
TENDENCIAS 2020
LA TECNOLOGÍA SE ESTÁ VOLVIENDO CADA VEZ MÁS INTELIGENTE. ¿Y NOSOTROS?

# ÍNDICE

# INTRODUCCIÓN

***Dado que los dispositivos son cada vez más inteligentes, es inevitable preguntarse si los usuarios también están adquiriendo la "inteligencia" suficiente para beneficiarse de estos avances tecnológicos sin sufrir percances.***

Año tras año, los especialistas de seguridad de ESET de alrededor del mundo se proponen aventurarse sobre los aspectos de seguridad en torno a los últimos avances de la tecnología. Y dado que es innegable que los dispositivos son cada vez más inteligentes, la pregunta que surge es: ¿están los usuarios siguiendo el paso de los avances tecnológicos en cuanto a la "inteligencia" requerida para aprovecharlos al máximo sin sufrir percances? A lo largo de las cinco secciones de este informe, estaremos repasando diferentes aspectos relacionados a la seguridad, diferentes actores sociales como usuarios, gobiernos y empresas, y conceptos generales como la privacidad, la democracia, la transformación digital y mucho más.

En primer lugar, Tony Anscombe aborda el tema de las elecciones presidenciales de los Estados Unidos y los ecos de las repercusiones que las fake news y las denuncias de interferencias foráneas tuvieron en las elecciones anteriores. Pero no ha sido el único lugar del mundo en el que se ha dado este escenario y casi con certeza, a lo largo de 2020 será un tema que estará en la agenda pública y política, por lo que vale la pena hacer un repaso de cómo la (des)información y las fake news pueden jugar un rol en los procesos democráticos venideros.

En "Machine Learning vs Machine Learning: ¿Creando seguridad o atacándola?", Jake Moore abarca uno de los tópicos de los que más se ha hablado en los últimos tiempos: el machine learning. Este término se ha venido utilizando para diferentes desarrollos tecnológicos, pero en 2019 una de sus aplicaciones cobró relevancia pública con la efímera popularidad que tuvo FaceApp y con el perfeccionamiento de las técnicas de deepfake que se han visto a lo largo del año. ¿Qué implicancias de seguridad tiene el machine learning? ¿Podría ser utilizado para vulnerar la seguridad y privacidad de usuarios y organizaciones?

Todas estas cuestiones están íntimamente relacionadas con la privacidad de los usuarios. En su sección, Lysa Myers revisa cómo está el tema de la privacidad luego de lo que fue el caso de Cambridge Analytica, la implementación de legislaciones a diferentes niveles y qué implicancias para las empresas y gobiernos tendrá el desencanto de los usuarios en torno a la privacidad de sus datos.

La tendencia "Smart" no sólo ha llegado a los objetos que los usuarios utilizan día a día, sino que ya está tomando una escala mayor y podemos ver distintos ejemplos de edificios inteligentes alrededor del mundo, y con la promesa de que pronto las ciudades sean las próximas en incorporarse a esto. ¿Acaso esto podría ocasionar nuevos tipos de ataque que mezclen lo digital y lo físico? ¿Están dadas las condiciones de seguridad para que estas implementaciones se realicen sin poner en riesgo a usuarios/ciudadanos y organizaciones? Cecilia Pastorino desarrolla estas y otras cuestiones en su sección.

Este cambio de paradigma quizás se evidencia más notablemente en los procesos de transformación digital que están corriendo muchas empresas alrededor del mundo, los cuales han desafiado a los equipos de IT a tratar de seguir el ritmo de todos los cambios tecnológicos. Camilo Gutiérrez profundiza sobre esta cuestión y cuáles serán los desafíos para el ámbito corporativo en el futuro cercano.

Una de las herramientas para poder estar preparado para el futuro es estar informado, por lo que los invitamos a que lean el informe completo de Tendencias 2020 para conocer lo que se viene para el 2020 y los años venideros.

# 2020: LA NIEBLA SE ESPESA

- Fake news
- Desinformación dirigida y propaganda
- El proceso de votación
- ¿Desmitificando todo?


**AUTOR**

**Tony Anscombe**

Global Security Evangelist

# 2020: La niebla se espesa

***El 2020 puede ser otro año confuso para el proceso democrático. ¿Qué puede interponerse en nuestro camino al momento de tomar decisiones basadas en hechos?***

A medida que nos acercamos al año 2020, hay una de las predicciones incluidas en este reporte de Tendencias que probablemente esté garantizada: a lo largo del año, habrá reclamos de intrusiones y manipulación de los procesos electorales.

Se trata de asuntos complejos; y si bien es sencillo hacer acusaciones sobre sospechas de alguna interferencia, puede resultar difícil probarlas, más allá de toda duda razonable. La complejidad comienza dada la variedad de tipos de interferencia, que pueden conducir los resultados electorales a cierto desenlace o tal vez a no representar realmente el voto del electorado. Al observar los problemas cibernéticos, o en línea, podemos ver desde fake news y fraude en las máquinas electorales, hasta el aprovechamiento de los grupos más influenciables de la población tomándolos como blanco para el envío de información tendenciosa.

Las elecciones presidenciales de 2016 en Estados Unidos se vieron envueltas en controversias postelectorales, con reclamos de fake news, de interferencia de otras naciones-estado y de la potencial vulneración de los propios procesos de votación. Además, hay quienes afirman que el referéndum del Brexit en el Reino Unido se vio sesgado debido a las intromisiones, y que la desinformación vía WhatsApp posiblemente haya afectado las elecciones de 2018 en Brasil. ¿Podemos esperar que los votantes confíen en el proceso democrático con todos estos factores quitando transparencia a los resultados?

Este capítulo resume algunos de los métodos que sin dudas serán utilizados por individuos, grupos activistas, estados-nación e incluso cibercriminales en 2020, en sus intentos por interferir con los procesos democráticos globales para beneficio propio, sin importa cuál sea este.

## Fake news

El Diccionario Collins designó a este término *Palabra del Año* en 2017. Su salto a la fama tuvo mucho que ver con las elecciones presidenciales de 2016 en Estados Unidos y los continuos reclamos de los candidatos sobre la falsedad de los artículos que aparecían en los medios y de las historias difundidas en redes sociales. El *significado del término* es autoexplicativo y refiere al sensacionalismo o la falsa información que se difunde bajo la apariencia de una cobertura periodística.

Tras las elecciones, Pew Research condujo una *encuesta* sobre las percepciones de las fake news. Los resultados fueron sorprendentes, con el 88% de los estadounidenses asegurando estar amplia o medianamente confundidos sobre los hechos reales, producto de las fake news.

Ofcom, la oficina de Comunicaciones del Reino Unido, lanzó un *reporte* que establece que la mitad de los adultos del Reino Unido recibe noticias vía redes sociales y que el 75% declaró que Facebook es una de esas fuentes. Esto se da a pesar de que en el reporte se considera a las redes sociales como parciales, poco confiables e imprecisas. La televisión se mantuvo como el medio más utilizado, con un 75% de los adultos encuestados mencionándola entre sus fuentes de noticias, pero la influencia de las redes sociales no debería subestimarse y ha llegado para quedarse.

Hay distintos tipos de fake news: para obtener ganancias, para beneficio político, para el crimen, para realizar engaños y para bromas virales. Incluso pueden combinarse: crear un engaño que ponga a un candidato político en el foco puede generar un beneficio político, y con la publicidad "correcta" alrededor de la historia, puede hasta generarse ganancias. Si los creadores de dichas campañas pudieran ser identificados, es probable que hayan cometido un crimen, pero identificar la fuente no siempre es posible.

En el camino hacia la elección general del Reino Unido en 2019, una organización de investigaciones y consultoría, Future Advocacy, junto a un artista inglés, Bill Posters, creó un video falso para redes sociales, también llamado "deepfake". El video muestra a los principales candidatos aparentemente respaldándose los unos a los otros para el cargo de Primer Ministro. Este ejemplo de fake news fue creado en un intento por demostrar la dificultad de identificar lo real de lo falso, y que la democracia está potencialmente siendo debilitada.

Pero el problema no es nuevo. Frecuentemente leo las portadas de las revistas cuando llego a la caja en el supermercado de mi barrio: celebridades que se separan, integrantes de la Familia Real del Reino Unido divorciándose, o alienígenas que aterrizan en el estacionamiento. Con algo de suerte, los lectores de dichas revistas sabrán que esas historias son falsas cuando eligen adquirirlas, pero cuando vamos a las historias en Internet, que se difunden rápidamente y a audiencias mucho más amplias, no resulta sencillo distinguir el bien del mal.

Algunas redes sociales y buscadores en línea están intentando combatir este problema de forma responsable, bajo la presión de enojos públicos y políticos. Por ejemplo, Twitter ha anunciado recientemente la prohibición de todo tipo de campaña política paga sobre candidatos, elecciones y asuntos relacionados a política en la previa de las elecciones presidenciales de 2020 en Estados Unidos. Pero este es un tema complejo al que incluso se han referido como una violación a la libertad de expresión si alguien se ve privado de la posibilidad de publicar avisos con cierto punto de vista. En realidad, con la difusión de las fake news, las impresiones aumentan y se obtienen ingresos por publicidad, y no todos los actores que muestran publicidad en sitios web son responsables.

El problema está en la velocidad en que se propaga la desinformación – una historia que aparezca en la próxima hora se difundirá rápidamente, especialmente si su creador la promociona y comparte desde múltiples cuentas y redes al mismo tiempo. Las compañías responsables de las plataformas han innovado en los métodos de detección y creado mecanismos de reporte para que, cuando resulte posible, se detecten automáticamente o se permita a los usuarios que reporten estas noticias falsas. Confiar en los reportes, sin embargo, es una solución a medias cuando la desinformación ya se ha difundido. Por ello, es probable que muchos usuarios no den ese paso extra para reportarla, y es poco probable que aquellos que han sido testigos (y quizás han sido influenciados) de la desinformación sean conscientes de su retracción.

Como profesional en ciberseguridad, considero a las fake news que dañan la democracia como maliciosas – tanto como las intrusiones de malware en tus dispositivos. Es necesario que haya soluciones tecnológicas más robustas para frenar la difusión de fake news apenas aparecen y cortarlas de raíz, de la misma manera en que los exploits zero-day son detectados por productos antimalware. Con la adopción de machine learning, es probable que salgan al mercado algunas soluciones novedosas que detectarán y frenarán o eliminarán al menos algunas de las fake news antes de que lleguen al usuario.

La educación es también una solución de largo término para este problema, pero los resultados son más lentos. En julio de 2019, el gobierno británico publicó una nueva guía de seguridad para escuelas; parte de está política actualizada establece que cada niño aprenderá acerca del sesgo de confirmación y los riesgos en línea como parte obligatoria de la currícula escolar. Esto ayudará a que los estudiantes conozcan técnicas utilizadas para la persuasión y para identificar fake news y aprender sobre sus riesgos, pero tomará muchos años hasta que una generación entera distinga entre lo real y lo falso. (Mi colega, Jake Moore, habla del espectro de deepfakes en otro capítulo de este reporte titulado "Machine Learning vs Machine Learning: ¿Creando seguridad o atacándola?"). Sin embargo, entender qué es real y qué es falso dará a la siguiente generación confianza en el sistema electoral democrático. Son más los gobiernos que tienden a tomar esta postura proactiva y añadir esto a sus políticas educativas. Si no lo hacen, deberían.

## Desinformación dirigida y propaganda

El abuso de datos personales de Cambridge Analytica asombró al mundo, pero no sorprendió a los que siempre lo hemos dicho – "si no pagas por ello, entonces tú eres el producto"; por ejemplo, cada usuario de Facebook en Estados Unidos y Canadá *genera más de US$130 dólares* para la compañía por año. Eventualmente, el escándalo se hizo público cuando tres nuevas organizaciones combinaron recursos y causaron la tracción suficiente para que cualquiera lo notara – tras más de dos años.

Avanzamos un poco en la historia; Facebook fue multado con US$5 mil millones por la Comisión Federal de Comercio (FTC, por sus siglas en inglés) por su participación en la brecha de datos. No estoy seguro de poder describirlo como una brecha, aunque los documentos, que ahora son de dominio público, muestran que Facebook sabía qué estaba sucediendo – fue más un abuso de confianza para obtener ganancia económica. El día que la FTC anunció la multa de Facebook, el precio de las acciones de la red social subieron – está claro que el mercado esperaba que la pena fuera más dura o comprendió que el acuerdo con la FTC fue en realidad a favor de Facebook.
El uso de la información como arma, ya sea desinformación o propaganda, continuará y tomará distintos cami-

nos a medida que los benefactores exploran y adoptan nuevos métodos para atacar la democracia u obtener dinero. En el centro de este asunto invasivo y silencioso está la minería de datos, algo que no podemos ver y es difícil de comprender para muchos.

Los puntos de información disponibles acerca de individuos, considerando que la mayoría de las personas *comparte demasiado en redes sociales*, son varios. La habilidad para ajustar y manipular el mensaje enviado a un sujeto está accionado por la tecnología, que permite individualizar los mensajes enviados a millones de personas, todo con solo un clic.

## El proceso de votación

Este tampoco es un asunto nuevo e involucra tanto al sistema de votación tradicional en papel como al electrónico. Además, es un problema que no parece estar por resolverse pronto.

Muchos estados de Estados Unidos han gastado millones de dólares para mejorar los sistemas que serán utilizados en las elecciones de 2020. Uno de ellos, Pensilvania, ha recibido *US$14 millones para optimizar sus sistemas electorales*, pero incluso éstos pueden ser vulnerables debido al sistema operativo, Windows 7, que – a no ser que se pague una tasa – no recibirá más parches de Microsoft una vez que esta versión del sistema operativo alcance el fin de su ciclo de vida en enero de 2020, once meses antes de las elecciones presidenciales en Estados Unidos.

En la conferencia DEF CON número 27, realizada en agosto de 2019, se realizaron desafíos en tiempo real para hallar *vulnerabilidades en sistemas electorales*. Uno de esos experimentos halló vulnerabilidades en un sistema de marcado de boletas. En esta instancia, el atacante tenía acceso total y conexión directa a los dispositivos, algo que jamás debería suceder en el mundo real. Espero que alguien esté en condiciones de notar si un atacante desarma una terminal y conecta cables a ella. Sin embargo, esto sí depende de que los dispositivos estén asegurados en el plano físico antes y durante el proceso electoral, lo cual, en algunas instancias previas a las elecciones, no ha sido el caso. Ello puede también perder relevancia si los dispositivos quedan separados y nunca son conectados a una red pública. Si bien hay muchos dispositivos que en teoría podrían ser vulnerables, esto no necesariamente significa que pueden ser o serán explotados.

Está claro que las soluciones tecnológicas para el registro y la votación seguirán teniendo problemas. Si constantemente somos testigos de masivas brechas de datos y sistemas comprometidos en compañías y departamentos gubernamentales, ¿por qué deberíamos creer que los sistemas o procesos de votación están excentos de ataques similares? La buena noticia es que las elecciones presidenciales de 2016 en Estados Unidos generaron una mayor conciencia sobre posibles vulnerabilidades en los sistemas electorales utilizados, lo cual derivó en una directa asignación de presupuesto y en la comprensión de la necesidad de que los sistemas fueran asegurados por naturaleza.

## ¿Desmitificando todo?

En 2020 se llevarán a cabo numerosas elecciones alrededor del mundo y habrá incontables inconvenientes en sus sistemas y procesos, tanto tecnológicos como físicos. Es de esperar que se haga uso de todos los métodos aquí mencionados, pero la pregunta es a qué escala serán utilizados y si la interferencia modificará los resultados.

Como votantes, y espero que también como creyentes en la democracia, pondremos presión a las compañías que distribuyen fake news y desinformación para que detecten y cesen con esta práctica. Sin embargo, las altas ganancias percibidas por estas prácticas y la falta de compromiso de los consumidores, probablemente signifique que seguiremos viendo una ola de desinformación, ya sea parcialmente engañosa o completamente fabricada.

Así como con muchas otras prácticas cuestionables, como el abuso de la privacidad de los consumidores que hemos experimentado durante los últimos 10 años, sin intervención del gobierno ni regulaciones o legislaciones, seguiremos insistiendo hasta que estas prácticas ya no puedan ser toleradas. Pero no esperen que suceda en los próximos 12 meses.

# MACHINE LEARNING VS. MACHINE LEARNING: ¿CREANDO SEGURIDAD O ATACÁNDOLA?

- Engañando al ojo humano
- Engañando al algoritmo
- ¿Una oportunidad o una pesadilla?


**AUTOR**

**Jake Moore**

Security Specialist

# Machine Learning vs. Machine Learning: ¿Creando seguridad o atacándola?

***Los avances en machine learning han aportado considerables beneficios a los defensores de la ciberseguridad, pero su potencial no pasa desapercibido para quienes buscan utilizarlo con malas intenciones.***

El aprendizaje automático o "machine learning" (ML) está, sin dudas, cambiando nuestras vidas. El aumento de poder de cómputo y el uso de grandes almacenes de datos está mejorando rápidamente nuestras capacidades en múltiples industrias. Además, si el primo lejano del ML, conocido como la verdadera Inteligencia Artificial (IA), también despega y las computadoras empiezan a "pensar por sí mismas", estaremos frente a un futuro maravilloso donde mucho de lo que antes se creía inimaginable podría llegar a ser posible. Por ahora, sin embargo, la IA autosostenible todavía parece estar muy lejos, mientras que el ML está avanzando en uno de los desarrollos tecnológicos más emocionantes de la historia.

El ML también ha aportado varios *beneficios a los ciberdefensores*, incluyendo un escaneo eficiente, una detección más rápida y mejoras en la capacidad de detectar anomalías. De hecho, algunas empresas de ciberseguridad han estado aprovechando esta tecnología durante años para mejorar las capacidades de detección de sus productos.

Sin embargo, ¿qué pasa si el ML se utiliza indebidamente para atacarnos a nosotros y a los sistemas que hemos creado? No es difícil comprender por qué y cómo el malware basado en ML (o incluso en AI) puede ofrecer nuevos y únicos vectores de ataque, más potentes de lo que estamos acostumbrados actualmente. Está quedando claro, entonces, que el ML será un componente importante en la batalla futura.

Esta tecnología también ha avanzado a pasos agigantados en otras aplicaciones. En este capítulo de Tendencias, por tanto, nos centraremos en dos maneras en las que los algoritmos de ML podrían utilizarse como instrumentos para causar daño.

## Engañando al ojo humano

Seguramente has visto uno de los tantos y convincentes videos de intercambio de rostros que aparecen en Internet, especialmente en redes sociales. Tales deepfakes –videos, audios o imágenes manipuladas y diseñadas para reproducir el aspecto y el sonido de seres humanos reales– pueden parecer desconcertantemente legítimos e incluso chocantes. De hecho, con frecuencia los deepfakes involucran a celebridades o figuras públicas en comportamientos inesperados o en comentarios escandalosos que normalmente no son respaldadas por ellos.

Los deepfakes están aumentando en calidad a un ritmo impresionante, como se puede ver en *videos como éste* en el que a un Barack Obama generado se le escucha decir cosas que el verdadero no dijo. Además, cuando uno observa a *Bill Hader* siendo transformado sin esfuerzo en Tom Cruise y en Seth Rogan, es cuando se da cuenta de que podemos tener un gran problema en nuestras manos a menos que se aborde esta amenaza. Como con cualquier cosa en Internet, el futuro podría llevar a que esta tecnología se utilice para dañar a las figuras públicas haciendo que parezca que dicen lo que el creador quiere, ya sea para dañar a la sociedad o incluso para manipular procesos electorales alrededor del mundo.

¿Estamos preparados para el impacto real de los deepfakes? Con escándalos políticos, seudónimos y escenarios casi inimaginables que involucran videos falsos, es posible que, sin darnos cuenta, estemos ante el comienzo de una epidemia en la que la línea entre la verdad y la mentira sea imposible de determinar. ¿Qué impacto social podrían tener las deepfakes en la sociedad? A la luz de lo que fue el escándalo de Cambridge Analytica en el que los científicos de datos fueron capaces de transformar encuestas y datos de gráficos sociales de Facebook en un arma de mensajería política a través de la elaboración de perfiles psicográficos, parece que los deepfakes podrían acelerar el proceso de influir en el público de cara a las elecciones. ¿Llegará un momento en el que ni siquiera confiaremos en lo que vemos y escuchamos?

Después de lo que fue el efímero auge de FaceApp, la app que envejece rostros, surgió la pregunta de si algún día se podrían crear vídeos de personas sin su conocimiento. La realidad es que se necesitan muchos datos (muchas fotos, vídeos y grabaciones de voz) incluso para hacer un clip corto de un deepfake donde el creador tiene el control de lo que se dice. Además, obtener una cantidad significativa de datos sobre una figura no pública es una tarea en sí misma. Sin embargo, esto es sólo si pensamos en el 2019, pero ¿qué pasa si pensamos el año que viene o en una década? ¿Se podrá en el futuro crear un deepfake a partir de una o dos historias cortas de Instagram que sea creíble por la mayoría de nuestros contactos? Considero que esto es lo que sucederá en el futuro y que existirá una aplicación en nuestros teléfonos que permitirá crear estos deepfakes de forma natural y sin esfuerzo.

Durante la próxima década veremos videos falsos que involucrarán a figuras públicas y que antes nos hubieran parecido inimaginables. Pero, además, con el tiempo veremos que estos videos incluirán a personas más cercanas a nosotros, como pueden ser colegas, compañeros o familiares. No cabe duda de que los sitios pornográficos explotarán a las celebridades sin su consentimiento, así como también que los ciberdelincuentes utilizarán esta tecnología para engañar a sus víctimas. Los deepfakes lograrán que algunos de nosotros incluso no confiemos en nada, por más que nuestros sentidos nos digan que estamos ante un contenido verdadero.

Entonces, ¿qué se puede hacer para estar preparado ante esta amenaza? Primero, necesitamos educar mejor a la gente acerca de la existencia de los deepfakes. La gente tendrá que aprender a tratar con cierto grado de escepticismo incluso a los vídeos más realistas. Además, y aunque es una tarea difícil, se necesita desarrollar una tecnología que detecte mejor los deepfakes. Aunque el machine learning es una pieza central en la creación de estos contenidos falsos, es necesario crear algo que actúe como antídoto y que sea capaz de detectarlos sin depender únicamente de la intuición humana. Además, las plataformas sociales deberán reconocer y abordar esta potencial amenaza tan pronto como sea posible, ya que es a través de estas plataformas donde es más probable que se difundan y tengan un impacto perjudicial en la sociedad.

## Engañando al algoritmo

El reconocimiento facial es cada vez más frecuente en la tecnología actual. Si bien la implementación del reconocimiento facial puede que todavía no sea 100% exacta, estamos recién en 2019 y las cosas sólo pueden mejorar, ¿verdad?

Algunas ciudades en Estados Unidos han prohibido que el reconocimiento facial sea utilizado por las fuerzas del orden después de que se utilizara para identificar, erróneamente, a 26 personas como criminales cuando en realidad se trataba de ciudadanos respetuosos de la ley. De hecho, una investigación de la Oficina de Responsabilidad Gubernamental del Gobierno de los Estados Unidos encontró que los algoritmos del FBI eran inexactos el 14% de las veces, además de ser más propensos a identificar erróneamente a las personas según sus etnias y a las mujeres. Además, Microsoft se ha negado recientemente a instalar tecnología de reconocimiento facial para una fuerza policial estadounidense, debido a la preocupación por el sesgo de la tecnología machine learning. En estos casos los datos han sido introducidos por humanos, quienes tienen una variedad de sesgos no intencionales que influyen en el resultado del machine learning.

Sin embargo, hay argumentos a favor de que el reconocimiento facial se extienda por todas partes y se instale junto a los millones de cámaras de vigilancia que ya están capturando casi todos nuestros movimientos en público. Por ejemplo, si se toma el reconocimiento facial en su forma básica fundamental, ofrece una forma de recopilar información sobre quién ha estado y dónde en un momento dado. Esto no es tan diferente a lo que puede realizar un buen oficial de policía que es capaz de reconocer a un criminal local dentro de su área de operaciones (conozco a algunos oficiales de policía que pueden hacer esto - tienen recuerdos increíbles). Por lo tanto, si el reconocimiento facial con el tiempo puede llegar a ser casi 100% exacto, entonces puede estar vigilando cada uno de nuestros movimientos pronto.

Pero si las fuerzas del orden son capaces de dar con el paradero de delincuentes y de sospechosos, ¿qué pasará con los delincuentes que utilicen el software a su favor o que roben enormes bases de datos que contienen información de localización confidencial? Es posible que las bases de datos de los rostros de las personas puedan ser comprometidas, lo que significaría que las técnicas de verificación, como el reconocimiento facial o de voz, podrían ser engañadas y, por lo tanto, la seguridad de múltiples capas sería evadible.

## ¿Una oportunidad o una pesadilla?

Vendrán ataques complejos basados en machine learning y no debemos olvidar que, debido a la escala de poder que utilizarán, muchos de estos ataques son actualmente insondables, por lo que tienen el potencial de ser más grandes de lo que podemos anticipar. Por lo tanto, como es posible que los atacantes hagan uso de forma maliciosa del aprendizaje automático, debemos estar preparados y ser conscientes de cómo combatir tales ataques, ya que tendrán la capacidad de aprender lo que funcionó y lo que no funcionó sobre la marcha y luego volver a entrenarse a sí mismos con el fin de superar las defensas existentes. Los defensores de la seguridad informática necesitan entender cómo se crearán estos ataques basados en machine learning, cuáles podrían ser sus capacidades y unirse para hacerles frente.

# CAMBIOS SUSTANCIALES EN MATERIA DE PRIVACIDAD

- Diseño al servicio de la privacidad y la seguridad
- Mejorar la tecnología publicitaria
- Consecuencias legislativas en caso de abuso de confianza
- Mejorar la autenticación y la verificación
- Cambiemos el rumbo

**AUTORA**

**Lysa Myers**

ESET Senior Security Researcher

# Cambios sustanciales en materia de privacidad

***La confianza en nuestro entorno digital no ha tenido una buena racha últimamente, y cada vez más gente está preocupada por la seguridad de sus datos. ¿Qué se ha hecho y qué queda por hacer para que la marea cambie?***

Algo que ocurre cuando has estado un largo tiempo hablando acerca de seguridad y privacidad es que habrás hecho predicciones sobre cómo será el escenario de las amenazas en el futuro, y habrá pasado el tiempo suficiente para que puedas comprobar lo acertadas que fueron tus propias predicciones.

En la mayoría de los casos, esto sucede en la escala del futuro cercano, como es el caso de este capítulo de Tendencias; aunque a veces está en la escala de una década o más. En mi propia experiencia con respecto a este fenómeno he notado algunos cambios importantes que, en su gran mayoría, giran en torno a la ganancia o la pérdida de la confianza de nuestro entorno online compartido.

Mientras decidía qué escribir para este capítulo, busqué en Internet la frase "año de privacidad" y añadí a la búsqueda un año reciente; por ejemplo, "año de privacidad 2018". Los titulares que incluyen esta frase pueden ser un buen indicador de que los autores de estas noticias pensaron que se avecinaba un gran cambio en cuanto a la percepción pública de la privacidad, ya sea positiva o negativa. Creo que la primera vez que predije que algo de eso sucedería fue durante la revisión del año 2013, así que tenía curiosidad de saber cuántas veces se había dicho algo similar. Por cada año entre 2009 y 2015, esos términos de búsqueda arrojaron más de un millón de resultados. Después de ese período se redujo la cantidad y cada año arrojó "solo" entre ochocientos y novecientos mil resultados.

¿Este descenso significa que el 2016 fue el año en el que mucha gente, de manera colectiva, abandonó toda esperanza de tener control sobre su información personal? De alguna manera, esto puede haber sido así; parece haber habido un cierto sentido de resignación colectiva. Pero también parece como si hubiéramos llegado al punto en el que los legisladores y los jueces comenzaron a ponerse al día con la ira colectiva provocada por un constante aluvión de errores e infracciones en materia de privacidad.

Y ese aluvión ha continuado – sólo en 2019, hemos visto a bastantes *países* y estados de EE.UU. *aprobar o implementar leyes de notificación de violaciones nuevas o ampliadas*. También hemos visto que varios estados de EE.UU. promulgaron legislaciones sobre privacidad de datos (aunque sólo en California se aprobó esta legislación), que se han impuesto varias multas importantes a las empresas responsables de *recientes brechas de datos* (aunque se considera que, en general, se trata de meras palmadas en la muñeca), y que ejecutivos de *compañías que sufrieron brechas* han tenido que testificar ante audiencias del Congreso sobre estos incidentes.

El cambio ha sido lento, y podría decirse que estos esfuerzos aún no han supuesto una gran diferencia positiva. El consenso general entre gran parte de la población estadounidense es que sienten que *no pueden confiar* en las empresas para proteger sus datos, y este es el caso también en *otros países*. Esta situación, junto con el fraude desenfrenado y otros tipos de tráfico malicioso, ha creado un entorno de "*baja confianza*" en el que estamos cada vez más interconectados pero nos sentimos cada vez más inseguros. Cuando tenemos que abordar todo en Internet con paranoia y escepticismo, la gente se siente comprensiblemente reacia a participar en ello.

En materia de seguridad, a menudo decimos que una buena práctica es "confiar, pero verificar": en la situación en la que nos encontramos ahora, la desconfianza es generalizada y los métodos de verificación están repletos de fallos. Hasta que no solucionemos esto, Internet seguirá siendo un lugar aterrador para la mayoría de las personas.

Entonces, ¿qué tenemos que hacer para salir de esta omnipresente sensación de desconfianza?

## Diseño al servicio de la privacidad y la seguridad

Una de las cosas más importantes que hay que hacer para mejorar la confianza de los clientes es crear productos y servicios tecnológicos que se diseñen teniendo en cuenta la seguridad y la privacidad desde el inicio. La Asociación Internacional de Profesionales de la Privacidad (IAPP, por sus siglas en inglés) ha creado un documento que resume sus recomendaciones para los principios de *Privacidad por Diseño*.

Muchas de las cosas que se mencionan en este documento son las que uno podría esperar: ganarse la confianza a través de la apertura y la transparencia, promulgando una seguridad de extremo a extremo, creando políticas que establezcan la responsabilidad del negocio y obteniendo el consentimiento continuo de clientes que son informados de la manera correcta. Pero hay una recomendación más que cabe destacar y que puede sorprender a muchas personas: permitir la plena funcionalidad respetando la privacidad, de tal manera que beneficie tanto a la empresa como al usuario.

Debido a que el modelo actual para gran parte de la Internet es utilizar los datos de los clientes como un producto que se vende, esta recomendación en particular puede requerir un pensamiento verdaderamente innovador; y probablemente, las empresas que logren esta hazaña tendrán una ventaja competitiva en el mercado.

## Mejorar la tecnología publicitaria

Ya que estamos en el tema de la venta de datos de clientes, también deberíamos discutir las mejoras necesarias en la tecnología publicitaria. En *una encuesta* reciente, menos del 20% de los participantes consideró que los anuncios dirigidos tenían un comportamiento ético. En *otras encuestas*, se descubrió que en algunos casos los anuncios dirigidos podían resultar contraproducentes y provocar una menor interacción con el cliente.

A las empresas que utilizan tácticas de venta de alta presión, como la *escasez y la prueba social*, tampoco les va bien. Una encuesta en Reino Unido reportó que casi la mitad de los participantes dijo que este comportamiento los haría desconfiar de la compañía. Un tercio expresó una reacción emocional negativa (como disgusto o desprecio). Y el 40% informó que estas tácticas les harían querer hacer lo contrario de cualquier acción que se estuviera sugiriendo.

Cuanto más a menudo nos bombardean con tácticas de venta de alta presión y tácticas de monitoreo agresivas, más rápidamente se reduce su (muy limitada) eficacia. Dado que muchos profesionales del marketing han hecho un uso excesivo de estas estrategias, es probable que hayan limitado las oportunidades para otras empresas. Necesitamos formas más efectivas de comercialización que sean honestas, transparentes y respetuosas con nuestros potenciales clientes.

## Consecuencias legislativas en caso de abuso de confianza

Es poco probable que mejore el sentimiento de desconfianza de las personas hacia las compañías tecnológicas hasta que no exista la sensación de que pueden perder tanto como sus clientes cuando se produce un incidente de privacidad. Aunque las recientes multas por violación a la privacidad en los Estados Unidos y el Reino Unido están batiendo récords, el impacto económico de estas sanciones es muy poco significativo en relación a los ingresos que obtienen las grandes empresas a partir de la utilización de nuestros datos. Hasta que estas multas no se acerquen a cifras que comprometan más los *ingresos de una empresa*, estas sanciones seguirán siendo más disuasivas para las pequeñas empresas que para las grandes corporaciones.

## Mejorar la autenticación y la verificación

Los nombres de usuario y las contraseñas simplemente ya no son suficientes para mantener segura la identidad de las personas. Esto puede disminuir la confianza tanto de los propietarios de cuentas en línea como de las personas que interactúan con cuentas potencialmente secuestradas. La autenticación multifactorial *mejora significativamente* esta situación, pero *muy pocas personas* la han adoptado hasta el momento. Para cambiar esto necesitaremos una *mejor educación* sobre esta tecnología, que más empresas *ofrezcan incentivos* para usarla, así como mejoras continuas en su usabilidad.

## Cambiemos el rumbo

Hace poco más de diez años me pidieron por primera vez que predijera el estado de la seguridad en Internet para la próxima década. En esa oportunidad recuerdo decir que veía que las cosas iban en dos posibles direcciones: o bien comenzábamos a comprender de manera colectiva lo que ocurría y las cosas mejoraban, o bien continuábamos postergando esta decisión e Internet se convertiría en una larga pila de residuos inutilizables. Aunque nadie podría argumentar con éxito que la gente está utilizando Internet menos de lo que lo hacía hace diez años, sí es cierto que ahora debemos navegar en Internet a través de una mayor cantidad de información residual que la que había en la década de los años 2000.

Aquellos veteranos que han estado trabajando en ciberseguridad desde los primeros días de la industria y que han estado viviendo en este estado de desconfianza durante décadas; han visto que Internet se construyó sobre bases inestables que hicieron poco (o nada) para prevenir el mal uso. Afortunadamente, también han estado pensando -y hablando- sobre lo que hay que hacer para solucionarlo. No es demasiado tarde para tomar medidas significativas que apunten los esfuerzos de privacidad en la dirección correcta. Es mi esperanza que el deseo de cambios necesarios continúe creciendo, de forma que podamos llevar adelante esos cambios antes de que haya transcurrido mi próxima década en esta industria.

# 4

# DE DISPOSITIVOS IoT A EDIFICIOS Y CIUDADES INTELIGENTES: "SMART IS THE NEW SEXY"

- Edificios Inteligentes
- Ciudades inteligentes
- Ataques a infraestructuras inteligentes
- Malware
- Robo de Identidad
- Robo de información crítica


**AUTORA**

**Cecilia Pastorino**

Security Researcher

# De dispositivos IoT a edificios y ciudades inteligentes: "Smart is the new sexy"

***A medida que más y más ciudades incorporan tecnología inteligente que cambia la forma en que los municipios gestionan sus operaciones y servicios básicos, ¿qué impacto tienen estos desarrollos desde la perspectiva de la seguridad?***

Desde 1994, con la aparición del primer teléfono inteligente, esta palabra ha sido utilizada en los años siguientes para definir a todo dispositivo que potencia sus funciones a través de un software y una conexión a Internet. En el año 2009, Kevin Ashton, cofundador del Auto-ID Center del MIT, fue quien utilizó por primera vez la expresión Internet of Things (IoT) de forma pública y desde entonces, el crecimiento y la expectativa alrededor del término ha ido en aumento de forma exponencial.

La década del 2010 se caracteriza por la revolución de la Internet de las cosas con la aparición de relojes, termostatos, luces, cerraduras, cámaras, juguetes, heladeras y todo tipo de dispositivos inteligentes que alguien pueda imaginar y que luego pasan a ser parte de casas, oficinas, edificios y hasta ciudades inteligentes.

Hoy en día, el potencial de la Internet de las cosas no solo está en la automatización de tareas, sino también en el proceso analítico que se puede realizar de los grandes volúmenes de información generada. Las estructuras inteligentes aprovechan una variedad de tecnologías interdependientes, tales como Inteligencia Artificial (IA), redes inalámbricas de banda ancha, computación en la nube, sensores y dispositivos IoT. La gran cantidad de información generada por los sensores y dispositivos de la red es almacenada en grandes bases de datos y procesada por tecnologías de inteligencia artificial y análisis de datos con el objetivo de mejorar la eficiencia operativa y fomentar un ambiente seguro y productivo. Estas características son las que llevan a estos sistemas a ser llamados inteligentes. Sin embargo, dado que inteligente no siempre significa seguro y que la tecnología avanza a pasos agigantados, unos pocos nos preguntamos cuándo finalmente la seguridad acompañará estos avances desde el diseño.

## Edificios Inteligentes

Los edificios inteligentes utilizan tecnología para controlar distintas variables que forman parte del entorno con el objetivo de brindar mayor confort, contribuir a la salud y a la productividad de quienes trabajan o habitan en ellos. Para realizar esto, utilizan lo que se conoce como Sistemas de Automatización de Edificios, conocido en inglés como BAS. A partir de dispositivos IoT, como sensores de iluminación y/o temperatura, cámaras, controles de acceso, etc., estas construcciones son capaces de analizar, predecir, diagnosticar y mantener los distintos ambientes, así como también automatizar procesos y monitorear en tiempo real diferentes variables. Algunos ejemplos son la temperatura ambiente, la iluminación, el sistema de cámaras de seguridad, los ascensores, el estacionamiento, el suministro de agua, entre tantas otras.

Las ventajas de la implementación de dispositivos inteligentes son amplias. Por ejemplo, tal como *explicó* Tony Anscombe en una conferencia en la que abordó el tema de la seguridad en edificios inteligentes, un reconocido hotel la ciudad de Las Vegas colocó un sistema de automatización para el aire acondicionado que solo encendía la refrigeración cuando había ocupantes. Esta decisión representó en el primer año de la instalación del sistema inteligente un ahorro de aproximadamente dos millones de dólares gracias al ahorro energético que significó la automatización de este proceso. Por otro lado, un supermercado en Reino Unido *instaló* en su estacionamiento un sistema inteligente que aprovecha la circulación de los automóviles para generar energía, que luego es utilizada para alimentar sus cajas registradoras.

## Ciudades inteligentes

En la edición 2019 de la "*Consumer Electronics Show*" se mostraron distintas iniciativas de ciudades inteligentes que se están implementando (o planificando) en todo el mundo. Algunas de ellas dedicadas a mejorar el transporte a través de sensores que evalúan los flujos de tráfico, y en base a estas mediciones manejan el control de semáforos. Otras dedicadas a automatizar la iluminación en base a sensores de luz, medir la temperatura, agregar sistemas de monitoreo a través de redes de cámaras y muchos otros sensores para recolectar información que luego será analizada en alguna central con el objetivo de saber todo lo que está ocurriendo en la ciudad. Al igual que en los edificios inteligentes, pero a gran escala, a partir de información recopilada proveniente de sensores y dispositivos se utiliza el aprendizaje automático para analizar estos datos y automatizar servicios de forma eficiente.

El problema es que muchas de estas ciudades están apenas preparadas para gestionar de forma segura los grandes volúmenes de información que implican estos sistemas y un atacante podría fácilmente obtener acceso a los sensores, modificar mediciones y alterar servicios de transporte, tráfico, iluminación u otras infraestructuras críticas. Ya hemos visto pruebas de concepto de diferentes ataques a ciudades inteligentes y *sistemas automatizados* en conferencias internacionales como *Black Hat* o Defcon, por lo que en cualquier momento estos ejemplos en ambientes controlados podrían volverse una realidad. Además, si ciudades como Atlanta en Estados Unidos, que tiene como *proyecto convertirse en una ciudad inteligente líder a nivel mundial*, no ha sabido cómo evitar amenazas ya existentes como el *ransomware*, ¿por qué creer que están preparadas para afrontar desafíos mayores? De hecho, en la conferencia Smart City Expo que se llevó a cabo en septiembre de 2019 en esa misma ciudad, especialistas manifestaron su preocupación dado que el *rápido crecimiento de las ciudades inteligentes no está siendo acompasado por la capacidad de convertirlas en seguras*, por lo que se hace necesario reevaluar la forma de abordar la seguridad para este tipo de ciudades.

## Ataques a infraestructuras inteligentes

Si bien pareciera que los ataques a edificios o ciudades inteligentes solo pueden realizarse a través de elaborados planes dirigidos en el que los cibercriminales apuntan a un objetivo específico, lo cierto es que muchos sistemas de automatización de edificios (BAS), así como también sensores y dispositivos de ciudades inteligentes, se encuentran directamente expuestos a Internet. Actualmente se pueden encontrar en buscadores como Shodan o Cencys mas de 35.000 sistemas BAS y otros tantos cientos de miles de dispositivos críticos al alcance público en Internet a nivel mundial.

Muchos de estos dispositivos o sistemas no tienen una autenticación lo suficientemente fuerte ni protección contra ataques de fuerza bruta, no se encuentran actualizados, no están protegidos con soluciones de seguridad o simplemente tienen configuraciones inseguras que podrían permitirle a un atacante tomar control del equipo.

## Malware

Si bien los sistemas de ciudades o edificios inteligentes no navegan por la web ni abren correos electrónicos, aún deben protegerse contra el malware que podría brindarle acceso un cibercriminal a información crítica o causar daños en el equipo.

La propagación de códigos maliciosos puede darse a través de puertos expuestos a Internet, vulnerabilidades en los sistemas o incluso a través de un acceso físico a puertos USB no protegidos o al alcance de cualquier transeúnte. Tampoco hay que descuidar la protección de la red, especialmente aquella a la que se conectarán dispositivos personales de usuarios que podrían estar comprometidos.

Dentro de los múltiples códigos maliciosos que podrían atacar los sistemas informáticos de edificios o ciudades inteligentes, podríamos destacar a los que utilizan una botnet como herramienta, especialmente teniendo en cuenta casos recientes de botnets apuntadas a dispositivos IoT, *como una nueva variante de la botnet Mirai* o el pasado *ataque a equipos Mikrotik* con el objetivo de minar criptomonedas. ¿Será que en un futuro no muy lejano los dispositivos IoT de una ciudad entera podrían ser utilizados por un atacante para la minería de criptomonedas? Sin dudas que el *cryptojacking* es una de las amenazas que podría afectar a infraestructuras inteligentes, especialmente teniendo en cuenta el gran poder de procesamiento que caracterizan a estos equipos, pero no es la única.

Tres años atrás, en nuestro artículo de *Tendencias 2017*, presentábamos el concepto de "Jackware" para describir al software malicioso que intenta tomar el control de un dispositivo cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital. Inmediatamente se desprende el concepto de "*Ransomware of things*", que hace referencia al malware capaz de bloquear el acceso a dispositivos inteligentes. En aquel año discutimos una *prueba de concepto que involucraba a un automóvil* en la que el usuario recibía un mensaje en su teléfono indicando que debía pagar una cantidad de criptomonedas para recuperar el control de su vehículo. ¿Podemos quizás extrapolar este concepto a los edificios inteligentes o a los sistemas de control de grandes ciudades?

¿Qué sucedería si un atacante consigue comprometer el sistema de automatización de un edificio inteligente y amenaza con tomar el control a cambio del pago de un rescate de varios miles de dólares? Lo cierto es que *ya se han reportado incidentes de este estilo* en los que edificios completos fueron comprometidos.

## Robo de Identidad

El control de acceso a edificios inteligentes suele ser a través de sistemas informatizados en los que el usuario se identifica con datos biométricos o tarjetas magnéticas. Estos sistemas pueden llegar a ser vulnerados a través de ingeniería social o fallas en la implementación y permitirían a un individuo no autorizado obtener acceso físico a sectores restringidos.

Por otro lado, la suplantación de identidad digital por parte de un atacante puede causar estragos si gana privilegios de administrador que le permitan controlar el sistema a su antojo. A menudo esto ocurre a través de ataques de ingeniería social en los que el atacante logra hacerse de las credenciales y acceso de la víctima, que luego son utilizados para instalar un código malicioso, robar información, desplazarse dentro del sistema o una multitud de otras ofensas nefastas.

## Robo de información crítica

Las bases de datos son un objetivo atractivo para los cibercriminales, especialmente si contienen información valiosa que se puede vender o credenciales que les permitan un movimiento lateral. Si a esto le sumamos la gran cantidad de información que almacenan los sistemas de análisis de big data e inteligencia artificial que se encuentran en los edificios y ciudades inteligentes, estas bases de datos se vuelven un objetivo de interés para cibercriminales y grupos de ciberespionaje.

Por otro lado, los sensores y dispositivos IoT utilizados en la mayoría de los edificios e infraestructuras inteligentes pueden ser también un punto de entrada a la red, lo que le permitirían a un cibercriminal tener mayores privilegios o realizar movimientos laterales dentro de la infraestructura. Tal es el caso de un casino que fue víctima de un ataque en el que cibercriminales ingresaron a su red tras aprovecharse de una *vulnerabilidad en el termostato inteligente de un acuario* ubicado en el lobby. Luego, lograron infiltrarse en la red y acceder a la base de datos del casino, robando información que incluía los datos personales de apostadores.

Luego de este análisis podemos decir que los edificios y ciudades inteligentes ya no son una predicción de la ciencia ficción, sino que son una realidad que está entre nosotros; y si bien los incidentes de seguridad reportados pueden ser aún considerados como casos aislados, los ataques a sistemas de control de edificios o ciudades ya están entre los objetivos de los ciberdelincuentes.

Las medidas y consideraciones de seguridad para hacer frente a estas nuevas amenazas son las mismas que venimos reiterando ante cada nueva evolución tecnológica: destinar presupuesto acorde a la seguridad, contar con programas de manejo de vulnerabilidades, mantener los sistemas actualizados, monitorear la red y los dispositivos y contar con herramientas de seguridad y socios que tengan conocimientos en el campo de la seguridad.

Crecen los proyectos de construcción que incluyen la implementación de cada vez más soluciones tecnológicas, incorporando todo tipo de dispositivos para volverlos más "inteligentes", pero ¿acaso están estas medidas de seguridad consideradas dentro de esa inteligencia?

Por otro lado, el apoyo de una legislación que regule la seguridad desde el diseño en dispositivos inteligentes es sumamente necesaria y es algo que probablemente surja en los próximos años, especialmente tras las nuevas *iniciativas del Reino Unido* y el estado de *California* en esta materia. Así como existen estándares que regulan equipamientos críticos, es hora de comenzar a analizar cuáles son las normas y medidas de seguridad que deberían cumplir los dispositivos inteligentes que interactúan con nuestra información y privacidad.

La mayoría de las ciudades del mundo ya cuentan con sensores y cámaras conectados a Internet que permanentemente recopilan y envían información para operar diferentes servicios. Muchos de nosotros ya vivimos en esas ciudades y en un futuro no muy lejano pasaremos gran parte de nuestra jornada laboral habitando o realizando compras en edificios hiperconectados y repletos de tecnología. Y si bien todos esos avances pueden ser apasionantes y cautivantes, no debemos olvidar que detrás de todo esto debe haber, ante todo, personas inteligentes.

# TRANSFORMACIÓN DIGITAL Y SEGURIDAD DE LA INFORMACIÓN: EL RETO PARA LAS EMPRESAS

- Cambios en IT deben implicar cambios en la gestión de la seguridad
- Variedad de tecnologías como motor del cambio
- El camino de la movilidad
- Conceptos a mantener en la transformación digital
- Entonces, ¿qué deberían hacer las empresas?


**AUTOR**

**Camilo Gutiérrez**

ESET Senior Security Researcher

# Transformación digital y seguridadde la información: el reto para las empresas

***A medida que las organizaciones deciden emprender o continuar por el camino de la transformación se ven en la necesidad de replantearse todos los aspectos de sus operaciones. ¿Cómo pueden aprovechar los beneficios que supone este cambio hacia lo digital sin descarrilarse como consecuencia de haber fallado en el abordaje de los desafíos que presenta la seguridad de la información?***

La dinámica del mercado ha llevado a que la transformación digital se vuelva un tema a tratar en todas las áreas de una empresa, involucrando tecnologías que brinden mayor valor a sus clientes. Todas estas incorporaciones, que ya han comenzado en muchas empresas desde hace un par de años, suponen, por supuesto, un cambio cultural a nivel organizacional que representan un gran desafío.

Obviamente, la seguridad de la información no debe considerarse como un ítem ajeno a esta meta, sino como parte importante de los objetivos que deben trazarse las empresas para no quedar relegadas en esta carrera por la seguridad.

Como la transformación digital suele tener implícita una restructuración de los procesos y estrategias propias de cada organización que permita aprovechar la tecnología digital, esto abre nuevos perfiles de riesgo que las empresas no pueden perder de vista.

## Cambios en IT deben implicar cambios en la gestión de la seguridad

Aquellas empresas que ya están transitando procesos de transformación digital se han visto abocadas al desarrollo de modelos de negocio que tienen un alto componente tecnológico, lo que ha obligado a los equipos de IT a tener que adaptarse para soportar la velocidad de estos cambios.

Todas estas modificaciones llevan a que las empresas de a poco pasen de tener la mayoría de sus recursos centralizados a tener que contratar una amplia gama de servicios y activos para dar soporte a las actividades diarias, trayendo esto un aumento en la diversidad de tecnologías y plataformas sobre las cuales debe hacerse monitoreo.

Este proceso de transformación, que ocho de cada diez organizaciones ha decidido emprender durante los últimos cinco años, según un relevamiento por parte de *McKinsey*, ha tenido un impacto directo en la seguridad que obliga a las empresas a reducir las posibilidades de ser víctima de un ciberataque o una brecha de datos. En este sentido, los equipos de gestión se han visto inmersos en nuevos paradigmas que les permitan cumplir con esta misión, pero sin afectar la normal operación del negocio, ya que, para operar de manera exitosa en este ecosistema digital, las organizaciones deben ser capaces de asegurar los datos durante este proceso de transformación y en los respectivos entornos.

Según un estudio que llevó adelante el *Instituto Ponemon* en 2018 en distintos países, el 72% de los profesionales de la seguridad informática considera que la urgencia por lograr la transformación digital incrementó el riesgo a sufrir una brecha de datos. Si a esto sumamos que el 45% de las organizaciones aseguró no contar con una estrategia para afrontar la transformación digital, el escenario es cuando menos preocupante.

Para los equipos encargados de la gestión de la seguridad, se vuelve un requisito primordial contar con un flujo constante de información en torno a todos los cambios que se presentan al interior de la organización. Es por esta razón que las tecnologías de inteligencia y monitoreo de amenazas resultan importantes para proporcionar la base sobre la cual otros procesos puedan ejecutarse de manera segura y manteniendo el cumplimiento de normativas en toda la organización.

## Variedad de tecnologías como motor del cambio

Para las empresas es necesario considerar la seguridad de la información como parte de la digitalización de una organización. En este sentido, dado que son múltiples las tecnologías que se comienzan a considerar para este proceso, como es la computación en la nube, las plataformas móviles, conectividad 5G y el machine learning, por mencionar solo algunas, debe entenderse que no es solamente una sola la aplicación o tecnología que permita garantizar la seguridad de los datos y la continuidad del negocio.

Seguramente, para aquellas empresas que ya lo estén considerando, una de las principales dudas sea por dónde comenzar. Y el punto de partida es precisamente comprender que toda esta transformación también está cambiando de manera radical y muy rápidamente a la sociedad global: la forma trabajar, de socializar, de comprar y de interactuar con las múltiples necesidades que forman parte de lo cotidiano.

## El camino de la movilidad

En todos estos escenarios de cambio al interior de las empresas, hay uno en particular que para el 2020 será un factor importante en la aceleración de todo este proceso de transformación: la movilidad del trabajo. Sin lugar a dudas, la capacidad de los dispositivos para mantener la conexión a las redes, independientemente de donde estén, sigue expandiendo la superficie de ataque que puede aprovechar un atacante.

Todo este cambio ya se ha venido generando lentamente en los últimos años, pero la adopción cada vez más acelerada por parte de las empresas del uso de tecnología móvil se realiza muchas veces sin considerar la seguridad. Por lo tanto, es importante que las empresas no sigan considerando la seguridad de manera clásica, sino que piensen en pasar a modelos adaptativos que puedan responder a los cambios.

Y más aún, los equipos de seguridad deben volcarse al aprovechamiento de las tecnologías de monitoreo, ya que no basta solamente con las tecnologías de detección. Es importante que las empresas habiliten sus procesos para responder ante un incidente y volver a la operación solucionando los incidentes y aplicando las medidas de corrección adecuadas.

## Conceptos a mantener en la transformación digital

Más allá de todas estas tecnologías específicas y que seguirán evolucionando, no se pueden perder de vista conceptos como los de privacidad. Estamos en un momento en el que cada vez más surgen leyes nuevas y más estrictas en cuanto a la protección de datos personales, lo que lleva a que las personas de a poco comiencen a conocer más sus derechos y estén más interesadas en cómo las empresas pueden llegar a manejar sus datos.

Durante los próximos meses veremos cómo las organizaciones desarrollan grandes cambios en casi todos los niveles de sus negocios, teniendo como eje central el manejo de la información y los datos propios de su operación. En este escenario, los modelos de negocio que generen confianza por parte del cliente correrán con ventaja.

## Entonces, ¿qué deberían hacer las empresas?

De cara a lo que van a enfrentar las empresas durante el próximo año, hay por lo menos cinco consideraciones que deben tener en cuenta para llevar adelante esta transformación de manera segura:

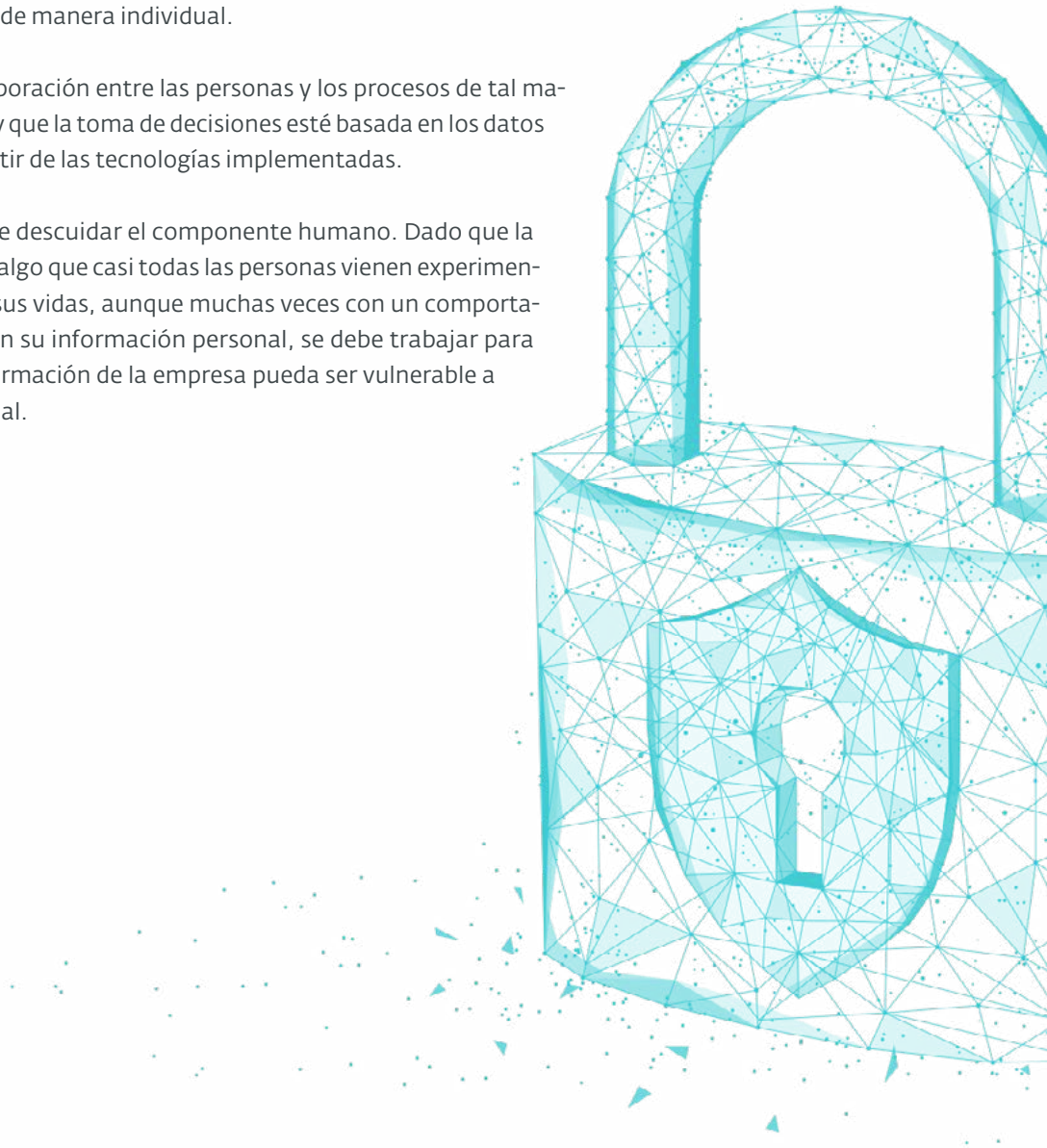
1. Buscar el equilibrio entre la implementación de las tecnologías y la ciberseguridad. Si desde el principio no se equilibran y se considera también a la seguridad como un habilitador del negocio, van a ser mayores los problemas que las soluciones.

2. Desarrollar proyectos que faciliten tanto la visibilidad como el control de las tecnologías, de esta manera el enfoque no debe estar centrado solamente en la prevención de incidentes, sino que deberá considerar la detección y la respuesta ante un incidente.

3. El enfoque de la seguridad no puede estar únicamente sobre los dispositivos, ya que cada vez son más los equipos y tecnologías como para pensar en implementar seguridad en cada componente de manera individual.

4. Propiciar una mayor colaboración entre las personas y los procesos de tal manera que estén alineados y que la toma de decisiones esté basada en los datos comunes generados a partir de las tecnologías implementadas.

5. Por supuesto, no se puede descuidar el componente humano. Dado que la transformación digital es algo que casi todas las personas vienen experimentando en la cotidianidad sus vidas, aunque muchas veces con un comportamientos riesgoso para con su información personal, se debe trabajar para evitar que también la información de la empresa pueda ser vulnerable a ataques de ingeniería social.



# CONCLUSIÓN

***Los retos que se avecinan son importantes y tenemos que prepararnos para que las generaciones actuales y las futuras dispongan de mejores herramientas, tanto desde el punto de vista tecnológico como educativo, para hacer frente a los desafíos que presenta la seguridad, ya que solo así se dará a la tecnología la oportunidad de desarrollar su verdadero potencial y que esto se traduzca en una mejor calidad de vida para la humanidad.***

Como vimos en cada una de las secciones que componen este documento, el mundo tiene la intención de seguir evolucionando en el uso de la tecnología e ir camino hacia a un mundo aún más "inteligente" que el actual. Pero solo cuando los avances en inteligencia artificial permitan realmente que las máquinas tengan la capacidad de pensar por sí mismas, cuando la transformación hacia lo que se conoce como ciudades inteligentes se convierta en un fenómeno global y cuando los procesos de transformación digital por los que atraviesan muchas empresas sea una cuestión del pasado, podremos analizar con mayor precisión cuáles fueron los costos de este proceso de transformación. Lo que sí está claro es que tal como se presenta la situación actual, la seguridad continuará estando un escalón por debajo en la consideración de los desarrollos tecnológicos y esto, posiblemente, traerá sus consecuencias en el corto plazo.

Si bien ha habido señales positivas que nos dan a entender que hay quienes dan cuenta de la importancia que tiene la seguridad y la necesidad de que tenga un rol más protagónico de cara al futuro, si pensamos que ocho de cada diez empresas durante los últimos cinco años decidió emprender el camino de la transformación digital y analizamos el *crecimiento que están teniendo las brechas de datos* a nivel global –sin mencionar el aumento en los costos que tendrá para las empresas hacer frente a este tipo de incidentes según las *proyecciones-* , las cifras dan cuenta de las dificultades que existen actualmente para evitar este tipo de incidentes de seguridad. Si además nos detenemos a pensar en el crecimiento proyectado para la construcción de edificios y ciudades inteligentes y que varias de las ciudades que actualmente apuestan por el concepto "Smart" han sido víctimas de amenazas ya conocidas como el ransomware, ¿por qué debemos ser optimistas y pensar que el futuro será mejor en materia de seguridad?

En esta misma línea, si tomamos como referencia los actuales avances en el uso del machine learning, el fenómeno de las fake news y lo que podemos esperar en un futuro aún distante del desarrollo de la inteligencia artificial, el desafío de estar preparado para lo que vendrá quizás pueda suponer una oportunidad para tomar medidas que realmente le den a la seguridad en un rol más protagónico.

Desde el 2016 a esta parte, las deepfake nos han dado señales del posible impacto que pueden llegar a tener a partir de lo que fue su participación en diferentes procesos electorales, generando gran confusión e incertidumbre acerca de qué información es verdadera y cuál es falsa; alimentando la desconfianza de individuos que, si bien están más interconectados, continúan exponiendo datos e información personal por desconocimiento de las buenas prácticas de seguridad. A su vez, varios de estos individuos deberán participar en procesos electorales en países que se inclinan por sistemas de votación electrónico pese a que han demostrado tener problemas.

Retomando la pregunta planteada anteriormente, se han visto señales positivas que permiten ser optimistas. Empresas como Facebook junto a universidades y otras importantes compañías han demostrado su preocupación por combatir fenómenos como las deepfake con iniciativas como el lanzamiento del desafío *"Deepfake Detection Challenge (DFDC)"*, a través del cual se intenta promover el desarrollo de tecnología capaz de combatir el impacto de las mismas. Asimismo, tal como explicó Lysa Myers en el capítulo "Cambios sustanciales en materia de privacidad", ha habido cambios en materia legislativa y regulatoria que, si bien han sido lentos y aún no han generado impacto relevante, son cambios positivos al fin.

Aún queda mucho por hacer y sigue siendo necesaria la intervención de los gobiernos para que impulsen medidas que le den un marco y una orientación al camino que se debe seguir de aquí en adelante. Pese a la falta de conciencia que aún existe por parte de los usuarios en varios aspectos que hacen a la seguridad, la desconfianza y descreimiento que muchos manifiestan son síntomas que reflejan que cada vez son menos ajenos al impacto que tiene la seguridad y la privacidad en sus vidas; y esto puede interpretarse también como una oportunidad para continuar trabajando en un factor clave como es la educación.

Son grandes desafíos los que se vienen y debemos estar preparados, tanto desde lo tecnológico como desde lo educativo, para que las generaciones actuales y futuras tengan las herramientas suficientes para hacerles frente y que la tecnología tenga la oportunidad para expresar su potencial y traducirlo en una mayor calidad de vida de los individuos.


CYBERSECURITY
EXPERTS ON YOUR SIDE