté segura en caso de ser interceptada por alguien que no tenga permiso para verla.
Firewall	Dispositivo de seguridad que monitorea el tráfico de red, discrimina si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
Geolocalización	Facultad que tienen los dispositivos para enviar información de la ubicación geográfica donde se encuentra a través de señales que se transmiten por la red satelital.
Hacker	Persona con conocimientos de informática que se dedica a detectar fallos de seguridad en sistemas informáticos.

HTTP / HTTPS	(Abreviatura de *HyperText Transfer Protocol / HyperText Transfer Protocol Secure*). La serie de comandos y servicios (protocolo) que se utilizan para transmitir datos a páginas de Internet. HTTP no está cifrado, por lo cual la información puede ser vista por cualquier persona, mientras que HTTPS sí está cifrada, haciéndola más segura.
Ingeniería social	Es un método para obtener información y datos confidenciales de las personas a través de la manipulación y el engaño. Quien ejecuta este tipo de actividades establece escenarios en los que la víctima tenga una urgencia de revelar información; por ejemplo, advertir de un posible fraude, por lo que se solicitan datos para detener el supuesto atraco. Esta técnica es comúnmente utilizada para usurpar datos que puedan otorgar suficientes credenciales para suplantar a la víctima y realizar actos en su nombre y sin su consentimiento.
Inteligencia artificial	Funciones que llevan a cabo computadoras o máquinas que se asemejan a las que utilizan los humanos. Incluye interacciones con humanos, así como el poder "construir" deducciones de acuerdo con información recibida.
Machine Learning	Aprendizaje de máquina. Es el proceso mediante el cual computadoras u otras máquinas "aprenden" combinando datos y adaptándose a nuevas situaciones para realizar tareas que no han sido programadas específicamente con anterioridad.
Malware	*Software* nocivo diseñado para infiltrarse en un dispositivo sin conocimiento del usuario.
Medio de autenticación	La forma en la que un usuario o programa se identifica ante otro. Esto puede incluir claves de acceso sencillas o múltiples, dispositivos adicionales, elementos físicos como huella digital, certificado (de seguridad), etcétera.
Mobbing	Se refiere a la violencia psicológica en el entorno laboral. A nivel cibernético, puede presentarse en la modalidad de acoso, chismes, comentarios contra la dignidad y prestigio de la persona acosada, por medio de mensajes de texto, correo electrónico, plataformas colaborativas, videoconferencias, uso de las redes sociales, etcétera.
NDA	Acuerdo de confidencialidad o acuerdo de no divulgación (por sus siglas en inglés *Non Disclosure Agreement*). Un documento que se firma donde se acuerda que cierta información comunicada a una o ambas partes no podrá ser divulgada a terceras personas.
Nube	Conjunto de servidores a los cuales se puede acceder desde conexiones en Internet; posibilita que se tenga acceso desde cualquier lugar y dispositivo permitido, porque la información no reside en el dispositivo como tal.
Pharming	Este método dirige a un usuario de Internet hacia un sitio web falso que simula uno auténtico. Al llevar al usuario a esta página falsa se le solicitan credenciales y datos personales para utilizarlos posteriormente.
Phishing	Método de engaño en donde se busca que la víctima comparta contraseñas, números de tarjeta de crédito y otra información confidencial, haciéndose pasar por una institución o fuente de confianza en un mensaje de correo electrónico, llamada telefónica o similar.
Piratería	Refiere a actos de utilización de información, paquetería o *apps* no autorizados directa o indirectamente por el titular de los derechos. Habitualmente, se utiliza para referirse a las conductas ilícitas de reproducción (copia) y distribución de ejemplares de obras y producciones intelectuales.

Pixel de rastreo	Es un código que define un gráfico imperceptible de 1 x 1 pixeles, el cual se inserta en alguna imagen o parte gráfica de una o varias páginas web. En el momento en que la imagen se despliega en el equipo del usuario a través de un navegador, el dueño del sitio recopila cierta información (como la dirección IP del equipo). En un proceso de compra, por ejemplo, es posible saber cómo el mismo usuario llegó al sitio, dónde dio click, cuál sección visualizó después y el momento en el que sale. Se utiliza principalmente en marketing digital para medir conversiones.
Protocolo (de seguridad)	Es un proceso informático que, a través de ciertas reglas y estructura, permite a los sistemas comunicarse entre sí para enviar, recibir e interpretar datos, así como para realizar ciertas acciones con base en órdenes específicas. Los protocolos enfocados a la seguridad digital están formados por reglas específicas para evaluar riesgos, identificar amenazas y tomar acciones que eviten o disminuyan la vulnerabilidad de los sistemas.
Ransomware	*Software* y mecanismo de extorsión por el cual un intruso (agresor externo) "secuestra" la información y el acceso a un equipo de cómputo a través de encriptar partes o la totalidad del sistema, impidiendo así que el propietario de la información pueda acceder a ella. El atacante solicita entonces un rescate (principalmente monetario a través de métodos no rastreables) a cambio de desencriptar los accesos y permitir que el usuario recupere el contenido. Para hacerlo, por lo regular, el agresor consigue ejecutar de manera remota el código malicioso en el equipo infectado, por medio de *phishing* u otros mecanismos de engaño.
Sistema operativo	La plataforma de *software* sobre la cual corren diversos programas específicos. Ejemplos de sistemas operativos son Windows, MacOS, IOS y Android.
SOC	Centro de operación de seguridad (por sus siglas en inglés *Security Operation Center*). Un lugar donde se concentran las funciones de seguridad, incluyendo detección, remediación, monitoreo, etcétera.
Spam	Consiste en mensajes (correos, mensajes de texto o pantallas emergentes) enviados masivamente a través de sistemas especializados para su distribución a gran escala, que llegan a los dispositivos de las personas o se despliegan ante el usuario sin su autorización. Se caracterizan por la incomodidad que causan al distraer atención y tiempo del usuario en asuntos que no son de su interés y por ocupar espacio de manera innecesaria. Comúnmente, la difusión de estos mensajes persigue objetivos comerciales o propagandísticos.
Spyware	Son pequeños programas o código que es instalado clandestinamente en la memoria de los dispositivos, con la finalidad de "espiar" u obtener información acerca de la actividad de los usuarios durante la operación de los mismos. Ejemplos de *spyware* son, entre otros, los lectores de pantalla, lectores de tecleo, grabadores de actividades, rastreadores de navegación, etcétera.
SSL	Capa de conexión segura (por sus siglas en inglés *Secure Sockets Layer*). Es una tecnología para encriptar información entre dispositivos, generalmente, entre un navegador y un sitio de Internet, por ejemplo.
Tarjeta digital	Una tarjeta bancaria que no existe físicamente. El banco la emite de manera virtual, algunos datos cambian para cada compra y tienen una vigencia muy corta. Es una manera más segura de comprar en línea, al no compartir datos que puedan ser reutilizados de manera fraudulenta porque dejan de ser válidos.

Virus	Es un programa que tiene por objetivo alterar el funcionamiento de equipos informáticos a favor de quien lo escribe, reemplazando otros programas necesarios para el funcionamiento intencional original. Estos "programas" suelen contener instrucciones para replicarse a otras máquinas e inocularlas. Sus intenciones son atrofiar funciones, o tomar control del dispositivo para uso remoto, o el robo de información.
VPN	Red privada virtual (por las siglas en inglés *Virtual Private Network*). Es una tecnología que permite establecer enlaces mediante redes públicas para conectarse a una ubicación específica como si se tratara de una red privada; de esta manera, se puede acceder a ciertos servicios y funcionalidades de administración. La paquetería y aplicaciones utilizadas mediante VPN gozan de la funcionalidad y seguridad de una red privada. Es común que este tipo de enlaces se transmita de manera cifrada.

Artículos de interés

La importancia (casi siempre comentada pero rara vez ejecutada) de los procesos en la seguridad de la información.

Por **John Serrano**
Director general
JFStrategy

Imaginemos un vuelo al espacio donde no se siguen procesos. Donde se mezcle el combustible a criterio de la persona encargada ese día, donde se revisen o no los diversos módulos antes de iniciar el viaje, donde se deje a la casualidad la fecha y el ángulo de despegue, reentrada a la atmósfera o aterrizaje. ¿Qué podría salir mal?
Suena absurdo y, sin embargo, en temas de seguridad de la información, la gran mayoría de las empresas no siguen procesos claros y definidos, lo cual resulta en pérdidas, robos, falta de disponibilidad de información e, inclusive, en mucho trabajo y esfuerzo adicional no redituable.
¿Por qué muchas empresas no siguen procesos? En la experiencia de JFStrategy, hay varios motivos comunes:

- Las empresas no han realizado el trabajo suficiente para establecer los procesos necesarios.
- No se han llevado a cabo los esfuerzos que son fundamentales para comunicar, revisar y evaluar la ejecución de los procesos.
- Los procesos no van de acuerdo con la realidad operativa de la empresa.
- Los procesos son un “libro muerto” que se hizo únicamente para cumplir con algún requisito.

Todos estos temas están ligados, de alguna manera, al hecho de que muchas empresas no le dan la debida importancia al establecimiento de procesos adecuados. ¿Qué debe tener un proceso en seguridad de la información?

- Tiene que proteger lo que se quiere proteger. Parece evidente, pero un proceso que protege algo innecesario, o que no protege algo importante, es inútil.
- Debe estar redactado claramente e incluir, entre otros temas:
  - Quién debe hacer qué.
  - Quién no debe hacer qué.
  - Quién debe estar comunicado respecto de qué.
- Ha de ser práctico. Esto es algo que se pierde de vista muchas veces. En un ejemplo de la vida real, en JFStrategy estábamos realizando un análisis de seguridad. Había un área donde se guardaban documentos valiosos. Para entrar

> a esta área se tenía que usar un detector de la palma de la mano, junto con una clave numérica para la cerradura. El problema es que en la misma área guardaban papelería en general, de uso común, y por lo cual personas tenían que entrar y salir una o dos veces por hora. Como resultó evidente, nadie usaba la palma de la mano más el código nueve o diez veces al día; la solución creativa fue trabar la puerta con una madera para facilitar el acceso.

A final de cuentas, un buen proceso de seguridad debe ser útil, relativamente fácil de seguir, no aumentar la burocracia o entorpecer la operación, debe ser revisado frecuentemente para ver si sigue cumpliendo su función y debe forma parte del ADN operativo de toda organización.

El papel del usuario en la seguridad de la ciudadanía digital

Por **Víctor Hugo O'Farrill**
Director de estrategia
JFStrategy

La reciente aceleración en la adopción de tecnologías digitales ha trastornado el entorno y ha colocado a los profesionales de este ámbito ante nuevas preguntas y líneas de investigación. Ahora bien, también han salido a relucir algunas preguntas añejas. Y en cuanto a seguridad digital, la situación pide atención de fondo y es inaplazable.

La reciente marejada digital nos ha hecho encarar de nuevo, y aún con más vehemencia, el caso de un factor bien conocido para quienes se dedican a la seguridad digital, pero que no deja de sorprender: los usuarios no se sienten parte del problema.

Si bien el atribuir el fracaso a factores exógenos y "a la suerte" es una condición humana muy común, no por esto deja de ser un tema de carácter prioritario el que los expertos en seguridad atiendan con más atención el factor humano. No hay opción si es que desean que sus sistemas logren la eficacia y eficiencia para la que los diseñaron y construyeron. Es la carencia de cultura de seguridad digital por parte de los usuarios una de las principales razones que hacen que incluso avanzados y sofisticados sistemas se queden cortos.

Los investigadores Steven Furnell e Ismini Vasileiou publican en 2017 el documento ***Security education and awareness: just let them burn?*** (doi.org/10.1016/S1353-4858(17)30122-8). En su texto, los investigadores demuestran cómo la vulnerabilidad de los sistemas es fuertemente afectada por la reducida conciencia, educación y entrenamiento en ciberseguridad en general. No es solamente un asunto técnico, nos dicen.

JFStrategy ha observado que hay un requisito necesario previo para propiciar un mejor entorno de actitud y aptitud, y que está presente en quien mejor implementa sistemas de seguridad: la conciencia de que la solución está en los usuarios (el virus de dos patas) como ciudadanos del mundo digital.

Own the problem es una frase que no resulta tan fácil de traducir al español, al menos no lo es de una manera tan sucinta como en el inglés. Significa hacerse total y personalmente responsable del problema y la solución. "Hacerse del problema" es indispensable si en realidad

queremos resolver algo. Es decir, tendemos a no resolver lo que no es un problema. Aún más, podemos estorbar a solucionar un problema nuestro cuando creemos que es de alguien más.

Provocar la actitud correcta de "*Ownership*" en los individuos y organizaciones no es necesariamente fácil. Sin embargo, es absolutamente necesario hacerlos parte de la solución para lograr una situación fértil para la adopción de tecnologías y métodos de seguridad digital.

Cuando estamos inmersos en el día a día, resulta caro y difícil identificar qué estamos haciendo y cómo lo estamos haciendo. Esta situación se puede gestionar de manera más certera y eficiente con la ayuda de agentes externos, consultores, que investiguen y procuren el desarrollo de técnicas y conocimiento. Mediante el uso de este tipo de agentes, podemos facilitar tanto la introspección como la implementación de mejores prácticas y la actitud correcta.

Si queremos avanzar en el terreno de seguridad digital, necesitamos de herramientas tecnológicas, mejores prácticas y, primordialmente, de usuarios conscientes de que la solución comienza por ellos mismos. Tomar en cuenta el vínculo personal con la situación es pilar para lograr niveles mínimos de seguridad; es necesario y urgente.

Cultura de riesgos a través del liderazgo

Por **Beatriz Sánchez**
Socia directora
BlackCat

Hoy en día, la vida no puede ser concebida sin la tecnología y los medios digitales que nos permiten comunicarnos más eficientemente. Sin embargo, así como pueden ser útiles, también conllevan riesgos y, por lo tanto, deben ser manejados con los cuidados necesarios para procurar la seguridad de sus usuarios.

En este estudio de "*Percepción sobre seguridad digital en México*", es evidente que los entrevistados están conscientes de los riesgos de seguridad a los que se enfrentan las personas y las empresas cuando utilizan estas tecnologías. Sin embargo, se sigue aplicando una estrategia obsoleta al abordarlos.

Hablando recientemente con el director general de una reconocida empresa, me decía que "no quería pensar sobre la seguridad", refiriéndose a que cuando los sistemas y su seguridad funcionan bien, no es notable; como un iceberg tecnológico imperceptible para el usuario. Es sólo cuando hay un problema que los usuarios piensan en el tema y en su trascendencia.

Su punto de vista es comprensible, así como la necesidad de que el negocio se enfoque en sus objetivos y que, de manera paralela, exista certeza en la confiabilidad y seguridad de sus herramientas tecnológicas. La problemática con esta perspectiva es que la obligación de entregar servicios funcionales y seguros recae totalmente en las áreas de seguridad y TI, deslindando a los usuarios de la responsabilidad por su manejo y a la Alta Dirección por su supervisión.

Para que las empresas puedan utilizar estos medios digitales como habilitadores para el negocio, es indispensable que la Alta Dirección tome responsabilidad sobre el gobierno de la seguridad. Informes realizados por organismos internacionales, tales como el Foro Económico Mundial, reconocen dentro de los principales riesgos actuales y futuros a los ciberataques, el fraude o robo de información y las fallas de la infraestructura. Considerarlos dentro de los riesgos de operación permite a la Dirección mantener su visibilidad y tratarlos adecuadamente.

En cuanto a la responsabilidad de los usuarios, se torna imprescindible reconocer la influencia de su comportamiento para la seguridad de la información. Actualmente, en muchas empresas, la capacitación y concientización de seguridad de la información no forma parte del currículo estándar a cubrir por los empleados. Esto se vuelve aún más preocupante cuando se presentan amenazas que dependen de la posibilidad de engaño, error o negligencia del usuario para causar una vulneración, tales como las expuestas en este estudio.

Encuentro relevante destacar los siguientes puntos clave para crear un cambio en la cultura de seguridad de la información de las empresas: involucrar a cada nivel, empezando por los más altos directivos, y permitir la comunicación bidireccional para escuchar los requerimientos de la empresa y las inquietudes del personal y actuar en consecuencia. La seguridad no puede funcionar si no se hacen partícipes al usuario y al negocio.

¿Por qué es relevante la seguridad en un sitio web?

Por **Eduardo Zimbrón**
Director de investigación
JFStrategy

Hay quien piensa que, al ser las instituciones financieras y las grandes marcas de la industria el principal objetivo para la delincuencia digital, la responsabilidad de proteger la integridad de un sitio web corresponde exclusivamente a las grandes corporaciones, bancos y tiendas de comercio electrónico. Algunas PyMEs y muchas personas físicas con actividad empresarial piensan que sus sitios web, por ser pequeños y poco conocidos, están al margen de ataques cibernéticos.

Es frecuente, principalmente en páginas web solicitadas por personas que quieren promover sus servicios como profesionistas independientes o empresas pequeñas, que les hagan un desarrollo rápido y de bajo costo. Y claro, cuando uno revisa las especificaciones expresadas por el cliente, pues el desarrollo "cumple": permite tener presencia en Internet, está habilitado para vender, provee cuentas de correo electrónico y, además, está bonito. Ya está, el proveedor formaliza la entrega y cobra, mientras el cliente contento teclea "www……", llega a la página que tanto le gustó (su página), recibe correos a una dirección con un dominio propio… y listo.

Lo que hasta este momento no sabe el cliente es que ningún sitio web, por pequeño o desconocido que sea, puede evitar ser "hackeado" cuando hay ciertas omisiones de seguridad que traen consecuencias de magnitudes diversas, desde las más leves hasta otras verdaderamente nocivas; y todo por una desatención que en la mayoría de los casos ni siquiera representa una inversión adicional significativa. Vienen los problemas y es hasta entonces, ya con "el niño en el pozo", cuando se piensa en la seguridad como una exigencia necesaria, en un momento donde el control de daños puede ser costoso en lo económico, en tiempo invertido o en lo reputacional.

¿Qué riesgos puede tener un descuido de esta naturaleza? Mencionemos aquí algunos de ellos:

- **Caída del sitio o alentamiento** del mismo, lo que puede generar abandonos prematuros, así como disminución de ventas y de otro tipo de conversiones.

- Uso del servidor de hospedaje, utilizando la cuenta del cliente, para **envío de *spam***. Esto puede provocar que el sitio web sea removido de los resultados de los buscadores, generar problemas reputacionales, complicaciones con otros servidores de correo o colocar el dominio del sitio en una lista negra.
- Uso de la lista de correos alojada en el sitio, o de números de teléfono almacenados, para propósitos de ***phishing* o *scamming***.
- **Redirección** de los visitantes hacia ***websites* maliciosos**.
- **Pérdida de información** y de valiosas horas de trabajo.
- **Robo de datos personales** de clientes / suscriptores.
- **Robo de información** bancaria, claves de acceso, etcétera.
- Intromisión para **cambiar el contenido del sitio** que puede causar un daño reputacional al propietario del mismo o bien difundir propaganda ideológica, política o religiosa.

¿Y qué se puede hacer para disminuir estos riesgos?

Si bien las opciones que se presentan a continuación no forman una lista exhaustiva, sí son algunas sugerencias que, de manera sencilla, pueden evitar dolores de cabeza innecesarios:

El primer paso, y uno de los más importantes, es contratar el hospedaje del sitio con un proveedor profesional y reconocido que tenga servicios probados de alta disponibilidad y seguridad. Ellos invierten grandes cantidades de dinero en infraestructura para una alta seguridad y mejor desempeño. Este es uno de los rubros en los que menos se debe escatimar.

En segundo lugar, es conveniente escoger un desarrollador web experimentado, que dé énfasis a las cuestiones de seguridad y se haga cargo, entre otras cosas, de las configuraciones en el servidor de hospedaje, configuraciones del Gestor de Contenidos Web (CMS) y los *plugins* respectivos, habilite el cifrado de datos, certificados digitales, etcétera.

Es importante que dentro del plan de hospedaje contratado se realicen respaldos automatizados del sitio completo, con la periodicidad más corta posible (de preferencia diaria). Eventualmente, conviene bajar respaldos del sitio y de la base de datos para almacenarlos de manera local, sobre todo antes de hacer cambios significativos a la estructura y funcionalidad del sitio.

Es necesario estar al pendiente de la publicación periódica de actualizaciones de todos los componentes del sitio (CMS, lenguaje de programación, *plugins*, extensiones, *scripts*, bases de datos) para instalarlas con oportunidad; no solo mejoran la funcionalidad de los sitios, sino que también ayudan a corregir diversas vulnerabilidades detectadas.

La capacitación de las personas que tienen privilegios para manipular parte o la totalidad del sitio es fundamental. No sólo se trata del personal del desarrollador del sitio, sino de todos los colaboradores (para alimentar un blog, por ejemplo) y del mismo cliente para subir promociones o actualizar el catálogo de sus productos.

Se debe tener un criterio desarrollado para la creación de contraseñas seguras para todos los colaboradores en el sitio, las cuales deberán cambiarse periódicamente.

Hay que asegurarse de que el sitio web, bien sea por medio de la infraestructura del servicio de hospedaje o por algún mecanismo complementario, cuenta con los servicios de *firewall*, protecciones *antimalware*, funciones de monitoreo, etcétera.

Dependiendo de las características del sitio y su propósito, puede solicitarse asesoría adicional sobre soluciones de seguridad complementarias. Así que, si se desea conocer más acerca de proveedores y mejores prácticas, conviene consultar a un experto.

Anexos

Anexo 1. Lista de participantes en la encuesta

(Listado en orden alfabético)

NOMBRE	PUESTO	EMPRESA
(confidencial a petición del participante)	Director general	*(confidencial a petición del participante)*
Abraham Achar	CEO	Novelty Corp de México
Aldo Mizrahi	CEO	Emida
Alejandro Almazán	Director general	Únete
Alejandro Chiapas	Director general	Net & Services Trantor
Alejandro García Cruz	Hyperscale Computing Manager	Seidor México
Alejandro Gorches	Director Administración y Finanzas	Consejo de la Judicatura Federal
Alejandro Ibarra	CEO	Digipro
Alejandro Martínez	Director comercial	Global Positive Systems
Alejandro Mayagoitia	VP Planeación estratégica	Iexpertus
Alejandro Zenteno	VP Global de RH	Grupo Lala
Alexander Van Tienhoven	Socio fundador	Kratos Capital, SC
Alfredo Duclaud	Director general	Medios Amsivos Mexicanos
Alma Zavala	Gerente eficiencia operativa	Farmacias San Pablo
Alonso Carral	EMC	Stratg Pte Lrd
Andrés Carral	Socio	Carral & Ass.
Andrés García	Gerente	Huawei
Andrés Velázquez	Presidente	Mattica
Ángel García-Lascurain	Socio director	Tantum Group
Antonio Dosal	Dueño	Dosalax
Antonio García	Director general	I Tech Selling Tech
Axel Vera	Arquitecto de soluciones	Juganu
Balbino Gallego	Gerente general	Sogams SA
Bárbara Mair	Directora	Automation Anywhere
Beatriz Sánchez	Socia directora	Blackcat Research SC
Benjamín Carrillo	Asesor de energía	Marsam Solar
Carlos Arzate	Gerente de tecnología	Cinépolis
Carlos Echegaray	Vicepresidente	Amac Impresos SA de CV
Carlos Niembro	Director comercial	Potencia Educativa
Carlos Salinas	VP	Mexico Consulting Partners
Carlos Villalobos	Desarrollo de negocios	Impulso Mexicano en Desarrollo de Negocios
Carolina Tatay	Director general	Neta Systems
César Buenrostro	Director general	Consultoría Interdisciplinaria en Planeación y Desarrollo, S.C.
Claudio Núñez	Director general	NSC Asesores
Dan Ostrosky	Presidente	Seguridata Privada
Daniel Roig	Director general	Grupo Bracsa

David Cárdenas	Director	Riskmg
David Leo	CIO	Grupo Toks
David Meza	Director desarrollo negocios TI	Mcpraxo
Diego Pérez Salazar	Socio	Ortomove
Edgar Matute	Founder/CEO	Wellbeing Network
Edmundo Gómez	Gerente de sistemas	Maquinados y Estampados Nacionales
Eduardo Hermosillo	Director general	Colegio Walden Dos
Eduardo Martínez	Director	Fresco
Eduardo Reinking	Subdirector comercial	Periódico Reforma
Eduardo Sicilia	Director general	Moulds Plus México SA de CV
Enrique Felgueres	President & CEO	Unico Travel by Felgueres
Enrique Gómez Gordillo	Director	Más Poder de Ventas
Enrique Haro	Founder	Code3E
Enrique Torres	Senior Product Manager	Huawei Technologies Engineering de México
Ernesto Chacón	Director Administración y Finanzas	Grupo Dival
Eugenio Perea	Venture Partner	Magma Partner
Eva Sander	Director ejecutivo	Accountability Lab México
Fernando Gutiérrez	Director División de Humanidades y Educación	Tecnológico de Monterrey
Fernando Pérez-Gavilán	Presidente	Born Free SA de CV
Fernando Serrato	CIO	Deloitte
Francisco Cándido	IT Coordinator	Hays Recruiting Experts
Francisco Reynoso	Director estrategia	Totalplay Empresarial
Freddy Turriaf	Director comercial	Zequenze
Gabriela Warkentin	Maestra	Escuela
Gael Thome	Socio	Multiplica
George Gelman	Director general	Centro Internacional de Inteligencia, SA de CV
Germán Olivera	CEO	Freedompop
Guillermo Cásares	Director general	Mexis
Guillermo Muñoz	Director general	Dispro
Guillermo Salcedo	Director de producto	IZZI
Guy Nae	Enterprise Head	Apple
Héctor Ortiz	CEO	Anzen Trading Llc
Héctor Treviño	Director ejecutivo	Asociación Mexicana de Energía Eólica, A.C. (Amdee)
Imanol Belausteguigoitia	Director	Centro de Desarrollo para la Empresa Familiar (ITAM)
Israel Madiedo	Director de Innovación Y Tecnología	IZZI
Javier Allard	Director general	Amiti
Javier Landeros	Director de Tecnologías de Información	The American School Foundation, A.C.
Jesús Saucedo	Managing Partner	Northgate Capital
Johannes Hauser	Director general	Camexa
John Farrell	General Partner	Dila Capital / Yaax Capital

Jorge Brandt	Socio	Legosoft
Jorge Esquivel	Account Manager	Cisco Systems
Jorge Félix	Socio	Prointelligence
Jorge Reteguín	CTO	Retoware
Jorge Rivas	Director comercial	Cisa Consultores
José Antonio Cano	Director	Grupo Financiero Banorte
José Gómez Obregón	Socio director	E Level Service SC
Juan Carlos Álvarez	Director comercial	El Informador
Juan Carlos García Caparrós	Associate Partner Cybersecurity	Ey México y Latam North
Juan Eduardo Balboa	Country Manager	BlueBull Energy
Juan Francisco Gortárez	Director general	Grupo Corporativo Gorna
Juan Francisco Torres	Consultor Sr	RiskProNorm
Juan Güémez	Coordinador de Planeación	Televisa
Juan José de Régules	Socio	Sherpa-X
Juan Luis Zamora	Socio director	Blackcat Research SC
Juan Pablo Marquina	Director general	Marsam Soluciones Ambientales, S.A. de C.V.
Julián Pérez Duarte	Socio director	Acertare
Julieta Munguía	Comercial	
Julio Méndez	Sales Director of Key Accounts México	Anixter de México
Lalo Durón	Managing Partner	Big, Ingeniería de Marketing
Lorena Juárez	PM Sr. Latam	The Adecco Group
Luis Befeler	Director general	Befeler y Compañía, S.C.
Luis Estrada	CEO	Spin
Luis Larrátegui	Director general	Grupo Conark
Luis Leonardo Pérez	Director de Operaciones	Neta Systems
Luis Olivé	Socio	Monemilia
Luis Sayrols	CEO	Lyrsa Comunicación
Luis Tenorio	Sales Sr Manager	Accenture
Malú Cisneros	Project Manager SR	
Manuel Torres	Chief Brand Officer	Zag Animation
Manuel Tron	Socio director	Manuel Tron SC
Mar Fuentes	CEO	El Gabinete. Museos + Historias + Tecnología
Mario Nissan	CEO	Isobar
Martín Orbea	Gerente Mercadotecnia	Grupo Affinitas
Mauricio Jessurun	Presidente	Corporación Unisol SA de CV
Michel Wohlmuth	CEO	Creatividad
Miguel Ángel Azuara	Director de TI Latinoamérica	Stanley Black & Decker
Miguel del Villar	CEO	PGT

Natalia Ortiz Mena	Socio director / Coach ejecutivo	Coaching y Desarrollo SC
Olivier Martín	Director de Operaciones	EXMAR
Otto Graff	Socio	Ignia
Pablo Musi	Managing Director	Marsh & Mclennan, Marsh Lorant
Paola Jiménez	Abogado	
Pascal Wolf	Consultor	Independiente
Pedro Asturiano	Director de Operaciones y Sistemas	Tele Urban
Rafael Morfín	Director	CRB Seguros y Fianzas
Raúl Lucido	CEO	International Telecom & IT Markets Consultants
Raúl Varela	Director de Riesgos de Crédito Consumo y Empresarial	Banco Inbursa
Raziel Latz	CEO	Yomero Consulting
Ricardo Álvarez	Investigador	Massachusetts Institute of Technology
Ricardo Olvera	Subdirector de Innovación	Alsea
Roberto Centeno	CIO	Aerolíneas Ejecutivas, SA de CV
Roberto Crespo	Director de TI (CIO)	Grupo Mexicano de Desarrollo
Roberto Toledo	Socio director	Alpha Consultoría
Rodolfo Cavalcanti	CEO	On&Off Network
Rodrigo Gómez	Managing Partner	Capital Índigo
Rolando López	Director	Soluciona México
Ronald Pool	Sr. Territory Manager	Epicor Software
Rosa Pisinger	Secretaria de Consejo Normativo Consultivo	American School Foundation
Rossana Fuentes	CEO	México Media Lab
Salvador Aponte	CIO	Alsea
Santiago Musi	Socio	IMA Consultores
Sergio F. Contreras	DGA	Grupo Efectivo Practivo
Sergio Sierra	Director	Sistemas y Equipo de Transporte
Susana Dávalos	Account Manager	Performance Talent Consulting
Thurston Hamer	Director	Garmin México
Victoria Haro	Rectora	Universidad del Medio Ambiente

Anexo 2. Respuestas más relevantes sobre las amenazas percibidas en Internet en general

(Listado en orden alfabético)

Acceso a información en dispositivos personales por medio de wifi no confiables.
Acceso a tu información y robo de identidad.
Acceso no autorizado a la información.
Ataques informáticos, robo de información, fraudes.
Child safety, Personal Data breach.
Clonación de información personal o uso mal intencionado de datos personales.
Conocimiento a detalle de gustos y necesidades.
DDOS y ataques al DNS.
Deficiente / inexistente rendición de cuentas.
Delincuencia organizada.
Entrar a sitos que contengan algún virus o te sigan después. Sitios falsos.
Espionaje.
Fake news, pornografía, identidades falsas.
Falta de conectividad.
Fraudes.
Hackeo, robo de identidad.
Hackers y piratas, robo de información.
Ignorancia.
Infecciones de *malware*, sustitución de identidad, acoso.
Información accesible a delincuentes.
La combinación de una arquitectura distribuida de servidores centralizadores de datos presenta una serie de vulnerabilidades de acceso y control que requiere de capas de control de acceso que por su complejidad incremental invariablemente tiende a colapsar.
La convivencia entre IPv4 e IPv6 evita la implementación de mejores medidas.
La gente carece de una cultura de seguridad mínima al navegar.
La poca protección de datos y su explotación comercial.
Links maliciosos.
Ninguna. Es un mundo en sí mismo y tenemos que aprender a vivir con y en él.
No hay privacidad.
Noticias falsas, virus, robo de información y de identidad, fraude, ciberterrorismo (ataque a infraestructura crítica).
Pérdida de información, hackeo de cuentas bancarias, acoso.
Phishing, robo de identidad.
Regulación.
Robo de datos.
Robo de identidad, espionaje, fraudes, acoso.
Robo de identidad, fraude, *malware*, virus.
Robo de identidad, infección de máquina.
Seguridad de la información personal sensible, tales como cuentas de banco.

Ser seguido por robots.
Sin aplicar censura, que los contenidos sean verdaderos.
Sistemas intrusivos.
Sitios fraudulentos, acceso remoto a información privada, proliferación de *malware*, etc.
Sitios inseguros / *apps* inseguras / redes inseguras.
Suplantación de identidad.
Virus informáticos.
Virus, hackers, gusanos, programas espía, otros. *Spam*, *phishing*.
Virus, *malware*, *phishing*, *ransomware*.
Vulnerabilidad por ignorancia.

Anexo 3. Respuestas más relevantes sobre las amenazas percibidas en redes sociales

(Listado en orden alfabético)

Abusos a menores, *bullying*.
Acceso a mi información.
Acceso y uso de información personal no autorizada.
Acoso
Bots, *grooming*, *phishing*.
Comunicación inadecuada y *hacking*.
Conocimiento profundo del usuario, sus hábitos, gustos y contactos directos.
Dar información personal sensible sin darse cuenta. *Fake news*. Perder el tiempo sin darse cuenta.
Deepfakes.
Demasiada confianza en los datos personales.
Desinformación.
Despersonalización de los servicios y las comunicaciones.
Difusión de información o noticias falsas.
Engaño a usuarios.
Fake news y mala información.
Fake news, pornografía, identidades falsas, depresión.
Secuestros, fraudes.
Falta de cultura y seguridad.
Falta de legislación.
Fraude.
Fuente de información para la delincuencia.
Hackeo de cuentas.
Hackeo de la información de los usuarios.
Hackers.
Robo de perfiles.
Ignorancia e ingenuidad.
Improductividad.
Incremento de bases sociales reforzados por métodos de *machine learning* e inteligencia artificial debido a una tendencia sistémica en la recolección masiva de datos. Reforzamiento algorítmico de prácticas sociales indeseables. Profunda invasión a la privacidad, cámaras de eco sociales que incrementan el peligro de las *fake news*, riesgo de abuso social sobre individuos.
Insiders que venden información, políticas deficientes de privacidad.
Invasión de privacidad.
La gente comparte su vida y expone sus datos de forma indiscriminada.
La ignorancia de los usuarios.
Links maliciosos.
Mal uso de datos personales y metadatos.
Malware.

Manejo de datos personales.
Manipulación.
Medio para publicar cosas que lastimen a otros si no se usan bien.
Mostrar niveles de vida.
Muchas actividades criminales se facilitan por estos medios. La gente no es consciente de la información que deja ver al público.
Nadie sabe poner bien su seguridad en las redes.
No están reguladas.
Phishing.
Pornografía infantil.
Problemas de suplantación de identidad y robo de información.
Que te estén "cazando" para secuestro o robo a través de info que publicas para tu empresa.
Reducción en productividad.
Riesgos reputacionales y uso de información personal.
Robar mi cuenta para emitir opiniones o acceder a mi información personal.
Robo de información del perfil social.
Sobresaturación que dificulta distinguir la importante de lo trivial.
Su uso para influir masivamente a través de noticias falsas.
Time sucker - La genta gasta demasiado tiempo.

Anexo 4. Respuestas más relevantes sobre las amenazas percibidas en comercio electrónico

(Listado en orden alfabético)

1. Poca venta 2. Fraude (en ese orden)
Acceder a mi información para hacer transacciones sin mi consentimiento.
Acceso a información bancaria privada y su posible mal uso y distribución no autorizada.
Baja penetración por temor al fraude cibernético.
Bank/ CC fraud.
Capturan tu número de tarjeta y PIN para clonarlo.
Clonación de tarjetas y medios de pago.
Robo de información bancaria.
Conocimiento de gustos, tendencias, hábitos de compra.
Consolidación de mercados en monopolios debido a la ventaja del primer jugador. Monopsonio en el mercado laboral en sector de *retail*. Vulnerabilidad en datos personales incluyendo datos financieros. perfilación intrusiva a partir de patrones de comportamiento y consumo.
Desconfianza de los consumidores.
Desconocimiento.
El desplazamiento de fuentes de empleo.
El robo de información a grandes empresas en el ramo.
Empresas no conocidas o patito causan desconfianza.
Extracción datos.
Fake login pages.
Falta seguridad en la transacción de dinero en portales no tradicionales.
Fraude, robo de identidad, robo de TC.
Fraudes y tiempos de entrega.
Fraudes, mala calidad en productos, robo de información confidencial.
Hackeo de información financiera y dinero
Hackers, programas sin compra protegida, robos de identidad, *malware*.
Incertidumbre de que opere toda la cadena hasta la entrega en casa.
Incipientes mecanismos de seguridad.
Las implementaciones actuales no son a prueba de los programadores internos. Guardan muchos elementos sensibles.
Legalidad y servicio al cliente.
Logística y experiencia de compra.
Los bancos no tienen los sistemas adecuados y menos si se trata de compras a través de equipos móviles.
Mal uso de datos bancarios.
Ninguna
Ninguna. Más bien, es un gran canal.
No existen sistemas de entrega de paquetería baratos y buenos.
Phishing, *spyware*, *big data*.
Poca oferta y mal servicio.
Robo de identidad
Robo de información bancaria

Anexo 5. Respuestas más relevantes sobre las amenazas percibidas en banca electrónica

(Listado en orden alfabético)

Acceder a mi información para hacer transacciones sin mi consentimiento.
Actividad fraudulenta desde los bancos.
Baja penetración por temor al fraude cibernético.
Bank/ CC fraud.
Clonación.
Compra no protegida, hackers.
Conocimiento de movimientos y tendencias para venta de productos.
Deben asegurarse de que sus esfuerzos tecnológicos realmente funcionen en tiempo y forma.
Delincuencia organizada.
Demasiado margen de maniobra financiero concentrado en un solo lugar.
Dificultad en el uso.
El medio más atacado.
Facilidad para usuarios, mayores riesgos.
Fake login pages.
Fallas en los sistemas bancarios
Falta de acceso.
Fraude.
Fraudes, hackeo, robo de identidad.
Fraudes, pérdida de transacciones.
Fraudes, robo de información.
Fuertes diferencias de las plataformas de los bancos.
Hackeo a cuentas.
Hackeo electrónico.
Hombre en medio interceptando información.
Intercepción de transferencias.
Intrusos en las cuentas bancarias de los usuarios.
La veo bastante segura.
Links maliciosos.
Lo veo bien.
Mal uso de los datos. Tardanza en aplicar la transacción. Espacio gris antes de confirmar que quedó realizada. Complejo hacer o recibir transacciones a / desde otros países. SAT más complejo y estricto cada vez.
Malware.
La virtualización del dinero presenta riesgos naturales para cuentahabientes en caso de no contar con políticas y sistemas claros de seguridad y protección.
Ninguna.
Ninguna. Igual que con las compras en línea, es un gran canal.
No veo muchos riesgos.
Páginas falsas.

Phishing / suplantación de identidad.
Pobre oferta de productos (aplicaciones), seguridad cuestionable.
Robo (fraude), robo de identidad.
Robo de contraseñas para acceder a banca.
Robo de identidad y clonación de medios de pago.
Robo de identidad y cuentas.
Robo de identidad y de claves de acceso. Fraudes.
Robo de información.
Robo de información bancaria y personal.
Robo de información financiera, fraudes.
Seguridad en organismos reguladores y jugadores todavía no dedican suficiente presupuesto y recursos para evitar quebrantos.
Seguridad en transacciones y con la confiabilidad de que tus datos permanecerán seguros y anónimos. Muy baja inversión en tecnología.
Ser banco siempre es un imán para los hackers, nadie se salva.
Servicios deficientes.
Sus propios empleados son el mayor peligro.
Transacciones fallidas
Va a perder relevancia, reemplazado por chats (alipay).

Anexo 6. Respuestas más relevantes sobre las amenazas percibidas en correo electrónico

(Listado en orden alfabético)

Abuso y falta de cultura.
Acceso a contactos.
Acceso a mi información.
Ataques a equipos.
Ataques informáticos, robo de identidad.
Clonación de personalidad.
Diseminación de virus.
Divulgación de direcciones por parte de listas de distribución.
El espionaje exterior a la red, es decir, la obtención de *passwords* por medios no electrónicos.
Espionaje.
Excesivo, riesgoso, ingeniería social.
Exposición a *spam* e intentos de fraude.
Falsa identidad del remitente.
Fraudes.
Fuga de información por errores de usuarios.
Hackers.
Intercepción de información.
Invasión a la privacidad usando *machine learning* sobre análisis automatizado de contenidos. Puerta fácil para control de sistemas personales y de la organización a través de *malware*, *phishing*, virus, etc.
La gente cree y abre todo lo que le llega. Falta una cultura en seguridad.
Links maliciosos.
Mal uso del *spam*.
Malware y hackeos.
Malware y *phishing*
Ninguna.
Ninguna. Sigue siendo un medio válido de comunicación.
Phishing.
Phishing, fraude, *spam*, obtención de información sin autorización.
Ransomware.
Proliferación de *malware*, *ransomware*, virus. Distribución de información no autorizada.
Robo de identidad.
Robo de información confidencial.
Spam y amenazas.
Uso indebido de una cuenta.
Uso malicioso de la cuenta de correo.
Virus
Virus, correos con información falsa.

Anexo 7. Respuestas más relevantes sobre las amenazas percibidas en *apps* móviles

(Listado en orden alfabético)

Acceso a datos privados.
Acceso a funciones del dispositivo y su posible mal uso: información personal, ubicación, cámara, micrófono, archivos.
Acceso a información personal por la *app*, no relevante para el uso de la misma.
Actualizaciones de seguridad tardías.
Almacenamiento de información personal sin consentimiento.
Apps patito que roban datos.
Ataques, robo de información.
Código malicioso.
Comprometer datos personales.
Dar información sensible sin darse cuenta.
Descontrol, virus, clonación.
El compromiso de la seguridad de la información del usuario.
El SS7 es la puerta de entrada para cualquier ataque.
Espionaje por parte de fabricantes y *malware*.
Exceso de competidores, desconfianza del usuario.
Fraude.
Hackers.
Infecciones, consumo desconocido de datos, robo de información.
Invasión de datos aunado a localización espacial y geográfica. Alta vulnerabilidad sobre datos personales y sistemas que hacen uso de los mismos. Riesgo de invasión activa sobre sensores en dispositivos móviles.
Investigación de comportamientos.
La mayoría, las considero buenas.
Links maliciosos.
Malware y *phishing* y robo de identidad.
Ninguna. Al contrario, son los medios para agregar todavía más valor a los teléfonos.
Nivel desarrollo con alta inseguridad.
No hay una regulación.
No sabes qué información están guardando y compartiendo. Algunos consumen mucha memoria.
Paginas falsas, virus y robo.
Phishing, *spyware*, términos y condiciones que acepta, etc.
Que no puedan adaptarse a cambios constantes en sistemas operativos.
Rastreo del usuario.
Riesgos de seguridad porque a través de ellas conozcan tus hábitos, lugares que frecuentas, etc.
Robo de identidad.
Robo de información.
Robo del equipo, sustitución de identidad.
Saturación, mala calidad, *fake reviews*, *clickbait.*
Sitios no seguros para descargar la aplicación.

Spam, robo de identidad, *bluejacking.*
Take over del dispositivo.
Uso de *apps* no autorizadas.
Venta de mis datos personales.
Vigilancia cibernética.
Virus, *malware.*

Anexo 8. Relación de sitios/*apps* percibidos como seguros o inseguros, que tuvieron sólo 1 mención

Sitios o *apps* considerados seguros o confiables (sólo con 1 mención)

(Listado en orden alfabético)

911 CD MX	Farmacias San Pablo	Safari
aa.com	Fintonic	SAT
ActiPass	Fiverr	Scotiabank
Albo	Gandhi	SeatGeek
Aliexpress	Google Drive	Sí Vale
American Express móvil	Google Play	Sitios bancarios
Banco Azteca	HBO Go	Sitios de viajes en general
Banco Azteca Móvil	Hotwire	Telcel
Best Day	HSBC	Telegram
Bonobos	Hulu	TELMEX
Cadenas de hoteles	Inbursa	Ticketmaster
Citipay	Inbursa móvil	Tiendas de autoservicio en línea
Claro video	Ingredienta	Travelocity
Claroshop	Kichinck	Tripcase
Commscope	Macy's	Twitter
Cualquiera con certificación SAFe Agilist	MexJet	Undostres
CyberPuerta	Microsoft	United
DELL	Microsoft Store	WeBank
Dolce Gusto Nescafé	Ninguno sin mecanismos apropiados de protección	Xbox
enviaflores.com	Orbitz	Yahoo
ETN	Periódicos	YouTube Red
E-Trade	PSN	Zappos
F1TV.com	Reforma	

Sitios o *apps* considerados inseguros o no confiables (sólo con 1 mención)

(Listado en orden alfabético)

Agua	Estado de México	NILPIX.COM
AirB&B	Farmacia San Pablo	OfficeDepot
Algunos de renta de autos	Farmacias del Ahorro	Open Table
American Express	FIT PASS	Osom
Aplicaciones de apuestas	FourSquare	Paguito.com

Aplicaciones de Telmex	Gmail	Playstation Store
Apss de descarga libre	Go Daddy	Santander
AT&T aplicación móvil	Gobierno Federal	SAT
Avianca	Google maps	Scotiabank
Bancarias en general	Grupo ADO	Sears
BitTorrent	Grupon	Secretaría de Finanzas de la Ciudad de México
Casi cualquier página de compras en línea	Hangouts	Segundamano
Chedraui	HBO Go	Sheet music plus
Cinemex	HSBC	Shein
Club Factory	HSBC móvil	Smaller *retailers* in general
Compras en Facebook	IBM	Tu Loerto
Coppel	La Europea	Tu tag pase
Cryptomonedas	La mayoría del AppStore	Twitter
Cualquier página chafita que vea, aunque tenga productos padres	Librerías Gandhi	Volaris
DHgate.com	Linio	WeChat
Divas.com	*Link*edIn	Wish
El hartista	Marriot	Yahoo
Equifax	Marti	youtube

Anexo 9. Relación de *software* o recursos de apoyo que ayudan a incrementar la seguridad, que tuvieron sólo 1 mención

(Listado en orden alfabético)

Akamai	Firefox	Preguntas de seguridad
Antiadware	Firma Electrónica	Prestashop
Antimalware	FreeScan	Protonmail
Anti*Spam*	Guardium	Qradar
Apple	IBM Trusteer	Security 360
Apps de mensajes encriptados	IDS	Signal
AVG	IEEE	Sistema Operativo Linux
Avira	IPS	Sniffers
Aviso si alguien está entrando a tu cuenta	Keepass	Sonicwall
AWS	Lawpay	*Spam*ina
Banamex-Wallet	*Links*canner	Splunk
Bancanet	Listas Negras	Suite GenSecure
BBVA móvil	LowRhyth	Thread Hunting
BBVA-Wallet	Magento	Tipalti
Bitcoin	Malwarebytes	Traps
Bitwarden	Master Card secure	Trustwave
Browsers en modo incógnito	Metasploit	Validacion via sms
Códigos de autenticidad	Mobile secure	Veritas
Comunicaciones seguras	Netcat	Vlans
Confide	Network Mapper	Watson for Cybersecurity
Desarrollo seguro -> Control de sesiones	Pagomobil	WhatsApp y FaceTime
Digicert	Palo Alto	Windows Defender
DuckDuckGo	Password managers	Wireshark
DUO	PayU	Woopra
e-card	PGP	YubiKey
Endpoint Security Clients	Políticas de privacidad	Zoom
Eset		

Anexo 10. Acciones concretas aplicadas que fueron compartidas por los entrevistados

(Listado en orden alfabético)

Archivo de correos, respaldo en la nube, instalación de suites de antivirus con detección de *ransomware* y *firewall* corporativo.
Auditorías de seguridad digital. Capacitación a los empleados en seguridad digital.
Back up en la nube.
Bloqueo de correos electrónicos en los celulares. Filtro de correos a terceros. Bloqueo de páginas de Internet no seguras.
BYOD.
Capacitación.
Capacitación, certificación, estructura organizacional, presupuesto.
Certificación ISO.
Certificación PCI.
Ciberseguridad en 5G.
Comunicación encriptada.
Con la alta inseguridad que vivimos en CDMX, procurar no sacar computadoras / laptops de la oficina. Nunca usarlas en público, salvo casos indispensables. Tabletas más fácilmente se esconden, ésas sí las sacamos a citas. Y poner más difícil contraseñas de acceso en celulares, más dígitos.
Control de acceso a Internet y puertos de acceso en las computadoras personales, sistemas de identificación de ataques cibernéticos, bloqueo de URLs inseguras.
Creación de comité de seguridad.
Crear diferentes niveles de acceso y permisos.
Cuidado de la información y redes internas. *Firewall*.
Debido al tamaño de nuestra empresa, al sector al que nos dedicamos y al tipo de información que manejamos, no consideramos estar en riesgo de un ataque cibernético, por lo que no tenemos medidas especiales o adicionales a las comunes y corrientes. Nuestro riesgo más importante es el de un robo físico de los equipos y ahí perder la información almacenada.
Doble autenticación, huella dactilar, retina.
Doble autentificación.
En evaluación de proveedores.
Encriptación del *email*, control de accesos con mayor nivel de seguridad, identificación digital de los usuarios.
Establecer políticas de seguridad entre los empleados. Recomendaciones de *passwords* seguros, cambio periódico de *passwords*, uso de VPN, respaldo de información, reglas de acceso por usuario.
Estamos evaluando mecanismos proactivos para la identificación/prevención de riesgos que viajen a través de la red mediante la utilización de inteligencia artificial y *machine learning*.
Estamos siendo asesorados por una empresa experta para tener un diagnóstico de la vulnerabilidad de nuestra información.
Estar seguros de que todas las estaciones de trabajo cuentan con sus sistemas antivirus actualizados. Respaldar en servidores propios de la empresa la información y código de aplicaciones estratégicas. Tener acceso vía móviles a la información de las estaciones de trabajo mediante los respaldos que hacemos *in house*.

Evitar el uso de servicios de nube.
Fundamentalmente, los archivos se respaldan de forma redundante y se cuida el acceso a ellos a usuarios autorizados, no tenemos información "altamente sensible" en la red.
Hacer énfasis entre los colaboradores en la implementación y uso de los procedimientos de seguridad TI.
Implementación de *software* que impida las descargas no autorizadas. Reforzamiento y actualización continua del *firewall* y *software* antivirus. Nada especial o fuera de lo común.
Implementar soluciones de seguridad en la nube.
Incorporando encriptación de datos, "tokenizando" las transacciones.
La seguridad está en el centro de todos nuestros servicios con el cliente, incluyendo controles administrativos, físicos y técnicos.
Los sistemas de seguridad de la compañía son propietarios, pero les puedo decir que incluyen elementos mucho más sofisticados que la mera encriptación.
Manejo de discos espejo, varios respaldos físicos y en la nube, *software* para protección.
Mantener capas no entrelazadas de seguridad en cuanto a la información abierta al público, comunicaciones internas y procesos administrativos.
Migración de información sensible a AWS como parte de un nuevo DRP/BCP.
Migramos la información a servidores externos de Google.
MIT mantiene los últimos estándares de seguridad de datos debido a la confidencialidad de la investigación realizada con los socios estratégicos de la organización, que van desde industrias militares, médicas, aeroespaciales, biotecnológicas y de *software*, entre otras.
Monitoreo constante, actualizaciones al día, equipos y sistemas de seguridad de última generación.
No hacemos nada, nosotros sólo confiamos en que las grandes empresas lo están haciendo.
Nube privada, segregación de funciones, controles de seguridad, seguridad multicapas.
Nuestra institución utiliza redes privadas virtuales (VPN), aplicaciones con estándares de seguridad aceptables en el mercado y sistemas de monitoreo para la detección de intromisiones o ataques.
Optimizar los procesos de consultoría.
Para el archivo muerto: usamos OneDrive, pero ciframos contenedores 7Zip con la información histórica con llaves de 32 bytes (2^5 bits). Para el día a día, empleamos listas de control de acceso, auditoría, control de versiones y no se pueden borrar.
Políticas, procesos, capacitaciones al personal, revisión, antivirus, otros.
Políticas, seguridad con *hardware*, seguridad con *software*, capacitación.
Por la naturaleza de nuestra empresa, se cuenta con un área específica de Seguridad de la Información en el grupo de IT. Adicional, los grupos de ingeniería, al utilizar servicios en nubes públicas, también tienen políticas al respecto (por área).
Protocolos de administración especializada de seguridad de la información. *Coding* de conducta de empleados, monitoreo constante, herramientas de seguridad cibernética.
Reducir el número de espacios en la nube donde se guarda información; por ejemplo, Dropbox, iCloud, o Onedrive, y tener sólo uno.
Reforzando los servidores con respaldos en automático en forma física.
Respaldo físico de la información en disco duro externo.
Robustecer las políticas en WAN y personalizarlas por función. Obtener más provecho de la seguridad actual de Windows Server.
Se está revisando antivirus en la nube y un analítico de *malware*.
Se están implementando tecnologías de nube para resguardo y disponibilidad de información.
Seguridad y nube es uno de los pilares estratégicos de Cisco.
SOC *as a Service*, correlacionador, pruebas de penetración.

Somos una empresa que presta servicios de seguridad en nubes y redes, por lo que ofrecemos a clientes una variedad de servicios para prevención de eventos. Y nosotros los usamos internamente.
Temas normales como candados, *passwords*, claves, huellas digitales.
Tenemos contratado un servidor dedicado de almacenaje en la nube.
Tenemos un servidor seguro con algunos servicios en *outsourcing* tales como correos (Microsoft) y el sitio web, además nos certificamos con PCI.
Tener discos espejo en servidores Linux, en dos nodos diferentes.
Tienen un marco (políticas) muy bien definidas, establecidas y se hacen las auditorías internas más exigentes que las externas.
Toda la info en G-Suite. Acceso vía 2FA.
Tratamos de resguardar la información más importante en un disco externo.
Usamos Telegram y Signal para comunicaciones estratégicas.
Usando plataformas y aplicaciones de uso interno que sólo permiten la conexión en oficinas.
Utilizamos Dropbox for Business para almacenamiento de archivos. Anteriormente, utilizábamos Google Drive, pero la experiencia de usuario en Dropbox es superior.
Utilizamos herramientas para escanear vulnerabilidades en nuestro sitio y vamos a adquirir certificados SSL para la página de ventas *online*.
Utilizar herramientas que manejan certificados de seguridad confiables.
Utilizar únicamente los canales más confiables autorizados por la empresa y firmar NDA's (*Non Disclosure Agreements*).

Anexo 11. Razones más relevantes de por qué se considera que México se encuentra mejor, igual o peor que otros países.

(Listados en orden alfabético)

Opiniones de por qué México es percibido mucho mejor

Existen notables avances de tecnología y disponibilidad.

Por la banca. Los bancos en México marcan la demanda y van a la cabeza siempre en estos temas.

Porque tenemos excelentes ingenieros de sistemas, gente que está al más alto nivel en temas de informática, sistemas de información y seguridad.

Opiniones de por qué México es percibido mejor

Es relativo, dependiendo con que países nos comparamos, pero hay buena penetración de Internet en México.

Hay mucha conciencia. Al ser un país donde el robo es cotidiano, creo que las empresas tienen muy claro que tarde o temprano les van a pegar *online*.

Hay campañas dentro y desde instituciones, así como por la comunidad a través de plataformas sociales.

Hay países en África, Asia y Latinoamérica que están mucho peor que México en cuestiones de seguridad informática.

Hemos crecido y adoptado mejores prácticas de otros países que ya han aprendido de las fallas.

Porque se ha visto que las empresas empiezan a tomar el tema de seguridad informática como relevante, de acuerdo con crecimiento del canal digital de ventas.

Por la globalización y por lo tanto se encuentra bajo regulaciones internacionales.

Opiniones de por qué México es percibido igual

Acceso a los mejores tipos de *software* a costo accesible.

Acceso a tecnología, capacidad de inversión. Si bien es el país con más fraudes en línea del mundo (creo), las empresas con *e-commerce* y banca en línea se protegen mucho. No deja de ser un problema.

Considero que el tema de seguridad informática es manejado por empresas trasnacionales, lo que iguala la circunstancias con otros países.

Creo hay avances, aunque todavía falta mucho conocimiento del tema y más uso de tecnología.

Creo que estamos igual que la mayoría de los países, aunque estoy seguro de que algunas naciones europeas están mucho mejor y algunos países del Medio Oriente o Asia están mucho peor.

Desafortunadamente, el crimen informático se ha desarrollado enormemente en todo el mundo, ya no es necesario estar a un costado de algo o de alguien para delinquir, basta con tener acceso a una red y estar capacitado para derribar *firewalls*, obtener claves etc.
Estamos apegándonos a lineamientos de seguridad internacionales.
Hay acceso a todo tipo de tecnología en México.
Hay organizaciones muy maduras (generalmente multinacionales), pero la mayoría de las empresas (PYMES) no tienen recursos para invertir en seguridad informática.
Hay tecnología y tenemos acceso a plataformas globales.
He escuchado más de este tipo de problemas en otros países/empresas.
La seguridad está globalizada, sólo es aplicarla.
Las empresas han implementado herramientas y procedimientos actuales para hacer frente a los temas de seguridad en TI.
Las herramientas que he mencionado son de uso global, no percibo un riesgo distinto entre México y Estados Unidos, por ejemplo, en tal caso.
Los casos de vulnerabilidad detectados en México se comparan con los que han ocurrido en otros países. Por ejemplo, Banorte vs Equifax.
Los problemas de seguridad que tiene un país como el nuestro son los mismos que sufren los países más desarrollados. Quizá el problema está en la preparación para este tipo de conflictos, que es menor con respecto a otros países.
Los riesgos informáticos son globales.
Mismos retos, mismo nivel de entendimiento de los riesgos que observo en otros países.
Mucha inversión en equipamiento de seguridad y poco análisis de riesgos que soporten las inversiones.
No creo que destaquemos, pero tampoco creo que estemos mal.
No creo que estén completamente seguros en ningún país.
No es un blanco importante, el índice de ataques a gran escala es mínimo y ha sido tan vulnerable en los últimos ataques de *ransomware* como otros países o, incluso, con menos daño reportado.
No existe una cultura de salvaguarda de la información y muchas personas no lo toman con la seriedad que merece.
No existe una madurez general con respecto a la importancia en la seguridad informática y de ahí que hayan proliferado tanto los fraudes cibernéticos, intentos de extorsión, llamadas no autorizadas de *telemarketing*, etc.
No he visto que México se distinga particularmente en la rama.
Nuevamente, es importante saber contra quién nos comparamos, pero a mi parecer México se encuentra en niveles aceptables de seguridad digital.
Por comparación con filiales en otros países (de Latam).
Por las herramientas que se usan; son prácticamente las mismas.
Por los estándares mundiales en el cifrado de datos.
Porque estamos generando tecnología similar para la conectividad y el desarrollo de las empresa públicas y privadas.
Por un lado se oye de eventos de pérdida o acceso a información de personas no autorizadas o hackeo, pero tampoco se escucha muy frecuente.
Porque estamos en un país con un alto grado de delincuencia cibernética, por lo que los usuarios nos protegemos y desconfiamos más.
Porque este tipo de tecnología no tiene fronteras.
Porque sigue habiendo falta de cultura en general.
Porque tenemos acceso a las mismas herramientas que otros países.

Promedio. Menor que países desarrollados y mejor que el resto.
Se han dado casos de hackeo de similar manera como en otros países.
Somos un país que está a la vanguardia informática.
Tenemos las mismas posibilidades de riesgo.
Tenemos los mismos problemas que otros países, pero México no es objetivo primordial por el momento.
Todavía no hay adopción de nuevas tecnologías como reconocimiento facial, doble o hasta triple verificación.
Ya que es constante ver casos en donde se han suscitado eventos que afectan la fuga de información o vulnerabilidad de la infraestructura, sobre todo en el ámbito bancario.

Opiniones de por qué México es percibido Peor

Aún se presta poca atención al tema. Aunque me parece que ha mejorado en años recientes, las empresas todavía no consideran la seguridad como una inversión sino como un gasto.
Aunque ha avanzado mucho, aún hay servicios atrasados en este tema y usuarios poco culturizados, así como retraso en materia legal/regulatoria.
Bajo nivel de conciencia a nivel de personas y empresas. Si no hay compromiso regulatorio, generalmente, existe una postura laxa o reactiva.
Bajos niveles de educación, poco avance del país tecnológicamente.
Con la excepción de empresas transnacionales con presencia en México, en general, percibo un importante rezago tecnológico.
Creo que la mayoría de las empresas no toman el tema con suficiente seriedad.
Dependemos de mucha tecnología de USA y no es la más confiable. Las redes de proveedores están infestadas de virus y *spam*.
En casi todo lo de tecnología vamos unos 3 a 10 años atrasados contra EUA, Europa, Japón, etc.
En la cultura mexicana los usuarios no tienen conciencia del daño que pueden causar por malas prácticas de seguridad en informática y los tomadores de decisión prefieren correr riesgos altos por los costos de implementar un buen sistema.
En muchas industrias no hay aún una conciencia del impacto, poca inversión en seguridad informática, visión de corto plazo.
En términos generales, las compañías procuran la seguridad en el manejo de la información, aunque no todas, y los usuarios aún tienen mucho que aprender.
Estadísticamente, México está por arriba en ataques e infecciones concretadas.
Existe mucha clonación de tarjetas de crédito.
Falta de atención, inversión, conocimiento.
Falta de conocimiento.
Falta infraestructura.
Falta saber más de opciones para tener estrategia adecuada para PYMES y profesionistas independientes, sin vulnerar su seguridad personal.
Falta de talento y presupuestos.
Fundamentalmente, porque no hay regulaciones claras en este sentido, es conocido el uso que se dio recientemente de *software* espía en teléfonos de activistas, luchadores sociales y periodistas, así como el uso de bots para crear tendencias de información política.

Hay tantos otros problemas de seguridad que no creo que éste sea el enfoque principal.
La falta de una legislación que se aplique correctamente, la falta de interés de las autoridades por regular eficientemente el tema.
La inversión en general en este reglón es muy baja.
Las empresas normalmente se preocupan por temas de seguridad una vez que tienen un problema, no hay una cultura de acciones proactiva al respecto.
Los altos índices de asaltos y secuestros se han ido incrementado.
Mala legislación, corrupción, falta de investigación y castigo.
No existe investigación y desarrollo. Si bien el IFAI ha impuesto medidas importantes, la regulación aún es laxa y la fiscalización insuficiente.
No hay coordinación del gobierno con las empresas, hay impunidad, no hay conocimientos.
No tenemos buenos hábitos de seguridad informática y la delincuencia va más rápido que nuestra capacidad de contenerla.
Nuestra tecnología y normatividad no están al nivel de los países más avanzados.
Por el nivel de impunidad.
Por falta de conciencia en la seguridad. Y falta de implementación generalizada de protocolos de seguridad.
Por la falta de cultura y los precios de sistemas de seguridad.
Por la falta de legislaciones y regulaciones.
Por la falta de madurez de los procesos organizacionales, mayormente impulsados por regulaciones y requerimientos de negocio en lugar de ser promovidos por la propia empresa.
Porque es un tema que para las empresas no ha sido prioridad en sus operaciones.
Porque forma parte del crimen organizado que es muy grande en México.
Porque recurrentemente veo que el tema no es prioritario para las organizaciones o no es entendido a profundidad. Se asume que por adquirir una tecnología en particular el problema está resuelto, cuando la seguridad en informática no es sólo un tema tecnológico, sino de cultura organizacional.
Porque conozco del tema y sé tanto lo que hay en México como lo que hay en otros países desarrollados.
Porque hay países como USA que invierten mucho más capital en seguridad.
Porque hemos visto filtraciones de información en la prensa, y el gobierno ha espiado a periodistas.
Porque se abusa del usuario, se le requieren protocolos excesivos por la paranoia de los informáticos.
Recientes noticias respecto de bandas de hackers que robaron millones de pesos durante años.
Rezago vs países avanzados.
Si lo comparamos con países del primer mundo pensaría que peor, si lo comparamos con países del 3er mundo quizá estemos igual.
Sin tener cifras precisas, es muy importante lo que sucede con el robo de bancos a través de cuentas o tarjetas de crédito.
Todavía no hay conciencia y no se dedican los recursos necesarios para mitigar este tema.
Xq aquí no se castiga.

Opiniones de por qué México es percibido mucho peor

#GobiernoEspía
El personal de seguridad que realmente sabe es muy escaso. Los demás son charlatanes.
Hay muy poca educación en seguridad de información.
La policía cibernética está en pañales y las amenazas y ataques ocurren a diario en todos los niveles.
Peor si hacemos comparaciones directas con USA.
Se observa en las estadísticas publicadas por diversas fuentes del ramo.
No considero que haya cultura para inversión en este ramo. Solo en ciertos sectores.

Anexo 12. Lista de los retos más relevantes de México, tal como fueron mencionados por los entrevistados

(Listado en orden alfabético)

1. Cultura 2. Comunicación 3. Conciencia 4. Responsabilidad compartida.
Al seguir creciendo las empresas mexicanas, deben adoptar los sistemas de seguridad más avanzados y esto representa una inversión fuerte, pero en nuestra cultura a veces pensamos que es sólo un gasto y optamos por opciones más económicas pero menos garantizadas para el futuro.
Alcanzar el nivel de seguridad de otros países.
Ataques internos, a servicios de infraestructura, así como *ransomware*.
Aterrizar plataformas globales en México, regulación anticuada y tardía.
Buenos y confiables proveedores de servicios, mejorar el conocimientos tecnológicos con alta capacitación al público en general, "cursos" apoyándose en empresas que ya están desarrollando esto.
Capacitación.
Capacitación y cultura.
Certeza jurídica.
Clonación de tarjetas de crédito y robo de identidad.
Combatir a los *hackers* cibernéticos y sus constantes nuevos virus.
Combatir al crimen organizado, más respeto a la privacidad y protección de datos personales. Especialmente, se permite a los grupos financieros cometer abusos en el uso de la información.
Combatir las vulnerabilidades, contar con más inversión, conciencia, mano de obra, etc.
Conciencia, regulación, inversión en nuevas tecnologías.
Conciencia sobre los riesgos que representa no estar debidamente protegido.
Confiabilidad en resguardo de datos personales.
Conocimiento de los riesgos y soluciones móviles en nube pública, a precios alcanzables.
Conocimiento y recursos.
Conocimiento, presupuesto, regulación, procuración de justicia.
Conocimiento y que estamos en manos de proveedores extranjeros.
Creación de infraestructura adecuada y formación de recursos.
Crear comunidades de expertos, implementar estándares tecnológicos como ISO 27000, ITIL, capacitación, pero sobre todo legislación que comprometa y sancione el uso inapropiado de la información digital.
Credibilidad en los servicios de seguridad, habiendo en general una cultura de desconfianza.
Creo que es el mismo reto que los demás países, ya que estos temas son globales.
Creo que es un tema de educación, cultura y de recursos. El futuro está en la habilidad de mover datos y eso se tiene que hacer con mucha eficiencia.
Cuidar la integridad personal de las personas, evitando ciberespionaje y acoso.
Cultura de seguridad, inversión por parte de las empresas.
Cultura informática.
Cultura, educación, leyes y persecución de delitos.
Cultura, mucho de los fraudes se realizan con ingeniería social, las personas fácilmente entregan su información de acceso si creen que están hablando con alguien de su banco, por ejemplo.
Desarrollo de DRP.
Desconocimiento del tema, falta de inversión, así como una gran corrupción a nivel gubernamental y, en menor grado, en el empresarial.

Difusión de opciones diversas y confiables para PYMES, para profesionistas independientes; no sólo para multinacionales y grandes empresas. Educar al público más en la materia. Robustecer los sitios electrónicos del gobierno de México; actualizados y con un funcionamiento confiable.

Educación.

Educación, conocimiento, técnica.

Educación, infraestructura.

Educar a la población para que sepa identificar cuándo poder compartir su información y hacer leyes como la de protección de datos que ayuden a tener un entorno más seguro.

Educar a los usuarios en el tema para que se tomen las medidas y se sigan protocolos que mitiguen los riesgos. También concientizar a los directivos responsables de las decisiones de que las inversiones en seguridad informática (sin exagerar) son un buen activo para su empresa.

Educar a los usuarios para el correcto manejo de las plataformas digitales

Educar a los usuarios que siempre deben estar alertas de correos/invitaciones/ fraudulentos.

El apetito por comerciar con los datos que aportamos para adquirir cosas o servicios.

El aseguramiento de que los medios informáticos están dentro de una legislación; que realmente se pueda regular.

El desarrollo de una cultura digital. Se va adoptando por reacción, no por previsión.

El estancamiento del país.

El gobierno socialista de AMLO y sus adjudicaciones.

El no relajar los esfuerzos que al día de hoy se han implementado. No dudo que se encuentren en vías de hacer más; sin embargo, es necesario hacerlo más rápido, baste revisar el reciente caso que puso en jaque al mismo Banxico.

El primero, es concientizar a gobierno y empresas que el activo más valioso que se tiene es la información. Cuando eso suceda, probablemente México mejore en esta área.

El principal es la modernización de sistemas de seguridad que van desde escuelas, gobierno, PyMEs que son los ramos donde no hay control o simplemente no se conoce la necesidad de la seguridad en informática.

El proyecto del gobierno para alcanzar una mayor cobertura bancaria a través de la banca digital, presentará una mayor incidencia de fraudes, por lo que se requiere redoblar esfuerzos en seguridad.

El robo de datos, ya sea para fines delincuenciales o fraude.

En el movimiento a la nube, entender retos asociados e implementar las buenas políticas y procesos.

Entender y alcanzar los estándares globales, al mismo tiempo que se incrementa la capacidad de sus plataformas tecnológicas y aumenta el uso masivo de estas herramientas por parte de la población en general.

Entendimiento, apertura, accesibilidad.

Estado de derecho.

Estrategia federal, cooperación internacional.

Evitar fraudes.

Evitar fraudes digitales, lo cual veo complicado.

Falta de cultura de protección. Falta de regulación o de aplicación de la normatividad.

Falta de Estado de Derecho. Penas y castigo.

Falta de innovación, falta de presupuesto, falta de Recursos Humanos.

Falta de legislación, falta de tecnología, falta de red en algunas zonas.

Falta de plan gubernamental.

Falta de políticas públicas y regulación.

Falta legislación.
Fortalecer las políticas públicas, adecuar la legislación, establecer alianzas entre instituciones públicas y empresas privadas, capacitar a los usuarios, policías, ministerios públicos y jueces, realizar campañas de concientización, compartición de información con otros países, apoyar e incrementar el desarrollo tecnológico.
Generar una cultura de seguridad informática en diferentes niveles.
Gobierno actual, bajo presupuesto, corrupción.
Hackers cachando porno.
Hay un rezago tecnológico importante, ni los equipos ni el *software* es de última generación en una parte importante de los usuarios.
Homologación con prácticas líderes a nivel mundial.
Incluir la estrategia de seguridad de la información como apoyo a los objetivos de negocio, ya que, en IMHO, la estrategia de seguridad es actualmente un gasto promovido por alguna necesidad o regulación en lugar de que ayude a impulsar el negocio.
Inclusión financiera y digital de más personas y empresas. Cultura informática y de seguridad. Gobierno retrógrada que no impulsa la transformación digital.
Infraestructura.
Infraestructura y personal altamente capacitado en la seguridad en informática.
Inseguridad por hackeo de información. Riesgo en las transferencias y pagos.
Inversión.
La cercanía con USA que permitiría a los ataques cibernéticos entrar por México para llegar a USA.
La concientización acerca de la importancia de invertir en seguridad de información.
La corrupción, falta de presupuesto en las empresas.
La Cuarta Transformación.
La cultura del usuario, regulación apropiada y adopción de tecnologías más seguras (aunque el precio tiene mucho que ver).
La cultura mexicana que, en general, no es previsiva y no planea a futuro sino que prefiere esperar a que haya un problema para resolverlo, es muy difícil de cambiar. Prepararse para los riesgos y prever posibles problemas de seguridad es la única manera de aumentar la seguridad informática. México no es un país que se preocupe demasiado por lo que pueda suceder.
La ética de la población.
La falta de cultura de la prevención.
La falta de profesionalismo de los empresarios y la total incompetencia del gobierno.
La ignorancia de los usuarios.
La intrusión de hackers en el sector financiero.
La penetración a todo nivel por la extensión del país y número de usuarios.
Las leyes gubernamentales se están fortaleciendo y por ende las empresas deben prepararse para su cumplimiento en la materia, a nivel fisco.
Las leyes y el gobierno... van años luz vs. lo que hay hoy en día.
Legislación en cuanto a seguridad informática.
Legislación y persecución en caso de delitos.
Legislación. Educación. Mayor oferta de servicios de seguridad informática que cumplan estándares internacionales.
Legislación/leyes.
Leyes que se apliquen. Seguimiento al ladrón.

Los costos y la falta de integración de los servicios de seguridad informática.
Los fraudes bancarios a los propios bancos como ya sucedió.
Los mismos que en todo el mundo.
Mantener la libertad y seguridad en el uso de Internet con acceso a toda la población, la regulación de las redes sin vulnerar las garantías de libertad fundamentales, esto implica políticas claras que además impulsen el desarrollo de estas herramientas y fortalezcan su uso en toda la sociedad.
Mayor comunicación desde el gobierno, cultura de seguridad desde las escuelas, promoción de seguridad desde las marcas. Ejecución de la justicia.
Mayor cultura de la seguridad en distintos ámbitos en el uso de cualquier dispositivo, la responsabilidad de ser custodios de información de los clientes y cómo accionar en caso de que suceda.
Mayor información para que los beneficios se conozcan mejor y se reafirme el convencimiento de invertir en este rubro.
Mejor entendimiento de las amenazas.
Mejor infraestructura de ciberseguridad y hacer conciencia en usuarios de la importancia de la protección de datos personales, metadatos, transacciones.
No estoy muy informado a nivel país; sin embargo, creo que en la medida que se avance acorde a los requerimientos comerciales y sociales, podremos empatar las necesidades que los mercados demandan en beneficio de todos.
No quisiera parecer repetitivo, pero el principal reto es concientizar a la gente del peligro que representa estar en línea y aprender a distinguir las amenazas.
No tener reglas o regulaciones vigentes.
Oferta de fuentes confiables. Difusión.
Personal capacitado en seguridad, marco legal moderno en temas de protección de la información, énfasis en el cumplimiento regulatorio por parte de autoridades.
Primero, se necesita mejorar la adopción y cuidado que desarrollos hechos en México cuentan con seguridad similar a las que ofrecen las compañías globales.
Que en muchas organizaciones está descuidada. Por ejemplo, los anuncios acerca de que las bases de datos del INE o de asegurados del ISSSTE, que tienen créditos hipotecarios, es fácil comprarlas en el mercado negro.
Que las empresas de todo tamaño vean la importancia del tema y que tomen interés por desarrollar programas, de acuerdo con su *core business* y capacidades que garanticen la seguridad de la información.
Que las instituciones privadas y públicas estén al día en temas de seguridad.
Que las personas tengan confianza de que su información está debidamente protegida.
Reconocimiento de la prioridad y relevancia de las inversiones para protegerse.
Requerimientos de alta inversión, corrupción, debilidad de las autoridades, oferta de expertos en ciberseguridad, falta de procesos, etc.
Reticencia de los usuarios. Mejoras legales/regulatorias.
Robo de información que alienta el crecimiento tecnológico.
Tener la capacidad de responder en forma y en tiempo a cualquier ataque o amenaza que intente vulnerar la seguridad.
Transformación cultural.
Una buena legislación y desarrollo tecnológico, así como el talento adecuado.
Una verdadera estrategia y política al respecto.