CIBERSEGURIDAD PARA LA SOBREVIVENCIA DE LAS MiPyMEs.

Ernesto Ibarra S.[4*]

Palabras Clave: Ciberseguridad, Seguridad de la Información, Ciberdelitos, Protección de Datos, MiPyMEs.

Resumen

El presente texto aborda la importancia de la ciberseguridad para las organizaciones, especialmente para las micro, pequeñas y medianas empresas (MiPyMEs). Haremos un repaso de los términos más importantes que nos permitirán comprender énfasis de los diversos riesgos, amenazas y vulnerabilidades, poniendo énfasis en los ciberdelitos, que pueden afectar la información de las organizaciones y su funcionamiento, las cuales en caso de concretarse pueden impactar en la reputación, economía, continuidad del negocio, valor de acciones y la imagen reputación de la marca.

Esta aportación pretende resaltar la importancia y urgencia de adoptar medidas de seguridad de la información como un proceso gradual y permanente que se vuelva un componente de la vida diaria de las empresas, más allá de cumplir con determinada ley por obligación o para evitar multas. Además, revisaremos someramente algunos ordenamientos jurídicos que refieren a la seguridad de la información aplicable a las MiPyMEs, como son: a) Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP); b) Ley Federal del Trabajo (LFT, en su

[4*]Jurista digital. Licenciado y maestro en Derecho por la UNAM. Doctorando en Derecho por la Universidad Panamericana (Campus Ciudad de México). Es presidente de la Academia Mexicana de Ciberseguridad y Derecho Digital A.C.; Vicepresidente de la Federación Iberoamericana de Asociaciones de Derecho e Informática FIADI A.C; es fundador de CyberLaw, consultoría en ciberseguridad y protección de datos personales; y también Coordinador de Ciberseguridad y Derecho Digital de la UDLAP Jenkins *Graduate School*. / @Eibarra_S @AMCID_Mx

apartado de Teletrabajo); c) Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech); y d) Ley Federal de Protección al Consumidor (LFPC).

Finalmente, se compartirán algunas consideraciones y recomendaciones para implementar en organización micro, pequeñas y medianas empresas para prevenir y mitigar el impacto de los riesgos cibernéticos, esperando contribuir a la supervivencia y sostenibilidad de las organizaciones en el entorno digital, y que ello permita que las micro y pequeñas empresas sigan creciendo y contribuyendo con el desarrollo del país.

1. Introducción

El valor de las Micro y pequeñas empresas en México es muy importante. "De 4.9 millones de establecimientos del sector privado y paraestatal registrados en los Censos Económicos 2019, el 99.8% pertenecen al conjunto de establecimientos micro, pequeños y medianos". En impacto en materia del aporte al empleo, tenemos que: las Micro (0 a 10 empleados) aportan un 37.8 %; las Pequeñas (11 a 50 empleados) aportan un 14.7%; las Medianas (51 a 250) aportan un 15.9%; y las Grandes un 31.6% de empleos a nivel nacional.[5]

El contexto actual de la sociedad en la era digital, de la Cuarta Revolución Industrial (Industria 4.0, caracterizada por una combinación de ambientes físico, natural y cibernético) ha representado una gran variedad de cambios en la dinámica de individuos y organizaciones públicas y privadas, en gran medida provocado por agentes tecnológicos, principalmente la Internet y el poder de cómputo o *cloud computing*[6] y tecnologías emergentes como Internet de las cosas e inteligencia artificial, *Big Data*, entre otras.

---

[5] INEGI. CENSO Económico. (2019). CENSO Económico 2019. Retrieved from INEGI: https://www.inegi.org.mx/contenidos/programas/ce/2019/doc/pro_ce2019.pdf

[6] Téllez Valdés, J. (2013). Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México. Ciudad de México, México: Instituto de Investigaciones Jurídicas de la UNAM. Retrieved mayo 2021, from http://ru.juridicas.unam.mx/xmlui/handle/123456789/12154 "Se usa el término "en la nube" para hacer alusión al dinamismo, la flexibilidad y la escalabilidad de los recursos compartidos de trabajo sobre la información y sus beneficios. El cómputo en la nube se asocia a *Internet*, que puede tomar formas diferentes como las propias nubes. Es así como se utiliza la metáfora de *Internet* como "nube". El cómputo en la nube es un modelo que permite el acceso ubicuo, conve- niente y bajo demanda de red a un conjunto de recursos informáticos con- figurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo en la nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicios y cuatro modelos de implementación." (p. 3 y 4). Para conocer más del término, sus generalidades y aspectos jurídicos véase: *Lex Cloud Computing*. Estudio jurídico del cómputo en

Hoy contamos con gran capacidad de generación de información y datos, así como alta velocidad para transferir y procesar grandes volúmenes de datos, así como de almacenamiento, sea en dispositivos portátiles o en servicios de cómputo en la nube. Lo anterior, aunado al incremento en el número de usuarios de Internet y mayor número de dispositivos móviles.

Antes de la pandemia ya se tenía claro por parte de empresas y organismos internacionales el valor de las TIC en la mejora de procesos e incluso la sobrevivencia de un negocio. Al respecto, coincido con la idea de Henriquez, al referir que:

> La digitalización, que antes parecía un "extra" para aumentar la productividad y las ganancias, hoy se ha vuelto un requisito para que las empresas sobrevivan. En particular, las MiPyMEs que comienzan a transitar por la ruta de la transformación digital necesitan dotarse muy rápidamente de una serie de elementos. Por un lado, necesitan conexiones de calidad y dispositivos tecnológicos (computadoras y servidores). Por otro, requieren soluciones digitales, incluyendo sistemas informáticos para ventas, *marketing* y gestión de clientes adaptados a sus necesidades específicas, **soluciones reforzadas de ciberseguridad,** y herramientas para potenciar sus oportunidades de negocio (plataforma de comercio electrónico, medios de pago digitales, etc.)[7]

Énfasis añadido.

La pandemia por COVID-19 ha sido uno de los agentes que ha propiciado el incremento en la digitalización de muchas Micro, Pequeñas y Medianas empresas, en diferente ritmo, pero, con similares retos y circunstancias (económicos, sanitarios, falta de habilidades digitales, entre otros). Muchos han visto el reto de la pandemia como una oportunidad para aumentar el uso de las TIC, la capacitación en habilidades digitales, el ambiente laboral y dinámica de trabajo, así como el incremento de mercado con la posibilidad de ampliar el ámbito de impacto gracias a Internet y la economía de escala.

---

la nube en México, México, Editorial Instituto de Investigaciones Jurídicas de la UNAM, 2013. Disponible en: http://ru.juridicas.unam.mx/xmlui/handle/123456789/12154 , consultada en mayo 2021.

[7] Henriquez, P. (2020, abril 29). COVID-19: ¿Una oportunidad para la transformación digital de las pymes? Retrieved mayo 2021, from https://blogs.iadb.org/innovacion/es/covid-19-oportunidad-transformacion-digital-pymes/ Señala que "Los gobiernos pueden ayudar a que, de forma ágil y rápida, una masa crítica de empresas pueda dotarse de capacidades digitales para continuar operando ininterrumpidamente en el contexto de las restricciones de esta pandemia y para maximizar oportunidades de crecimiento en la poscrisis. Para masificar y optimizar sus intervenciones y recursos, los gobiernos deben apoyarse en herramientas digitales que ya existen. Este tipo de programas se vienen impulsando con fuerza en los países desarrollados en el marco de agendas digitales integrales". Y como casos concretos de programas de apoyo en la materia, sugiere las siguientes acciones por parte del gobiernos: "a) Divulgación, b) Autodiagnóstico digital, c) Asistencia técnica y financiera, d) Centros tecnológicos, e) Becas para entrenamiento, f) Desarrollo de proveedores y g) Digitalización de sectores". Véase (Henriquez, 2020).

Gran número de organizaciones (públicas y privadas, pequeñas o grandes, de cualquier sector de la economía) usan tecnologías digitales (computadoras, dispositivos móviles, Internet, redes sociales, aplicativos o plataformas) e información para diferente actividades cotidianas de una empresa (obtención, almacenamiento, procesamiento, uso, transferencia de información o cualquier otro tratamiento de datos) vinculada a procesos como: contabilidad, recursos humanos, ventas, inventarios, clientes, usuarios de nuestro sitio *web*, publicidad, contratos, incluyendo la información y tecnología de directivos, empleados y visitantes. Es decir, todos los activos, procesos, personas están vinculados a sistemas de información, tecnologías y datos. Esos activos de información son cada vez más valiosos para organizaciones y de su protección y correcto funcionamiento depende la continuidad y sobrevivencia de su negocio.

En el marco de la pandemia por COVID-19 se ha incrementado el uso de Internet y otras tecnologías digitales por parte de las empresas. La digitalización ha sido, para muchas empresas y profesionales, un elemento fundamental para sortear los efectos económicos provocados por la pandemia, no obstante, para muchos parece un proceso complejo y poco asequible.

Para acercarnos a dimensionar el contexto digital en México podemos referir que, de acuerdo con la Encuesta Nacional de Usuarios de Tecnologías de la Información en los Hogares[8], México contaba, a finales de 2019, con: "**80.**6 millones de usuarios de Internet y **86.5** millones de usuarios de teléfonos celulares", así como con "el 76.6% de la población urbana es usuaria de Internet. En la zona rural la población usuaria se ubica en 47.7 por ciento". Estas cifras resultan relevantes para dimensionar parte del ecosistema de la actividad comercial o economía digital, refleja el potencial de mercado al que se le puede llegar vía tecnologías digital y el tipo de canal de comunicación, e incluso datos demográficos de los usuarios de Internet, que a su vez puede ser consumidores o clientes potenciales.

De acuerdo con la AMVO, en México "el comercio electrónico generó en 2020 un total de **$316 mil millones** de pesos. Lo que representa un 9% del total canal de menudeo en México"[9]. El mismo estudio refiere que los sectores con mayor crecimiento son: a) Tecnología, b) Comida a domicilio, c) Supermercado, d) medicamentos y e) medios y entretenimiento. De igual forma, señala que, entre los factores de desconfianza, los consumidores refirieron que aún no compran en canales digitales por el miedo a ser víctimas de fraudes y la desconfianza a entregar datos bancarios en las

[8] INEGI-IFT-SCT. (2021, febrero 17). Comunicado de Prensa número 103. Retrieved 05 2021, from ENDUTIH: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf
[9] AMVO. (2021). Estudio de Ventas On line. Estudio, Asociación Mexicana de Ventas on line, México.

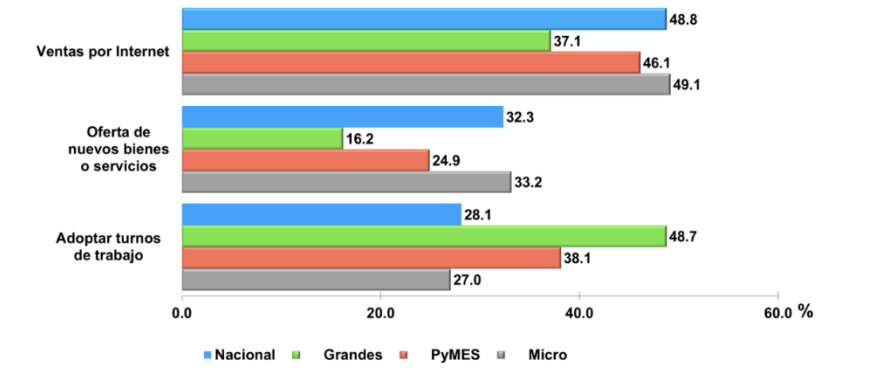
compras. A ello, en el referido estudio señala que: a) 80 % no quiere arriesgarse a un fraude electrónico, b) el 74 % no tiene confianza de dar datos bancarios, entre otros.[10]

En ese contexto, se ha detonado el comercio digital o los negocios digitales, teniendo como principales canales digitales las redes sociales, como *Facebook, Instagram y WhatsApp*, mismas que se encuentran entre las redes sociales más populares en México. Y el uso de los sitios web y páginas de Internet, en segundo término. De igual forma se puede observar la tendencia a la movilidad, destacando el uso de dispositivos móviles como *smartphones*, laptops y tabletas, dispositivos más usados por el internauta mexicano. [11]

Entre las medidas que se han adoptado en México para sortear la pandemia tenemos que: "La principal medida operativa que las empresas planean adoptar de forma permanente son las **ventas por Internet**, de las cuales, 49.1% son microempresas, 46.1% son PyMES y 37.1% son empresas grandes", tal como lo muestra la siguiente gráfica:

Adopción permanente de medidas operativas por tamaño

Gráfica 12a



Fuente: INEGI-ECOVID-IE, 2020.[12]

Otra de las circunstancias que se han presentado por la pandemia y el cumplimiento de las medidas sanitarias, es la compra por teléfono o plataformas, la entrega a domicilio, con lo cual se incrementó el uso de plataformas de entrega como: *Rappi, UberEats, Didi,* entre otras. El comercio electrónico, desde la oferta, compra-venta o prestación de bienes y servicios por Internet, el trabajo

[10] *Idem*

[11] INEGI-IFT-SCT. (2021, febrero 17). Comunicado de Prensa número 103. Retrieved 05 2021, from ENDUTIH: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf

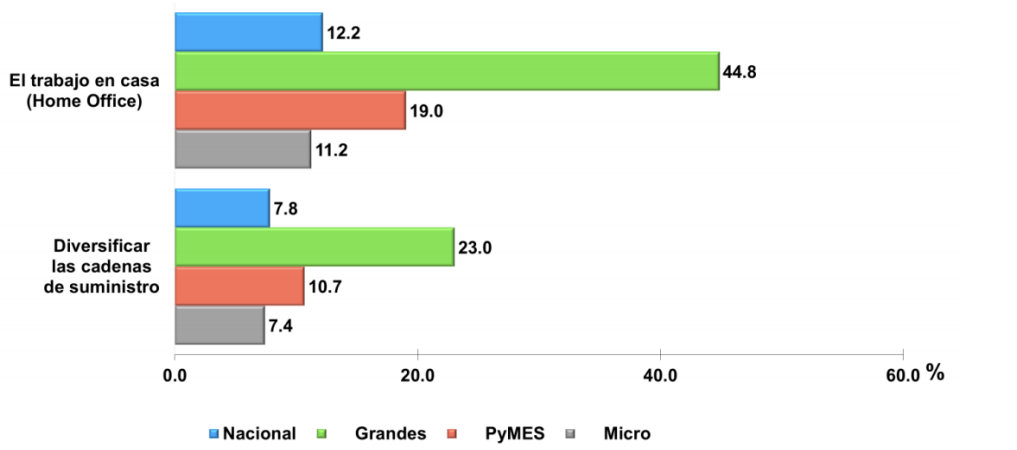
[12] INEGI-ECOVID-IE. (2020, diciembre). ECOVID-IE Y DEL ESTUDIO SOBRE LA DEMOGRAFÍA DE LOS NEGOCIOS 2020. Retrieved mayo 2021, from Comunicado de Prensa Num. 617/20: https://inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ECOVID-IE_DEMOGNEG.pdf

desde casa o teletrabajo (o *home office*) y o la entrega de bienes a domicilio, ha tenido un incremento en la mayoría de los sectores, entre los que destaca el sector de alimentos y tecnología.

En la misma Encuesta, "el trabajo en casa es una medida que las empresas probablemente adopten de forma permanente, aunque existe gran contraste al analizar por tamaño de empresa, ya que 11.2% son microempresas, 19.0% son PyMES y 44.8% son empresas grandes", así se puede observar en la siguiente gráfica:

Adopción permanente de medidas operativas por tamaño

Gráfica 12b



Fuente: INEGI-ECOVID-IE, 2020.[13]

Todos los sectores de la economía están aumentando el uso de TIC, especialmente de dispositivos conectados a Internet, y llevando la actividad de la oficina o centro de trabajo al entorno doméstico, sin que, en muchos casos, se incluyan medidas de capacitación en uso adecuado de TIC y Ciberseguridad.

Dicha circunstancia representa un factor que incrementa el riesgo para las organizaciones, debido al uso de dispositivos personales (reto aún mayor al llamado *bring your own device*), entornos domésticos, redes de Internet domésticas y medidas de seguridad, tecnología y otros factores que la empresa no logra controlar desde su administración central o no con los recursos humanos y tecnológicos habituales. Lo anterior significa que se amplían el espectro y elementos de protección, aumentando la vulnerabilidad y los riesgos de ser víctima de un ataque informático o sufrir un incidente de seguridad de la información, debido a que las medidas domésticas suelen ser

[13] *Ídem.*

nulas o deficientes para la adecuada protección de la información y los activos de información de una organización.

Por su parte, Microsoft señala que "más de 8 de cada 10 PyMEs mexicanas realizaron un cambio en su negocio ante el impacto de la crisis sanitaria y que, dentro de estos cambios, la adopción de tecnología ha tenido un papel central", agregando que: "el 41% de las PyMEs mexicanas encuestadas considera que la adopción de nuevas tecnologías se aceleró con la pandemia de COVID-19. Por otro lado, **el 83% de las** PyMEs considera que la adopción de nuevas tecnologías es importante para la reactivación de su empresa en el corto y mediano plazo". De este mismo estudio, resulta relevante -para nuestro propósito- mostrar la variedad de cambios tecnológicos:

> Dentro de los cambios tecnológicos que las PyMEs han implementado ante la pandemia destacan el **trabajo remoto** (49%), especialmente para las pequeñas y medianas, seguido de la reinvención del objetivo de negocio (42%), la **adopción de tecnologías** (28%) y las estrategias de ***marketing* digital** (26%). Para las micro, el aspecto más relevante fue la reinvención del objetivo y la estrategia del negocio (43%). Sin embargo, las micro y las pequeñas empresas que realizaron cambios en las tecnologías, destacan la **adquisición y/o cambio de equipos de cómputo portátiles**. Por su parte, las empresas medianas priorizaron **el *software* para videollamadas** y el **almacenamiento en la nube**.[14]
>
> Énfasis añadido.

Cada vez habrá más tecnología digital en la gestión de una empresa y más dispositivos conectados a Internet, más usuarios de dispositivos móviles, de Internet y redes sociales; ello representa mayores puertas de entrada a los ciberataques o incidentes de seguridad (causados por internos o externos), una organización conectada a Internet es un blanco atractivo para ciberdelincuente de cualquier parte del mundo.

Existen muchos riesgos y amenazas en el entorno digital, entre los riesgos se encuentran los ciberataques creados por delincuentes que usan tecnologías para afectar la información o sistemas de otra persona, aunado a amenazas como fenómenos naturales o humanos que pueden afectar la seguridad de la información de las organizaciones.

Entre las amenazas y riesgos causados por el ser humano, quiero destacar las principales conductas susceptibles de ser ciberdelitos y ciberdelitos[15] que afectan a las organizaciones; éstas

---

[14] MICROSOFT. (2021, enero 26). PyMEs Digitales. Retrieved mayo 2021, from Estudio de PyMEs Digitales: https://news.microsoft.com/es-xl/pymes-mexicanas-83-realizaron-un-cambio-en-su-negocio-debido-al-covid-19/

[15] Primero debemos distinguir que existen conductas que pueden dañar un sistema de información o la información como tal sin que se considere un delito (conducta susceptible de ser delito) que no está tipificada la conducta como tal. Y solo aquellas que sí tiene una redacción en un código penal o ley especial como delito,

son: ingeniería social, *phishing, ransomware,* fraude electrónico y usurpación de identidad, aunque existen muchas conductas o delitos que utilizan las tecnologías para afectar a las empresas.

Además de estos ciberdelitos, debemos considerar como riesgo las fugas de información o brechas de seguridad o exfiltración de información o datos personales, que en un gran porcentaje puede ocasionar pérdidas económicas o de reputación para la empresa y acercarla a una situación de crisis o llevarla a la quiebra.

En suma, las medidas de ciberseguridad son necesarias y urgentes para las micro y pequeñas empresas. En el presente aporte abordaremos la temática y compartiremos algunas recomendaciones para prevenir y adoptar medidas de ciberseguridad para fortalecer la madurez y resiliencia, y al mismo tiempo dar cumplimiento de algunos ordenamientos nacionales que lo exigen.

2. La importancia de la ciberseguridad

Antes de entrar en tecnicismos de ciberseguridad es importante conocernos como organización. Para ello, les propongo reflexionar a partir de las siguientes preguntas: ¿Quiénes somos, ¿cuáles son nuestros valores como organización? ¿Qué estamos cuidando? ¿Qué es importante para nuestra organización hoy día y en los próximos años?

Como resultado de las preguntas anteriores llegaremos a valorar la información, los activos de información de las organizaciones, sin importar su sector, tamaño o grado de digitalización.

Toda esta información tiene un valor en razón de su vínculo con sus titulares (personas) y sus derechos. Lo anterior exige, por tanto, un deber de cuidado y protección por parte de todas las organizaciones, ya sea para dar cumplimiento a un ordenamiento jurídico concreto o para proteger la información y otros activos vitales para el funcionamiento y continuidad de negocio.

Entre las consecuencias de no implementar medidas de ciberseguridad o realizarla en un enfoque poco integral, las organizaciones pueden ser víctimas de ataques informáticos o algún incidente sobre la información cuyo impacto puede generar, entre otras:

a) Afectación en la calidad o nivel de atención de la empresa para con sus socios, aliados, clientes, usuarios u otros.

---

entonces puede ser “delito” que usa tecnología o contra la información (ciberdelito), considerado éste como: aquellas conductas típica, antijurídica y culpable que afecta la confidencialidad, integridad o disponibilidad de la información (bien jurídicamente tutelado) o sistema de información, o bien contra el correcto funcionamiento de un sistema de información o tecnología.

b) Afectación al patrimonio de la empresa, o sus socios;
c) Responsabilidad legal y multas,
d) Afectación a la privacidad e intimidad de clientes o usuarios,
e) Daños a la reputación de una empresa,
f) Afectación al valor de mercado o presencia de marca,
g) Pérdida de información vinculada propiedad industrial y,
h) Posible violación a derechos humanos,

Debemos tener claro, que toda organización conectada a Internet o que usa alguna tecnología digital, para la gestión interna y otros procesos, es susceptible de ser afectada por un incidente cibernético (como es el caso de un ciberdelito) o sufrir un incidente de seguridad o de datos personales, ya sea desde el interior o por un completo desconocido que puede estar en cualquier parte del mundo debido a que somos parte de un escenario global.

Todas las organizaciones hoy en día se encuentran en un proceso de incorporación de tecnologías de la información y comunicación (TIC), proceso conocido también como digitalización o transformación digital. Lo anterior representa elevar las oportunidades y también asumir el reto de la ciberseguridad.

En suma, la ciberseguridad en las MiPyMEs la considero necesaria y valiosa para:

a) Fortalecer el proceso de digitalización que impulsará la empresa para obtener ventajas de la economía de escala y la era digital,
b) Elevar el nivel de seguridad de la información (activos tangibles e intangibles) en todas las áreas, procesos y sobre todas las personas que la integran.
c) Fortalecer la confianza en el interior y hacia el exterior de la organización, lo cual favorecerá el aumento de mercado y potenciales clientes
d) Generar un diferenciador respecto del modelo de negocio de la competencia.
e) Complementar las políticas de confidencialidad y privacidad y protección de datos personales.
f) Incrementa la certeza jurídica de cualquier organización,
g) Permite crecer de manera más ordenada, sin poner en riesgo la información que cada vez será en mayor volumen y criticidad
h) Complementa las políticas de inventario de activos, la capacitación del personal y la de archivos de la organización,

i) Favorece el cumplimiento de diversos ordenamientos legales, particularmente en materia de protección de datos personales,

j) Representa un avance en caso de que la empresa busque incorporarse a mercado de Norte america en el context del T-MEC,

k) El cumplimiento de estándares y certificaciones en materia de ciberseguridad favorece la buena reputación de las empresas para la creación de alianzas, fusiones o cualquier colaboración con empresas del extrajero,

l) El cumplimiento de normas técnicas o estándares internacionales en la materia genera mejor reputación y puede incrementar puntos a favor en la participación de convocatorias de contratación con entes públicos nacionales e internacionales.

3. Definiciones clave

Considero necesario que el lector conozca la referencia a los principales términos que referimos en el presente texto, y que son fundamentales para iniciar un proceso de adopción de ciberseguridad en cualquier organización. En tal sentido, es conveniente repasar las definiciones siguientes:

a) Ciberseguridad

Primero, debemos señalar que la "seguridad" en general es una condición, la condición de sentirse protegido, seguro ante cualquier agente externo e interno, que permita continuar con un desarrollo habitual y cumplir nuestras actividades y propósitos. Obtener dicha condición requiere una serie de circunstancias y la realización de acciones por individuos y organizaciones. En términos de información podemos referir a "seguridad de la información". No obstante, prefiero el término de ciberseguridad por coincidir con la postura de la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), la cual aprobó la Recomendación UIT–T X.1205, en la que defina la ciberseguridad es:

> El **conjunto de** herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse **para proteger** los activos de la organización y los usuarios en el ciber entorno.
> Los **activos de la organización y los usuarios** son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber entorno.

> **La ciberseguridad garantiza** que se alcancen y mantengan las **propiedades de seguridad** de los activos de la organización y los usuarios **contra** los riesgos de seguridad correspondientes en el ciber entorno.
> Las **propiedades de seguridad** incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad.[16]
>
> Énfasis añadido.

b) Seguridad de la Información.

Al referirnos a "**seguridad de la información"** propongo ver ésta como la circunstancia y capacidad de proteger la información, en particular sobre cuallquier riesgo o amenzas que puedan afectar una o varias de sus propiedades, es decir: **disponibilidad, integridad y confidencialidad**[17]:

1) **Disponibilidad**, refiere a que la información debe mantenerse disponible según los fines de la organización y características de la información, documento y soporte; entiéndase disponible en cualquier momento -siempre-, salvo reglas establecidas para su eliminación o destrucción, para la gestión de información de la organizción y para las personas que están autorizadas (que tienen permisos) conforme las reglas de organización (confidencialidad).
2) **Integridad,** refiere que la información (dato, información o documento en cualquier formato) deba permanecer íntegro (sin alteraciones) desde su momento de creación, durante el ciclo de vida de la misma y hasta el uso final particular para el que fue creada y hacia el futuro. La información debe ser exactamente la misma (integridad de los datos y metadatos) y ello permita identificar al creador (integridad de la fuente) y documento original o primigenio (con la posibilidad de identificar versiones); así como detectar cualquier manipulación posterior a su creación y a quien haya afectado dicha manipulación (trazabilidad y autoría o responsabilidad de la manipulación). La integridad procura que:

- Mantener la consistencia (identidad y exactitud) de los datos e información, y congruencia con el contexto que le rodea.
- Sólo quien (personas) tenga autorización pueda modificar datos (dejando registro de dicha modificación),

---

[16] ITU. (2010, noviembre). Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación Resolución 181. Retrieved mayo 2O21, from https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

[17] ISO. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved from ISO27000: https://www.iso27000.es/glosario.html Elaboración a partir de las ISO 27000 y 27001, y el Glosario de términos, ISO 2018

- No se modifiquen datos en un sistema de información (restricciones según roles y credenciales -confidencialidad-), y

3) **Confidencialidad,** refiere a que la información debe permanecer oculta o ilegible y únicamente de exclusivo acceso para quien está autorizado (legal y técnicamente de acuerdo a procedimientos y reglas), sin que deba divulgarse por quien no tenga dicha autorización, salvo la existencia de contrato de confidencialidad.

Además, se puede incorporar la cualidad de "no repudio", que refiere a que la información en tanto que cumple con las 3 cualidades anteriores, aunado a elementos de autenticación fiable (por ejemplo, una firma electrónica o mecanismos de identificación), permite asociar valores vinculantes sobre cualquier alteración y por tanto, permite que quien manifieste haber creado o quien lleve a cabo alguna alteración no pueda repudiar o rechazar dicha modificación.

La seguridad de la información suele referir a las propiedades anteriores como la triada de la seguridad de la información, o bien; el triángulo de la seguridad de la información.

La confidencialidad, integridad y disponibilidad de la información, se complementa de otros elementos secundarios o **subcategorías**: autenticidad, auditabilidad, protección a la duplicación, no repudio y legalidad.

i. **Autenticidad.** Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantiza el origen de la información, validando el emisor para evitar la suplantación de identidades.

ii. **Auditabilidad.** Define que todos los eventos o acciones de un sistema de información puedan tener trazabilidad y poder ser registrados y evaluados en control posterior.

iii. **Protección a la duplicación.** Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario y se genere registro pertinente, así como en impedir que se grabe una transacción para su posterior reproducción, con el objeto de simular múltiples peticiones del remitente original.

iv. **No repudio.** Se refiere a evitar que una persona o entidad (organización o máquina) que haya generado un documento, enviado o recibido información, o asumido el compromiso a que refiere el contenido alegue ante terceros que no la envió o recibió, o que no se obliga al contenido del documento.

v. **Legalidad.** Refiere al cumplimiento del marco jurídico al que está sujeta la institución de que se trate en relación a la información o sistema de información que utilice para la gestión de la información en su ciclo de vida y fanilidades.

c) Amenaza, vulnerabilidad y riesgo

Amenaza. Según la norma ISO2700122, señala que la amenaza es la "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización". Refiere a agentes internos o externos a una organización, que pueden ser creados por el hombre o la naturaleza, y que pueden materializarse en un "riesgo cuando se particularizan" hacia un objetivo concreto (usuario o sistema de información) en formato de riesgo.

Existen amenazas naturales como: tornado, huracán, tormenta eléctrica, inundación, terremoto, tormenta solar, (polvo, luz, agua, fuego) etc. Y amenazas causadas por humanos, entre las cuales se encuentran**:**

1. Errores accidentales o deliberados de las personas que interactúan con la información, por ejemplo: acciones no autorizadas como uso de *software o hardware* no autorizados,
2. Funcionamiento incorrecto por abuso o robo de derechos de acceso o errores en el uso,
3. Falta de disponibilidad, etc;
4. Información comprometida por robo de equipos,
5. Desvelado de secretos,
6. Espionaje, etc.[18]

También:

1. Interseptación de señales,
2. Espionaje remoto,
3. Escucha encubierta,
4. Robo de medios o documentos,
5. Robo de equipo,
6. Recuperación de medios reciclados o desechados (basura),
7. Divulgación,
8. Datos provenientes de fuentes no confiables,
9. Manipulación con Hardware /software.[19]

Vulnerabilidad. Refiere a una debilidad en un ente (organización) o un fallo en su configuración, sistema y funcionamiento que pone en riesgo a la información en alguno de sus atributos (confidencialidad, integridad y disponibilidad).

[18] INCIBE. (2015). GESTIÓN DE RIESGOS. Una guía de aproximación para el empresario. Retrieved mayo 2021, from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

[19] MINTIC. (2016). Guía de Gestión de Riesgos, Seguridad y privacidad de la información. Retrieved mayo 2021, from https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Cualquier debilidad o ausencia de medidas en los diferentes componentes (tecnológicos, humanos, procesos y productos) y espacios (físicos y digitales) pueden ser considerados una vulnerabilidad que puede aprovechar un delincuente para perpetrar su cometido (ciberataque) o bien favorecer acciones contra la seguridad que pueda ser ocasionadas por error o desconocimiento de personal interno de la organización misma.

Entre las vulnerabilidades podemos referir: Algún fallo o error de diseño: en la configuración o en el código fuente de un *software* o *hardware* usado en la organización; la falta de capacidad, concientización en las personas que integran la organización o; ausencia de políticas, planes, lineamientos en materia de ciberseguridad.

Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización,
- Procesos y procedimientos,
- Rutinas de gestión,
- Personal,
- Ambiente físico,
- Configuración del sistema de información,
- *Hardware, software* y equipos de comunicaciones, y
- Dependencia de partes externas.[20]

Otras:

- Equipamiento informático susceptible a variaciones de temperatura o humedad.
- Sistemas operativos que, por su estructura, configuración o mantenimiento son más vulnerables a algunos ataques
- Localizaciones que son más propensas a desastres naturales como por ejemplo inundaciones o que están en lugares con variaciones de suministro eléctrico
- Aplicaciones informáticas, que, por su diseño, son más inseguras que otras.
- Personal sin la formación adecuada, ausente o sin supervisión.
- Inexistencia de *software* o medidas de protección (antivirus, antispyware y antimalware).[21]

Riesgo. Según la norma ISO27001, señala que un riesgo es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

---

[20] *Ídem.*

[21] INCIBE. (2015). GESTIÓN DE RIESGOS. Una guía de aproximación para el empresario. Retrieved mayo 2021, from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

Los ejemplos de riesgos los podemos identificar cuando existen factores: 1) Existe un *phishing* (un ataque de malware) y 2) el desconocimiento de los usuarios y no existe un antivirus (vulnerabilidad). En consecuencia, se genera un impacto contra la información.

Existen criterios para medir las consecuencias o impacto contra la información:

1. Pérdidas financieras,
2. Costes de reparación o sustitución,
3. Interrupción del servicio,
4. Pérdida de reputación y confianza de los clientes,
5. Disminución del rendimiento,
6. Infracciones legales o ruptura de condiciones contractuales,
7. Pérdida de ventaja competitiva, y
8. Daños personales.[22]

C) Incidente Cibernético, ciberataque y ciberdelito

De igual forma, será más fácil comprender cada uno en una mirada integrada:

Incidente	**Ciberataque**	**Ciberdelito**
Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[23] -- Este puede ser un ciberataque (acción dolosa dirigida o no) o una situación provocada por accidente de personal interno, error o alguna vulnerabilidad explotada por una	Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.[24] -- Toda acción que pretenda afectar alguna de las propiedades de la seguridad de la información, puede o no materializarse, según la fortaleza del ataque y las medidas de control y	Refiere a una conducta antijurídica plasmada así en la ley, con una sanción; que mediante el uso de algún componente tecnológico (dentro o fuera del ciberespacio) afecta las propiedades de la información, sistema de información o cualquier componente de TIC de un individuo o ente. Estrictamente, el ciberdelito es aquella conducta tipificada (que sí tiene redacción legal y existencia en un cuerno normativo en la que contempla una sanción), antijurídica (porque contraviene la ley), que afecta el bien jurídico "información" (en cualquier componente: confidencial, integridad y disponibilidad) a través de afectar algún componente de información,

[22] *Idem.*
[23] ISO. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved from ISO27000: https://www.iso27000.es/glosario.html
[24] *Idem.*

amenaza natural (Como un incendio, inundación, etc).	protección de la organización. El ciberataque puede ser contra un objetivo concreto (una empresa, un usuario o un dispositivo específico) o aleatorio (como el spam o phishing que se lanza la red en espera de que cualquiera caiga en el engaño).	*hardware*, software o cualquier componente de TIC de una ente o persona. Existe conductas delictivas (como los anglicismos *phishing, smishing, ransomware, sexting, grooming*, etc.) que pueden no tener una redacción -tipo penal- en cuerpo penal o ley, pero que su afectación en la información y algún elemento físico y funcional son evidentes.

d) Activo de información

Refiere a "Cualquier recurso de la empresa necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo"[25]

Entre los activos de una micro, pequeña y mediana empresa, podemos referir aquellos relativos a: Instalaciones físicas, infraestructura (equipos tecnología, telecomunicaciones, TIC, operativa), información (en soporte digital o papel), la propiedad intelectual (como los secretos industriales, contratos, etc), e incluso debe darse valor a las personas, su experiencia y grado de conocimiento de la empresa o producto y servicio, a manera de valor de la persona en el funcionamiento de la organización.

1) **Ciberdelitos contra MiPyMEs**

Como hemos expresado antes, debe quedarnos claro que existen diversos tipos de riesgos y amenazas. Dentro de las amenazas causadas por factores humanos se encuentran los ciberataques y ciberdelitos. También reconocer que existen conductas delictivas (como una forma didáctica de referir a conductas que puedan no estar tipificadas, pero causan un daño) y conductas delictivas (si tipificadas -que existe texto en en ley-) las cuales referimos como ciberdelitos cuando usan las

[25] INCIBE. (2015). GESTIÓN DE RIESGOS. Una guía de aproximación para el empresario. Retrieved mayo 2021, from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

tecnologías digitales como medio o fin para afectar el bien jurídicamente protegido que es la información.

a. Costo de los ciberdelitos

Calcular los costos del cibercrimen es complejo, por diferentes razones, entre las cuales puedo señalar las siguientes:

a) Complejidad cuantificar el valor de la información o infraestructura atacada;
b) Dificultad de dar seguimiento al surgimiento de innumerables de amenazas y delitos cibernéticos que se comenten diariamente;
c) Dificultad de determinar el lugar del impacto y la distribución del mismo entre las varias partes afectadas;
d) Ausencia de una Estrategia Nacional de Ciberseguridad que a su vez incluya indicadores para dar seguimiento a la materia;
e) Ausencia de una Estrategia de combate al cibercrimen, en particular;
f) Incipiente intercambio de información entre los diferentes entes públicos de los tres poderes y entes autónomos; particularmente entre Fiscalías, general y locales; entre Secretarías de seguridad, particularmente policías cibernéticas y;
g) Falta de protocolos y mecanismos que favorezcan el intercambio de información sobre el tema por parte del sector privado y sociedad.
h) Condiciones desfavorables para estimular la denuncia de parte de la sociedad: sector privado, academias públicas y sociedad en general.
i) Falta de inversión para el desarrollo de capacidades en el combate y prevención de los ciberdelitos.

A reserva de la complejidad, existen diversos esfuerzos o actividades que nos permiten acercarnos al fenómeno, con las reservas del caso, aplicando diversas metodologías, dimensionar su alcance, impacto y finalidades secundarias.

Uno de los documentos más ilustradores en el avance que se tiene en la materia, a nivel regional, es el estudio "Ciberseguridad: riesgos, progreso y el camino a seguir en América Latina y el

Caribe"[26], refiere que el el impacto social y económico de los incidentes cibernéticos que, sólo en 2019, costaron más de **90.000 millones** de dólares.

Por otro lado, según *Symantec*, la ciberdelincuencia ha afectado a más de **1 billón** de personas adultas a nivel mundial, y cerca de **800 millone**s de víctimas en el último año.[27] El impacto de los ciberataques podría superar **el 1% del PIB** en algunos países. Los ciberataques a infraestructura crítica esta cifra podría alcanzar el **6% del PIB**. De una lista de 16 países, México se encuentra entre los **cuatro que más delitos cibernéticos** de **usurpación de identidad** han experimentado, tan solo después de China, Estados Unidos y Brasil, medido en términos del total de la población que ha sido víctima de este ciberdelito en 2019.[28]

De acuerdo con el reporte "Los costos ocultos del cibercrimen"[29] las pérdidas globales causadas por los ciberdelitos suman más de **$1 trillones de dólares**, aumentando más del 50 por ciento desde 2018. El mismo reporte estima que dos tercios de las empresas encuestadas informaron haber sufrido algún tipo de incidente cibernético en 2019. Por su parte, *Cybersecurity Ventures* predice que el ciberdelito costará al mundo más de $6 trillones USD anuales para 2021.[30]

En el caso de México, "en 2021 el ataque con mayor crecimiento en México será el ransomware y menos del 50% de las organizaciones cuentan con personal capacitado para enfrentarlo. En México el costo promedio de remediación para las organizaciones por un ataque de *ransomware* es de $470 mil US dólares y si se paga el rescate, es de $940 mil US dólares. En 2020, el ransomware se dirigió principalmente al sector manufacturero, las organizaciones de atención médica y las empresas de construcción, y el rescate promedio alcanzó los $500 mil US dólares"[31]

---

[26] OEA y BID. (2020). Ciberseguridad Riesgos, avances y el camino a seguir en América latina y el Caribe. Retrieved mayo 2021, from Obervatorio ciberseguridad: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[27] Norton. (2019). Retrieved mayo 2021, from Cyber Safety Insights Report Global Results: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf?promocode=DEFAULTWEB%20

[28] *Idem.*

[29] McAfee and CSIS. (2020, Diciembre 7). Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact. Retrieved mayo 2021, from https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629

[30] Cybersecurity Ventures. (2019). 2019 Official Annual Cybercrime Report. Retrieved Mayo 2021, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[31] SILINK. (2021, abril). EL CIBERCRIMEN AL ALZA: LOS ATAQUES DE RANSOMWARE SE VUELVEN MÁS COMUNES Y EFICIENTES. Retrieved mayo 2021, from Cybercrime: https://www.silikn.com/2021/04/el-cibercrimen-al-alza-los-ataques-de.html

De acuerdo a FBI, el fraude del CEO (BEC por sus siglas en inglés) en Estados Unidos, han resultado en pérdidas mundiales de al menos US$26.000 millones desde 2016**.**

Uno de los casos que más llama mi atención es el incremento del ransomware, en particular el incremento de ganancias que, de acuerdo con Elliptic, el grupo *DarkSide* ha obtenido 90 millones de dólares USD en bitcoins, desde octubre 2020 a mayo 2021. Con un promedio de 1.9 millones USD por víctima.[32]

Finalmente, la Guardia Nacional refiere que los incidentes cibernéticos, de diciembre de 2018 a diciembre de 2020, son los siguientes:

a) 188 mensajes de correo tipo spam;
b) 1,338 vulnerabilidades de ciberseguridad en infraestructuras tecnológicas;
c) 3,267 ataques de denegación de servicios DoS;
d) 3,720 divulgación no autorizada de información;
e) 6,502 ataques de fuerza bruta;
f) 11,182 sitios web fraudulentos (*phishing*) mitigados; y
g) 157,332 infección por código malicioso.[33]

b. Motivos del ciberataque

En este rubro vale la pena precisar que existen diversos tipos de delincuentes o ciberatacantes, así como diferentes motivaciones. Esto ayudará a que las organizaciones comprendan el contexto de sus amenazas y los actores que pueden estar detrás de la pretensión de afectar la seguridad de la información de una micro, pequeña o mediana empresa. Entre las **razóne**s por las que una persona u organización realiza ciberataques, están (con apoyo de materiales de INCIBE):

a) **Económicas.** Existe claro interés en obtener un beneficio económico para sí o para otra persona y la afectación se materializa contra información que permita obtener algún recurso con valor económico o directo para obtener un bien o valor.

   Ejemplo: fraudes o venta de bases de datos, robo de secretos industriales, *phishing* con fines de obtener claves bancarias o la obtención de una cantidad en criptomonedas a cambio de devolver la clave para acceder a la información o para evitar que se publique información personal o confidencial (como en el caso del *ransomware*).

[32] ELLIPTIC. (2021, mayo). DarkSide Ransomware has Netted Over $90 million in Bitcoin. Retrieved mayo 2021, from https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

[33] Guardia Nacional. (2021, mayo 3). 1era Jornada de Ciberseguridad. Retrieved mayo 2021, from Conferencia de Oliver González Barrales_División General Científica: https://www.facebook.com/udlapjenkinsgs/videos/333104624833555/

b) **Ideológicas.** Las actividades de ciberataques están motivadas por razones religiosas, de ideología política o filosófica.

   Ejemplo. Un ataque a un sitio web que difunde ideas de "pro aborto legal" o que "venda productos de origen anial", puede ser atacado por quien tenga una visión contraria. Es muy importante cuidar el lenguaje y significado de las publicaciones por redes sociales y las declaraciones personales de los directivos, evitar involucrarse en temas controversiales.

c) **Venganza contra empresa o personal.** Buscan afectar a una persona o empresa determinada. Generalmente buscan exhibir o divulgar información privada o confidencial que afecte la reputación y/o patrimonio de la empresa o la persona de cargos directivos.

d) **Desafío, reto o ego personal**. Las personas ponen a prueba sus capacidades para vulnerar un sistema de información o componente de TIC y sus medidas de seguridad, buscan demostrar su habilidad o darse a conocer.

   Ejemplo: Acceso ilícito a sustema de información, sin que afecten la información, el sistema mismo o a las personas sobre quienes refiere la información, muchas veces dejan un saludo y nombre con el que se le conocen en el ámbito cibernético.

e) **Nacionalismo extremo.** Aquellos delincuentes del ciberespacio que colaboran (con o sin pago) para una operación de ataque a una empresa o gobierno extranjero del cual tengan repudio o conflicto bélico, sin pertenecer a las fuerzas armadas.

4.3 Ciberdelitos y conductas delictivas contra MiPyMEs

Antes de referir particularmente a algunos de los ciberdelitos que pueden afectar la información de MiPyMEs, vale la pena precisar que:

a) El bien jurídico protegido es la información y la referencia a otros derechos que ésta puede tener.

b) Existen tipos penales tradicionales que pudieran realizarse por medios diferentes a los que señala la redacción penal, es decir por medio de tecnologías digitales; y ello deberá considerarse.

c) Existen conductas delictivas que se desarrollan necesariamente en el entorno digital, por lo que es muy probable que no exista referencia normativa.

d) Aunque muchas conductas delictivas no tengan un tipo penal en la legislación la afectación en otros derechos puede verse materializada, ello abre la pauta a exigir el apoyo de

autoridades y accionar el aparato de justicia, incluyendo la interpretación de órganos jurisdiccionales sobre la ley y las conductas que dañan a la sociedad y sus derechos.

e) Un alto porcentaje de los ciberdelitos pueden evitarse mediante concientización, educación, formación y capacitación de las personas que integran una organización.[34]

f) El éxito de las amenazas (ciberdelitos y otros incidentes) es directamente proporcional a la debilidad existente en áreas, procesos o tecnologías de las organizaciones.

Entre los ciberdelitos que consideró, de acuerdo a varios estudios o referencias de las principales fuentes de amenazas o vectores de ataque, pueden afectar a las MiPyMEs, en mayor medida son en seguimiento a:

Conducta delictiva / Ciberdelito	**¿Qué es o cómo se realiza?**	**Algún ejemplo**
a) Ingeniería social.	Son acciones o técnicas utilizadas para obtener información o datos de naturaleza sensible o confidencial, como es el caso de datos que puedan constituir contraseñas o información útil para preparar un ataque o ciberdelito. El objetivo es crear un escenario que facilite el engaño y que la víctima proporcione la información para ser utilizada por el delincuente. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución educación de la víctima.	Uno de los ejemplos más característicos es el *phishing (*crea un sitio web o mensaje falso idéntico al original*)*, *Smishing* (sobre mensajes de texto SMS), y otras técnicas vía correo electrónico o aplicaciones de mensajería como *WhatsApp*, Telegram u otras redes sociales. Entre los métodos de ingeniería social, podemos referir: phishing, smishing, vishing, baiting (una USB regalada o abandonada con malware), spam malicioso, entre otras.

[34] De acuerdo con IBM, en su informe de ciberseguridad conocido como IBM X-Force Threat Intelligence Index 2018, se observó que un porcentaje de 95% de incidencias de ciberseguridad se deben a errores humanos. El estudio analizó las causas de diversos incidentes de seguridad de 2015, 2016, 2017 y 2018. En tal sentido, podemos reforzar el argumento de apostar por la formación y capacitación de las personas. El mismo estudio, 2020, reveló que el *ransomware* fue el método de ataque más popular en 2020, alcanzando un el 23% de de todos los incidentes. Véase IBM X-Force Threat Intelligence Index 2021 en: https://www.ibm.com/downloads/cas/AWJ3PE1M

b) Phishing	Es el principal vector de ataque, principalmente por correo electrónico, aunque puede llegar por mensajería (web o app). El atacante crea un mensaje o sitio web falto idéntico al original con el que engaña a la víctima y le hace entregar información personal, financiera o credenciales para ingresar a algún sistema, del cual puede obtener más información o la capacidad de generar algún beneficio económico para sí o un tercero. El phishing suele verse acompañado de *spam* (publicidad no deseada o no solicitada).	Ejemplo. Un correo de nuestra institución bancaria, tienda departamental o cualquier comercio que requiere actualizar contraseña y proporcionar datos de cuenta, vigencia y código de seguridad. Con esa información, el delincuente obtiene los datos bancarios necesarios para luego retirar o realizar compras en línea a cargo de nuestra tarjeta. 
c) Ransomware	Es un ataque con *malware* (software malicioso) vía remota, que puede utilizar la técnica de *phishing* como canal conductor, donde el ciberdelincuente logra infectar el sistema de información del objetivo, tomando control del equipo infectado; cifra la información, y amenaza a la organización o usuario (extorsión) para que le pague un rescate a cambio de no divulgar información o para devolver la clave que permita acceder a la información cifrada.	Uno de los casos más recientes es el de los oleoductos estadounidenses que administra la empresa Colonial Pipeline, la cual fue afectada con ransomware atribuible a DarkSide, grupo de delincuencia organizada de Europa del Este, por el cual dicha empresa pagó 5 millones de USD para recuperar el acceso a la información.[36] Otro caso reciente es el caso FatFace, donde ciberdelincuentes rusos (*Wizard Spider*) atacó a la cadena británica de ropa, la cual tuvo que cerrar 200 tiendas en todo el país y a la que le exigieron pagar 8

[36] DW. (2021, mayo). Medios: Colonial Pipeline pagó 5 millones a los hackers para rescatar su sistema. Retrieved from https://www.dw.com/es/medios-colonial-pipeline-pag%C3%B3-5-millones-a-los-hackers-para-rescatar-su-sistema/a-57526639

	Hemos podido observar que el rescate se pide en criptomonedas, ya que éstas permiten ocultar rastro y complicar la tarea de investigación de autoridades. En el caso del grupo DarkSide el pago por rescate en el caso Colonial PipeLine fue cercano a 75 *bitcoins*.[35]	millones, de los cuales pagó solo 2 millones.[37]
d) Fraude del CEO (*Business E mail Compromise*)	Consiste en que un empleado de alto rango, o el contable de la empresa, con capacidad para hacer transferencias o acceso a datos de cuentas, recibe un correo, supuestamente de su jefe, ya sea su CEO, presidente o director de la empresa, o de un alto funcionario de una tercera organización (socio, proveedor o cliente). En este mensaje le pide ayuda para una operación financiera **confidencial y urgente**.[38]	El Centro de Quejas de Delitos en Internet (IC3), del Buró Federal de Investigaciones (FBI, por su sigla en inglés) del gobierno de Estados Unidos ha visto un incremento del uso de criptomonedas en esquemas de fraudes de compromiso de correos electrónicos empresariales (BEC), o personales, que también son conocidos como fraudes del CEO.[39] Un ejemplo de texto es el siguiente: "Oye, el trato está hecho. Por favor transfiere US$8 millones a esta cuenta para finalizar la adquisición lo antes posible. Hay que

[35] ELLIPTIC. (2021, mayo). DarkSide Ransomware has Netted Over $90 million in Bitcoin. Retrieved mayo 2021, from https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

[37] EL Confidencial. (2021, mayo 23). EL NEGOCIO DEL QUE NADIE QUIERE HABLAR. Retrieved mayo 2021, from Llame al seguro y envíe 8 millones": La gasolina que alimenta el alud de cibersecuestros: https://www.elconfidencial.com/tecnologia/2021-05-23/ransomware-ciberataques-sepe-glovo-aseguradoras_3088831/

[38] INCIBE. (2017). Retrieved mayo 2021, from Glosario de términos de ciberseguridad. Una Guía de aproximación para el empresario: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[39] EL Economista. (2021, abril 19). EL Economista. Retrieved mayo 2021, from FBI alerta de "fraudes del CEO" relacionados con criptomonedas: https://www.eleconomista.com.mx/economia/FBI-alerta-de-fraudes-del-CEO-relacionados-con-criptomonedas-20210419-0101.html

		hacerlo antes de que termine el día. Gracias."[40]
e) Usurpación de identidad	Típicamente conocida como "robo de identidad". Refiere a cualquier acción que utiliza diferentes técnicas de ingeniería social o malware con el objetivo principal de obtener información de identidad, credenciales o permisos respecto de una cuenta o para gestionar la identidad. También puede entenderse como "Es una actividad malintencionada que busca hacerse pasar por otra persona o entidad por diferentes motivos: robo de datos, fraudes y engaños para obtener información o un beneficio económico"[41]. Los ataques y fraudes basados en la suplantación de identidad pueden ser muy variados, aunque se distinguen principalmente por dos cosas: a) **Robo o** acceso no autorizado a una cuenta: cuando el atacante ha conseguido acceder a nuestra cuenta haciendo uso de nuestras contraseñas, que ha obtenido	La forma más didáctica es con una imagen. En la siguiente imagen se muestra un mensaje (probablemente vía phishing) para obtener información de identidad del usuario.[42] 

[40] BBC News. (2019, septiembre 30). Retrieved mayo 2021, from Qué es el "fraude del CEO" con el que los hackers han robado US$26.000 millones de empresas desde 2016: https://www.bbc.com/mundo/noticias-49878717

[41] INCIBE. (2021, febrero). Suplantación de identidad y secuestro de cuentas: ¿cómo actuar? Retrieved mayo 2021, from https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar

[42] *Ídem.*

	a través de distintas técnicas y ataques. b) **Creación de perfil falso**. el atacante ha creado una cuenta o perfil muy similar al nuestro o al de otra persona, entidad o empresa.	
f) Fraude al comercio electrónico	Refiere a la conducta de engañar, usando algún tipo de tecnología, para obtener algún beneficio económico para sí o para otro. Entre las variables pueden ser: *g) Spam* *h) Spoofing* *i) Phishing* *j) Smishing* k) *Pharming*[43]	Otro de los más comunes es el fraude en el comercio electrónico. Puede constituirse mediante un sitio web falso (*spoofing*), un correo con identidad falta (*phishing*) o un nombre de dominio falso (*DNS spoofing*), o la oferta de un producto falso o la no entrega del producto ofertado en un sitio de comercio electrónico o por redes sociales. Ejemplo de mensa: 

Como hemos podido observar, existen muchas conductas delictivas o delitos, y conforme avanza la tecnología se podrán observar variantes en la ejecución, modalidad e impacto de las mismas.

El costo de los ciberdelitos cada vez es mayor y la variedad de conductas se vuelve más sofisticada y compleja para la labor de investigación y sanción de los ciberdelitos. No obstante, en

[43] INCIBE. (2017). Retrieved mayo 2021, from Glosario de términos de ciberseguridad. Una Guía de aproximación para el empresario: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

México ya se cuenta con cierto avance en materia regulatoria, tanto desde la perspectiva de ciberdelitos como de la consideración u obligación de adoptar medidas de ciberseguridad.

2) Regulación de la ciberseguridad

En términos generales la ciberseguridad es adoptada como un complemento del desarrollo tecnológico y en los últimos años también se ha incrementado la referencia de la ciberseguridad, en sus diferentes aristas, en ordenamientos administrativos, normas técnicas para desarrollo de procesos vinculados a tecnologías digitales y también en diversos ordenamientos que pueden vincularse con trámites y servicios y sobretodo, para la protección de la información y datos personales de individuos y empresas.

Particularmente, hemos visto avances considerables en esta etapa de pandemia, en la cual diversas organizaciones, públicas y privadas, han adoptado un proceso de digitalización acelerada y ante los constantes incidentes cibernéticos y su impacto económico en en términos de derechos cada día más Estados y empresas privadas asumen la ciberseguridad como un compromiso para con sus clientes y comunidad de usuarios.

Al respecto, a continuación, daremos un repaso de algunos ordenamientos jurídicos mexicanos que refieren a medidas de ciberseguridad como componente aplicable a micro, pequeñas y medianas empresas.

En primer lugar, la propia Carta Magna precisa que toda persona tiene derecho a nor ser molestado persona, familia, domicilio, papeles o posesiones (Art. 16 párrafo primero), derecho a la protección de sus datos personales (Art. 16 2do párrafo) y de su vida privada (Art. 6), libertad de expresión (Artículo. 7º) la inviolabilidad de sus comunicaciones (Art. 16 párrafo 12); a recibir seguridad pública por parte del Estado cuyo fin es salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas. Lo anterior, constituye el fundamento constitucional del derecho a la protección de datos personales, los cuales constituyen una de las diferentes formas de expresión en formato de información que debe ser protegida en favor de su titular y por las diversas vías (físicas, tecnológicas y otras que sean necesarias y pertinentes).[44]

Especialmente es una obligación de las autoridades o entes públicos del Estado mexicano y cualquier persona moral (como las MiPyMEs) y física que posea información y datos de las personas

[44] CPEUM_Congreso de la Unión. (2021). Constitución Política de los Estados Unidos Mexicanos. Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_170521.pdf

físicas o morales, pues la información (datos personales o no) guardan directa relevancia con derechos y libertades.

En tal sentido, la seguridad (en el entorno digital) o ciberseguridad es también una obligación del Estado Mexicanao, y es prudente transferir -a través de diversos ordenamientos federales o generales- la responsabilidad, obligación y compromiso, a las MiPyMEs que tratan datos de clientes, usuarios, trabajadores, proveedores u otra persona física o moral que sea titular de dicha información o dato personal.

a) **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP);**

Este ordenamiento es aplicable a cualquier persona física o moral (como es el caso de las MiPyMEs) que **traten** (obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio) **datos personales** (cualquier información concerniente a una persona física identificada o identificable).

Entre los principios del Derecho de protección de datos personales, en la propia ley refiere que éstos son:

> Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y **responsabilidad**, previstos en la Ley.[45]

Derivado del principio de responsabilidad, los destinatarios de la LFPDPPP asumen obligaciones de proteger los datos personales, y todas las MiPyMEs deben adoptar medidas de seguridad administrativa, técnicas o lógicas y físicas, como lo señala el artículo 19 de la LFPDPPP, que a la letra dice:

> Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá **establecer y mantener medidas de seguridad** administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
>
> Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.[46]

---

[45] RLFPDPPP. (2021). Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

[46] *Idem.*

Aunado a lo anterior, en relación a los incidentes de ciberseguridad, toda vulneración (entiéndase todo incidente contra la integridad, disponibilidad o integridad de los datos personales) en cualquier fase del tratamiento, debe notificarse al titular para que éste determine si ejerce sus derechos ARCO. (Artículo 20 LFPDPPP).

Existen el delito de tratamiento indebido de datos personales, en el cual podría incurrir una MiPyME si no realiza las medidas de seguridad de la información adecuada, tal circunstancia será aplicable "al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia" y "al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos".[47].

A manera de ampliación, el Reglamento de la LFPDPPP[48], aporta elementos valiosos que ayudarán a las MiPyMEs a identificar qué medidas de seguridad (ciberseguridad) debe / puede desarrollar para incrementar la protección de los activos de información de la organización. Éste ordenamiento refiere que las medidas de seguridad son:

a) "Medidas de **seguridad administrativas** (Artículo 2, f. V): Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;"
b) Medidas de **seguridad técnicas** (Artículo 2, f. VII): "Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:
    a. El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
    b. El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
    c. Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
    d. Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;"
c) Medidas de **seguridad físicas** (Artículo 2, f. VI): "Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para":
    a. Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
    b. Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

[47] *Ídem.*
[48] *Ídem*

c. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
d. Garantizar la eliminación de datos de forma segura;"[49]

Como puede observarse, es un desarrollo importante para la protección de la información en su vertiente de "dato personal". No obstante, faltan se requiere ampliar el alcance a todo tipo de información.

b) **Ley Federal del Trabajo, en su apartado de Teletrabajo;**

El pasado once de enero de 2021, se publicó por el que se reforma el artículo 311 y se adiciona el capítulo XII Bis de la Ley Federal del Trabajo (LFT), en materia de Teletrabajo (DOF Teletrabajo, 2021), el cual refirió el **teletrabajo** como "una forma de organización laboral subordinada que consiste en el desempeño de actividades remuneradas, en lugares distintos al establecimiento o establecimientos del patrón, por lo que no se requiere la presencia física de la persona trabajadora bajo la modalidad de teletrabajo, en el centro de trabajo, utilizando primordialmente las tecnologías de la información y comunicación, para el contacto y mando entre la persona trabajadora bajo la modalidad de teletrabajo y el patrón.

La **persona trabajadora** bajo la modalidad de teletrabajo será quien preste sus servicios personal, remunerado y subordinado en lugar distinto a las instalaciones de la empresa o fuente de trabajo del patrón y utilice las tecnologías de la información y la comunicación.

Con la precisión de que: No será considerado teletrabajo aquel que se realice de forma ocasional o esporádica.

> **Artículo 330-E.-** En modalidad de teletrabajo, los patrones tendrán las obligaciones especiales siguientes:
>
> …
>
> **V.** Implementar mecanismos que preserven la **seguridad de la información y datos** utilizados por las personas trabajadoras en la modalidad de teletrabajo;[50]

c) **Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech)**

---

[49] *Ídem*

[50] DOF_Teletrabajo. (2021, O1 11). DECRETO por el que se reforma el artículo 311 y se adiciona el capítulo XII Bis de la Ley Federal del Trabajo, en materia de Teletrabajo. Retrieved mayo 2021, from Reforma Ley Federal del Trabajo: http://www.diputados.gob.mx/LeyesBiblio/legis/reflxiv/129_LFT_11ene21.doc

Fintech se refiere a tecnologías financieras o uso de tecnologías en actividades del sector financiero. También refiere al sector de la economía vinculado a servicios financieros que se pueden ofrecer y desarrollar a través de tecnologías digitales actuales y futuras. Entre impactos del sector fintech, se encuentran: a) el impulso a la democratización de servicios financieros; b) usuarios más exigentes en la calidad del servicio; c) surgimiento de startups que brindan servicios financieros innovadores; d) que los actores "tradicionales" incorporen modelos fintech a sus operaciones financieras, ya sea adquiriendo startup fintech, desarrollando in house su servicio fintech o mediante alianza.[51]

Sobre el ecosistema fintech en México, Luis Silva de La Torre, Director General de la Asociación Fintech México; refirió que 4.6 millones de personas o empresas utilizan (en 2020) alguna solución basada en fintech y para 2021 se espera que la cifra se duplique alcanzando hasta a 9.2 millones de usuarios, impulsados por el contexto de la pandemia de Covid-19.[52]

El ordenamiento jurídico aplicable es la Ley para Regular las Instituciones de Tecnología Financiera (Ley fintech) se publicó en marzo de 2018. Su objeto es (Artículo 1) crear un marco jurídico que brinde certeza y establezca las bases para la entrada de nuevos jugadores al sistema financiero, fomentar mayores oportunidades de inversión y proteger derechos de los consumidores, (principalmente su patrimonio).

La Ley fintech, de manera general, contempla la regulación de los servicios financieros que prestan: a) Instituciones de financiamiento colectivo (de deuda, de capital o de copropiedad) y b) Instituciones de fondos de pago electrónico (emisión, administración, redención y transmisión de fondos de pago electrónico); a estos 2 rubros se le denomina Instituciones de Tecnología Financiera (ITF).

Por otro lado, también refiere a servicios financieros que sean ofrecidos o realizados por medios innovadores -*sandbox*- sujetos a alguna normatividad especial.

Los principios rectores de la Ley Fintech son:

1) Inclusión e innovación financiera,

2) Promoción de la competencia,

---

[51] ALAI. (2019, mayo). Recomendaciones para el fortalecimiento del sector fintech en México. Retrieved mayo 2021, from www.ala.lat: https://alai.lat/wp-content/uploads/2019/05/Recomendaciones-para-el-fortalecimiento-del-sector-Fintech-en-Mexico.pdf

[52] FORBES. (2021, abril 21). forbes.com.mx. (L. S. Torre, Producer) Retrieved mayo 2021, from Empresas fintech experimentan el impulso de la pandemia: https://www.forbes.com.mx/foro-empresas-fintech-impulso-pandemia/#:~:text=Para%202021%20se%20espera%20que,digitalizaci%C3%B3n%20derivada%20de%20la%20pandemia.

3) Protección al consumidor,

4) Preservación de la estabilidad financiera,

5) Prevención de operaciones ilícitas y;

6) Neutralidad tecnológica.[53]

En materia de ciberseguridad, como parte del objetivo de la protección al consumidor y la seguridad que deben ofrecer a sus clientes, aunado a la obligación de adoptar medidas de seguridad que le exige la LFPDPPP (que ya revisamos), como requisito para la obtención de autorización por la CNBV, lo siguiente:

> Artículo 39.- Las solicitudes para obtener las autorizaciones de la CNBV previstas en el presente Capítulo deberán acompañarse de lo siguiente:
>
> ...
>
> VI. Las medidas y políticas en materia de control de riesgos operativos, así como de **seguridad de la información, incluyendo las políticas de confidencialidad**, con la evidencia de que cuentan con un soporte tecnológico seguro, confiable y preciso para sus Clientes y con los estándares mínimos de seguridad que aseguren la **confidencialidad, disponibilidad e integridad de la información** y prevención de fraudes y ataques cibernéticos, de conformidad con lo establecido en las disposiciones de carácter general aplicables;[54]

Para el cumplimiento de lo anterior, la CNBV deberá emitir las disposiciones de carácter general para el correcto funcionamiento de las ITF, en materia de controles internos y administración de riesgos. Así, respecto de la seguridad de la información tenemos que la Comisión (Artículo 48, Ley Fintech):

a) Tratándose de **instituciones de financiamiento colectivo** podrá emitir disposiciones de carácter general en materia de seguridad de la información, incluyendo las políticas de confidencialidad, uso de medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos y continuidad operativa.

---

[53] DOF_LeyFintech. (2018, marzo 9). DECRETO por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de Organizaciones y Act. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

[54] DOF. (2021). LFPDPPP. Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

b) Tratándose de **instituciones de fondos de pago electrónico**, la CNBV y el Banco de México **emitirán conjuntamente** disposiciones de carácter general en materia de seguridad de la información, incluyendo las políticas de confidencialidad y registro de cuentas sobre movimientos transaccionales, el uso de medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos y continuidad operativa.[55]

La Ley Fitech le confiere a la Secretaría (Secretaría de Hacienda y Crédito Público) la atribución de emitir los lineamientos sobre el procedimiento y criterios, casos, forma, términos y plazos que deberán observar las ITF, en materia de seguridad de la información (Artículo 58, párrafo tercero, fracción III):

> III. La forma en que las ITF deberán resguardar y garantizar la **seguridad de la información y documentación** relativas a la identificación de sus Clientes o quienes lo hayan sido, así como la de aquellos actos, Operaciones y servicios reportados conforme al presente artículo;

La atribución anterior, dio fundamento a otras disposiciones:

a) Las "Disposiciones de carácter general a que se refiere el Artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera", que en materia de seguridad de la información considera que:[56]

1) **Artículo 25.-** Las ITF están **obligadas a conservar, por un periodo no menor a diez años**, contados a partir de la ejecución de la Operación, actividad o servicio realizado con o por sus Clientes, lo siguiente: …

i. La conservación prevista en este artículo podrá realizarse por medio de Mensajes de Datos siempre que cumpla con la norma oficial mexicana sobre digitalización y conservación de mensajes de datos aplicable, o bien, por Medios Electrónicos que aseguren que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta y se garantice la seguridad de la información recabada del Cliente, de conformidad con los estándares de seguridad que al efecto establezca la CNBV.

2) **Artículo 56.-** Las ITF deberán contar con **sistemas automatizados** que desarrollen, entre otras funciones, las siguientes: … XI. Mantener esquemas de **seguridad de la**

[55] DOF_LeyFintech. (2018, marzo 9). DECRETO por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de Organizaciones y Act. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

[56] DOF. (2018, 09 10). DISPOSICIONES de carácter general a que se refiere el Artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera. Retrieved from https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018

información procesada, que garanticen la integridad, disponibilidad, auditabilidad y confidencialidad de la misma.

b) Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera:[57]

Capítulo VI De la Seguridad de la información.

Artículo 63.- El director general o, en su caso, el administrador único de la **institución de financiamiento[58] colectivo**, será responsable de la implementación de los controles internos en materia de **seguridad de la información** que procure su confidencialidad, integridad y disponibilidad. El marco de gestión a que se refiere este párrafo, deberá asegurar que la Infraestructura Tecnológica de dicha institución, ya sea propia o provista por terceros, se apegue a los requerimientos siguientes:

…

III.Que se hayan considerado aspectos de seguridad de la información en la definición de proyectos para adquirir o desarrollar cada uno de sus componentes, debiendo incluirlos durante las diversas etapas del ciclo de vida. Este comprenderá la elaboración de requerimientos, diseño, desarrollo o adquisición, pruebas de implementación, pruebas de aceptación por parte de los Usuarios de la Infraestructura Tecnológica, procesos de liberación incluyendo pruebas de vulnerabilidades y análisis de código previos a su puesta en producción, pruebas periódicas, gestión de cambios, reemplazo y destrucción de información.

a) Segregación lógica, o lógica y física de las diferentes redes,
b) Configuración segura de acuerdo al componente,
c) Mecanismos de seguridad en las aplicaciones que procuren que, durante su ejecución se protejan de ataques o intrusiones, tales como inyección de código, manipulación de la sesión, fuga de información, alteración de privilegios de acceso, entre otros (…).

IV. Que cada uno de sus componentes sea probado antes de ser implementado o modificado (…),
V. "Implementar controles que permitan asegurar la confidencialidad, integridad y disponibilidad de la información de los Clientes,
VI. "Que cuente con las licencias o autorizaciones de uso, en su caso".
VII. "Que cuente con medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada (…)

…

[57] DOF_DG. (2018, 09 10). Retrieved mayo 2021, from Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera: https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf

[58] DOF_LFPC. (1992, 12 24). Retrieved mayo 2021, from Ley Federal de Protección al Consumidor: http://www.diputados.gob.mx/LeyesBiblio/pdf/113_241220.pdf

(Artículo 65). Las instituciones de financiamiento colectivo **deberán contar con una persona** que se desempeñe como **oficial en jefe de seguridad de la información (**conocido como CISO por sus siglas en inglés: *Chief Information Security Officer).*

Aunado a lo anterior, la regulación refiere otros roles o profesionales vinculados a la ciberseguridad, tales como:

- Oficial en Jefe de Seguridad de la Información (puede ser un tercero o proveedor)
- Responsable de la Administración de Riesgos.
- Comité de Auditoría y Comité de Riesgos. (opcional)
- Equipo de atención y respuesta a Incidentes de Ciberseguridad.

(Artículo 67) Informar cuando ocurra un incidente o evento de seguridad de la información en: (i) los componentes de la Infraestructura Tecnológica de la institución de financiamiento colectivo; (ii) los canales de atención a los Clientes, tales como Medios Electrónicos, o (iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la institución de financiamiento colectivo.

…

c) Disposiciones aplicables a **las instituciones de fondos de pago electrónico** a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera",[59] que respecto a seguridad de la información expresa:
d) Capítulo II de "Seguridad de la Información" con referencia a: Infraestructura Tecnológica frente a los Clientes, Canales de Instrucción y las Operaciones, Autenticación en los Canales de Instrucción; requerimientos de seguridad de información en los Canales de Instrucción; Infraestructura Tecnológica en los procesos internos;
e) Disposiciones complementarias: a) indicadores de seguridad de la información; b) requerimientos mínimos para el Plan de Continuidad de Negocio; c) Indicates y d) Informe de incidentes; e) Supervisión, diseño o implementación de políticas y procedimientos para la seguridad de la información, uso de Canales de Instrucción o continuidad operativa; f)

[59] DOF. (2021, 01 28). Retrieved from Disposiciones aplicables a las instituciones de fondos de pago electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera: https://dof.gob.mx/nota_detalle.php?codigo=5610487&fecha=28/01/2021

Contratación o relación con proveedores de servicios vinculados a seguridad de información y evaluación de cumplimiento; entre otros.[60] Estos Anexos, incluyen formatos o tablas que favorecen el cumplimiento de las medidas y ayudan a la evaluación y seguimiento de medidas en la materia.

Aunado a estas disposiciones, también existen circulares emitidas por BANXICO en materia de seguridad de la información aplicables a una parte de ITF, más la regulación aplicable a instituciones de crédito. Como se puede observar, las medidas de seguridad de la información para el sector fintech se encuentran más desarrolladas que para otras empresas en otros sectores. Estas disposiciones pueden ser un referente para cualquier MiPyME.

d) **Ley Federal de Protección al Consumidor (LFPC).**

Si la organización (MiPyMEs) realiza actos de comercio, debe saber que la LFPC establece principios, derechos y obligaciones y cultura del consumidor, precisando algunos requisitos o obligaciones a los comerciantes, así como diversas circunstancias vinculadas con la seguridad de la información, tal es el caso de los siguientes principios referidos en el artículo primero, párrafo tercero[61]:

> Son principios básicos en las relaciones de consumo:
>
> …
>
> IV. La efectiva prevención y reparación de daños patrimoniales y morales, individuales o colectivos;
>
> …
>
> VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios.
>
> VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, **electrónicos**, ópticos o de cualquier otra tecnología y la **adecuada utilización de los datos** aportados;

Como punto de partida debemos tener claras las definiciones de:

---

[60] *Ídem*.

[61] DOF_RLFPC. (2019, diciembre 19). Reglamento de la LFPC. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPC_191219.pdf

a) Proveedor (Artículo 2, f II): la persona física o moral en términos del Código Civil Federal, que habitual o periódicamente ofrece, distribuye, vende, arrienda o concede el uso o disfrute de bienes, productos y servicios;
b) Consumidor (Artículo 2, f III): Consumidor: la persona física o moral que adquiere, realiza o disfruta como destinatario final bienes, productos o servicios. Se entiende también por consumidor a la persona física o moral que adquiera, almacene, utilice o consuma bienes o servicios con objeto de integrarlos en procesos de producción, transformación, comercialización o prestación de servicios a terceros

Lo anterior sirve para conectar que las MiPyMEs pueden ser consumidores o proveedores, y asistentes derechos u obligaciones (separada o concurrentemente) en materia de ciberseguridad.

Al respecto, el Capítulo VIII Bis (artículo 76), relativo a Derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos refiere ciertos derechos vinculados a la seguridad de la información:

> Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
>
> I. El proveedor **utilizará la información** proporcionada por el consumidor en forma **confidencial**, por lo que no podrá **difundirla** o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
> II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar **seguridad y confidencialidad a la información** proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

Como se puede observar, se encuentra establecido como derecho del consumidor la seguridad de la información en relación a los actos de comercio a través de medios electrónicos, ello representa, por otro lado, la obligación de los proveedores.

En el Reglamento de la propia LFPC, ahondando en la materia, contiene un Capítulo relativo a la privacidad y la publicidad, del cual se puede retomar como un referente para evitar el envío de publicidad no solicitada o el uso de información con apego a los procedimientos.[62]

[62] DOF_RLFPC. (2019, diciembre 19). Reglamento de la LFPC. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPC_191219.pdf

Además, recientemente se publicó el Acuerdo por el que se emite el Código de Ética en materia de Comercio Electrónico, el cual no es vinculante, salvo para quien asuma adoptarlo, y contempla algunas referencias a la seguridad de la información:[63]

a) Es de adopción voluntaria y aplicable a las personas físicas y morales, nacionales y extranjeras que ofrece, distribuye, vende, arrienda o concede el uso o disfrute de bienes productos y servicios, en las transacciones, efectuadas a través del uso de medios electrónicos digitales en el territorio nacional.
b) En los Mecanismos de identidad, pago y envio o entrega (artículo 6) refiere a que "Toda tienda virtual o plataforma de comercio electrónico deberá poner a disposición de los consumidores al menos lo siguiente:[64]

…

- El tratamiento que le dará a sus **datos personales**;
- Términos y condiciones a que estarán sujetas las transacciones;
- Métodos de pago y facturación fáciles de usar, implementando **medidas de seguridad** proporcionales a los riesgos relacionados con los pagos, incluyendo los que derivan del acceso o el uso no autorizado de datos personales, prácticas comerciales engañosas y el robo de identidad;

c) Contempla la adopción de los principios generales en materia de protección de datos personales a que refieren la CPEUM y la LFPDPPP, aunado a lo siguiente:

- el proveedor deberá contar con un Aviso de privacidad, como mecanismo accesible, seguro, fácil de entender, con un lenguaje sencillo y claro que permita al Consumidor acceder a toda la información inherente al tratamiento y protección que se dará a sus datos personales.
- Los proveedores deberán incluir en su plataforma o tienda virtual, y en todo el proceso de compra, leyendas de advertencia para que las niñas, niños y adolescentes se abstengan de facilitar sus datos personales, sin la autorización de sus padres o tutores, para que la compra se realice directamente por estos últimos.
- Asimismo, el proveedor está obligado a verificar lo siguiente:
  i. Deberá identificar los contenidos dirigidos únicamente a adultos;
  ii. No deberá incitar directamente a las niñas, niños y adolescentes a la compra de un bien, producto o servicio, aprovechando su inexperiencia o su credulidad, ni a que persuadan a sus padres o tutores, o a los padres o tutores de terceros, para que compren los productos o servicios de que se trate;
  iii. No deberá, sin motivo justificado, exponer a las niñas, niños y adolescentes en situaciones peligrosas;

[63] DOF_Acuerdo Código. (2021, 02 26). Retrieved mayo 2021, from ACUERDO por el que se emite el Código de Ética en materia de Comercio Electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5612351&fecha=26/02/2021
[64] *Ídem*

iv. No publicarán en sus sitios web contenidos, declaraciones o presentaciones visuales ilícitas o que pudieran producir perjuicio mental, moral o físico a las niñas, niños y adolescentes;[65]

Como puede observarse este Código promueve la autorregulación, la protección de datos personales conforme a la legislación aplicable y considera elementos de cultura de ciberseguridad en el entorno del comercio electrónico que favorece la construcción y/o consolidación de la confianza digital.

Cabe señalar que estos ordenamientos no representan el total de los ordenamientos jurídicos aplicables a la seguridad de las empresas u organizaciones. Son algunos de los varios ordenamientos aplicables.

Finalmente, es muy importante que el lector considere la seguridad de la ciberseguridad como algo que cada día es más necesario y está presente en nuestras vidas, nuestras acitivdades, y llegó para quedarse; más vale iniciar el viaje de concientización, informarnos y prepararnos en la materia, pues la inforación está vinculada a los derechos y libertades y será pieda angular para la sociedad del presente y futuro.

3) Consideraciones Finales y Recomendaciones

La ciberseguridad es una condición que e nutre de muchos factores, al igual que la seguridad en el entorno físico. Como ya vimos, la dinámica de la sociedad digital está cada día más vinculada a información y el uso de datos e infomración que se genera con mayor rapidez, precisión, en grandes volúmenes y con tecnología que cuenta con alto potencial de tratamiento.

Todo el cúmulo de datos que generamos como individuos y entes (máquinas o personas morales) así como el uso cada vez más dependiente de tecologías digitales hace que la humanidad incremente su nivel, probabilidad de riesgo e impacto, sto debido al surgimiento constante de nuevas amenazas y más vulnerabilidades que que traerá consigo el Internet de todas las cosas y la carrera constante de la innovación y la digitalización.

Pudimos observar el valor de los activos de información en las organizaciones y cómo todas etán expuestas a ciberataques o a sufrir un incidente de ciberseguridad. Revisamos también que

[65] CPEUM_Congreso de la Unión. (2021). Constitución Política de los Estados Unidos Mexicanos. Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_170521.pdf

existe una amplia gana de conductas delictivas y ciberdelitos, así como una variedad importante de objetivos, motivaciones y tipos de delincuentes.

En el ámbito jurídico, revisamos varios ordenamientos que dan cuenta del avance normativo en diversos sectores y hacia diferentes destinatarios de la norma, sin que fuera exhaustiva.

De todo lo anterior, considero relevante dejar las consideraciones sigueintes, a manera de invitación para emprendedores, MiPyMEs, y hacedores de política pública en la materia:

a) Es urgente una Política Nacional de Ciberseguridad, que considere entre otros grandes ejes de trabajo el fortalecimiento y acompañamiento, en materia de ciberseguridad, para las MiPyMEs, aunado a una política de digitalización de las micro y pequeñas empresas, estrechamente vinculadas con educación y habilidaded digitales.
b) Se requiere visión en emprendedoras y empresarios para considerar la ciberseguridad, en sus diversas aristas, como pilar fundamental para el crecimiento económico y como un tema de alta importancia ante un proceso de digitalización que han iniciado o iniciarán pronto; particularmente en la prevención, la concinetización y la formación.
c) Debemos considerar una revisón de la normativa nacional para simplificar el andamiaje jurídico vinculado a la seguridad de la información y al mismo tiempo bridar más seguridad jurídica en la protección de las activdiades de las organizaciones.
d) Es fundamental fortalecer las capacidades de instituciones públicas que contribuyan a la concientización, educación, prevencion y combate y persecusión de ciberdelitos, así como equipos de respuesta aincidentes que puedan acompañar y asistir a las empresas ante la existencia de un incidente de ciberseguridad.
e) Será positivo que las cámaras empresariales o las grandes empresas realicen esfuerzos solidarios para compartir recursos o experiencias de ciberseguridad para las MiPyMEs en el entendido de que el sector económico es un sistema y parte de la misma cadema, entre todos será más fácil avanzar en forma sostenida por una madurez en ciberseguridad para el sector formal y esto iradiará en otros ámbitos como el público.
f) Sin duda, es igualmente importnate reforzar las campañas de concientización y educación para la prevención de riesgos y delitos para la población en general, usuarios y consumidores. Ninguna acción será exitosa si la población usuaria no está informada de los riesgos, su impacto y por ello debe conocer cóm outoprotegerse.

Existen muchos retos y desafíos en la materia. Por ahora, les invito a dar el primer paso.

4) Bibliografía

- ALAI. (2019, mayo). Recomendaciones para el fortalecimiento del sector fintech en México. Retrieved mayo 2021, from www.ala.lat: https://alai.lat/wp-content/uploads/2019/05/Recomendaciones-para-el-fortalecimiento-del-sector-Fintech-en-Mexico.pdf
- AMVO. (2021). Estudio de Ventas On line. Estudio, Asociación Mexicana de Ventas on line, México.
- BBC News. (2019, septiembre 30). Retrieved mayo 2021, from Qué es el "fraude del CEO" con el que los hackers han robado US$26.000 millones de empresas desde 2016: https://www.bbc.com/mundo/noticias-49878717
- CPEUM_Congreso de la Unión. (2021). Constitución Política de los Estados Unidos Mexicanos. Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_170521.pdf
- Cybersecurity Ventures. (2019). 2019 Official Annual Cybercrime Report. Retrieved Mayo 2021, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
- DOF. (2018, 09 10). DISPOSICIONES de carácter general a que se refiere el Artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera. Retrieved from https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018
- DOF. (2021, 01 28). Retrieved from Disposiciones aplicables a las instituciones de fondos de pago electrónico a que se refieren los artículos 48, segundo párrafo; 54, primer párrafo, y 56, primer y segundo párrafos de la Ley para Regular las Instituciones de Tecnología Financiera: https://dof.gob.mx/nota_detalle.php?codigo=5610487&fecha=28/01/2021
- DOF. (2021). LFPDPPP. Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
- DOF_LeyFintech. (2018, marzo 9). DECRETO por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de

Organizaciones y Act. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

- DOF_LFPC. (1992, 12 24). Retrieved mayo 2021, from Ley Federal de Protección al Consumidor: http://www.diputados.gob.mx/LeyesBiblio/pdf/113_241220.pdf
- DOF_Acuerdo Código. (2021, 02 26). Retrieved mayo 2021, from ACUERDO por el que se emite el Código de Ética en materia de Comercio Electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5612351&fecha=26/02/2021
- DOF_DG. (2018, 09 10). Retrieved mayo 2021, from Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera: https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20car%C3%A1cter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf
- DOF_RLFPC. (2019, diciembre 19). Reglamento de la LFPC. Retrieved mayo 2021, from http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPC_191219.pdf
- DOF_Teletrabajo. (2021, O1 11). DECRETO por el que se reforma el artículo 311 y se adiciona el capítulo XII Bis de la Ley Federal del Trabajo, en materia de Teletrabajo. Retrieved mayo 2021, from Reforma Ley Federal del Trabajo: http://www.diputados.gob.mx/LeyesBiblio/legis/reflxiv/129_LFT_11ene21.doc
- DW. (2021, mayo). Medios: Colonial Pipeline pagó 5 millones a los hackers para rescatar su sistema. Retrieved from https://www.dw.com/es/medios-colonial-pipeline-pag%C3%B3-5-millones-a-los-hackers-para-rescatar-su-sistema/a-57526639
- EL Confidencial. (2021, mayo 23). EL NEGOCIO DEL QUE NADIE QUIERE HABLAR. Retrieved mayo 2021, from Llame al seguro y envíe 8 millones": La gasolina que alimenta el alud de cibersecuestros: https://www.elconfidencial.com/tecnologia/2021-05-23/ransomware-ciberataques-sepe-glovo-aseguradoras_3088831/
- EL Economista. (2021, abril 19). EL Economista. Retrieved mayo 2021, from FBI alerta de “fraudes del CEO” relacionados con criptomonedas: https://www.eleconomista.com.mx/economia/FBI-alerta-de-fraudes-del-CEO-relacionados-con-criptomonedas-20210419-0101.html
- ELLIPTIC. (2021, mayo). DarkSide Ransomware has Netted Over $90 million in Bitcoin. Retrieved mayo 2021, from https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

- FORBES. (2021, abril 21). forbes.com.mx. (L. S. Torre, Producer) Retrieved mayo 2021, from Empresas fintech experimentan el impulso de la pandemia: https://www.forbes.com.mx/foro-empresas-fintech-impulso-pandemia/#:~:text=Para%202021%20se%20espera%20que,digitalizaci%C3%B3n%20derivada%20de%20la%20pandemia.
- Guardia Nacional. (2021, mayo 3). 1era Jornada de Ciberseguridad. Retrieved mayo 2021, from Conferencia de Oliver González Barrales_División General Científica: https://www.facebook.com/udlapjenkinsgs/videos/333104624833555/
- Henriquez, P. (2020, abril 29). COVID-19: ¿Una oportunidad para la transformación digital de las pymes? Retrieved mayo 2021, from https://blogs.iadb.org/innovacion/es/covid-19-oportunidad-transformacion-digital-pymes/
- INCIBE. (2015). GESTIÓN DE RIESGOS. Una guía de aproximación para el empresario. Retrieved mayo 2021, from https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf
- INCIBE. (2017). Retrieved mayo 2021, from Glosario de términos de ciberseguridad. Una Guía de aproximación para el empresario: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
- INCIBE. (2017, 01 19). Fraude del CEO. Retrieved mayo 2021, from https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo
- INCIBE. (2021, febrero). Suplantación de identidad y secuestro de cuentas: ¿cómo actuar? Retrieved mayo 2021, from https://www.osi.es/es/actualidad/blog/2021/02/05/suplantacion-de-identidad-y-secuestro-de-cuentas-como-actuar
- INEGI. CENSO Económico. (2019). CENSO Económico 2019. Retrieved from INEGI: https://www.inegi.org.mx/contenidos/programas/ce/2019/doc/pro_ce2019.pdf
- INEGI-ECOVID-IE. (2020, diciembre). ECOVID-IE Y DEL ESTUDIO SOBRE LA DEMOGRAFÍA DE LOS NEGOCIOS 2020. Retrieved mayo 2021, from Comunicado de Prensa Num. 617/20: https://inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ECOVID-IE_DEMOGNEG.pdf

- INEGI-IFT-SCT. (2021, febrero 17). Comunicado de Prensa número 103. Retrieved 05 2021, from ENDUTIH: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf
- ISO. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Retrieved from ISO27000: https://www.iso27000.es/glosario.html
- ITU. (2010, Noviembre). Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación Resolución 181. Retrieved mayo 2O21, from https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf
- McAfee and CSIS. (2020, Diciembre 7). Uncovers the Hidden Costs of Cybercrime Beyond Economic Impact. Retrieved mayo 2021, from https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629
- MICROSOFT. (2021, enero 26). PyMEs Digitales. Retrieved mayo 2021, from Estudio de PyMEs Digitales: https://news.microsoft.com/es-xl/pymes-mexicanas-83-realizaron-un-cambio-en-su-negocio-debido-al-covid-19/
- MINTIC. (2016). Guía de Gestión de Riesgos, Seguridad y privacidad de la información. Retrieved mayo 2021, from https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf
- Norton. (2019). Retrieved mayo 2021, from Cyber Safety Insights Report Global Results: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_US_Media_Deck.pdf?promocode=DEFAULTWEB%20
- OEA y BID. (2020). Ciberseguridad Riesgos, avances y el camino a seguir en América latina y el Caribe. Retrieved mayo 2021, from Obervatorio ciberseguridad: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
- RLFPDPPP. (2021). Retrieved mayo 2021, from Diputados.gob.mx: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

- SILINK. (2021, abril). EL CIBERCRIMEN AL ALZA: LOS ATAQUES DE RANSOMWARE SE VUELVEN MÁS COMUNES Y EFICIENTES. Retrieved mayo 2021, from Cybercrime: https://www.silikn.com/2021/04/el-cibercrimen-al-alza-los-ataques-de.html
- Téllez Valdés, J. (2013). Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México. Ciudad de México, México: Instituto de Investigaciones Jurídicas de la UNAM. Retrieved mayo 2021, from http://ru.juridicas.unam.mx/xmlui/handle/123456789/12154