**ARTICULO DE REFLEXIÓN**

**Recibido: 5/09/2018**
**Revisado: 20/11/2018**
**Aprobado: 20/12/2018**

# SEGURIDAD DE LA INFORMACIÓN. UN RECORRIDO BAJO LA PERSPECTIVA DE MARC GOODMAN[1]

**ÁNGELA MARÍA ARTEAGA FIGUEROA**
Magister en Seguridad Informática
Universidad de la Rioja – España

**RESUMEN**

En el documento el lector encontrará una reflexión al enjundioso trabajo del investigador, Marc Goodman y su fascinante libro "Los delitos del futuro", de manera particular en su capítulo titulado "Sobrevivir al Progreso" en virtud a que en el mismo se ofrece un panorama inquietante; que llama la atención, a esta sociedad que ha entregado sus procesos fundamentales, a las dinámicas sugeridas por las tecnologías de la información y las comunicaciones.

**Palabras clave:** Seguridad, información.

**ABSTRACT**

In the document the reader will find a reflection on the substantial work of the researcher, Marc Goodman and his fascinating book "The Crimes of the Future", particularly in his chapter entitled "Surviving Progress" because it offers a panorama disturbing; that draws attention, to this society that has delivered its fundamental processes, to the dynamics suggested by information and communication technologies.

**Key Words:** Security, information.

1. Marc Goodman sargento e investigador estadounidense en tecnologías de la información, fundador del Future Crimes Institute y la Cátedra de Políticas, Leyes y Ética de la Singularity University de Silicon Valley, actualmente continúa investigando la intersección intrigante y a menudo terrorífica de la ciencia y la seguridad, descubriendo amenazas nacientes y combatiendo los lados más oscuros de la tecnología.

El lector encontrará en lo que sigue una reflexión al enjundioso trabajo del investigador, Marc Goodman y su fascinante libro "Los delitos del futuro", me he detenido en su capítulo titulado "Sobrevivir al progreso" en virtud a que en el mismo se ofrece un panorama inquietante; que llama la atención, a esta sociedad que ha entregado sus procesos fundamentales, a las dinámicas sugeridas por las tecnologías de la información y las comunicaciones.

Goodman observa que en el mundo de hoy, el mundo de la tecnología y la información es el espacio donde millones de personas en este momento están empleando alguna clase de tecnología moderna para realizar una actividad en particular, el vertiginoso avance del orbe tecnológico ha brindado una nueva perspectiva sobre una realidad inimaginable hace años atrás.

Efectivamente estamos frente a una revolución tecnológica masiva e imparable, rápidamente nacen nuevas tecnologías que agilizan procesos en corto tiempo, permitiendo satisfacer innumerables necesidades, la tecnología ha transcendido fronteras de espacio y tiempo, los beneficios son múltiples, el mundo celebra un nuevo invento, un nuevo hallazgo, una nueva creación, convirtiéndose en una oportunidad de transcender y quizá garantizar un mejor bienestar social.

Cuando usted accede a estas tecnologías revolucionarias no solamente las interioriza convirtiéndolas en propias, las hace parte importante del diario vivir. Sin embargo, usted como usuario se ha preguntado sobre los efectos negativos que pueden tener estas aplicaciones; aunque muchos de nosotros en un primer momento observamos una dimensión positiva de la tecnología, también debemos tener presente lo siguiente: la tecnología tiene un lado oscuro.

La tecnología de hoy en día es una conquista del hombre, pero los proyectos tecnológicos del presente y de un futuro en las manos equivocadas pueden traer consecuencias perjudiciales, Goodman (2015) "colaborador del Departamento de Policía de Los Ángeles, el FBI, el Servicio Secreto Estadounidense y la Interpol" (p. 12) nos enseña que ninguna tecnología es confiable.

Si es usted de las personas que pone su vida al servicio del internet, debe cuestionarse acerca de los riesgos; los mismos que podrían poner en jaque su información, por ejemplo: existen innumerables plataformas encargadas de almacenar datos de usuarios relacionados con su entorno más íntimo como la familia, trabajo, estudios, entre otros muchos más, y ofertarlos a personas con intenciones malignas capaces de convertir una vida común y corriente en una verdadera pesadilla virtual.

Los delitos no solamente ocurren en la vida real, la virtualidad es un nuevo escenario, los ciberdelincuentes[2] están al orden del día, tratando de almacenar información para sus iniciativas no éticas, no morales, que ponen en alerta

2. Ciberdelincuente: **Personas que realizan actividades delictivas en internet** como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los **delitos e ilegalidad**.

máxima a todos los usuarios. Las armas de un ciberdelincuente no se limitan a la disponibilidad de un ordenador, sencillamente, es la confianza de millones de personas que publican y comparten sus acciones cotidianas en un medio virtual de dominio público; las que aperturan vulnerabilidad, donde la información no es tuya, es propiedad de todos.

En el capítulo que se comenta se demuestra que las amenazas tecnológicas son progresivas, posiblemente usted no perciba esto y quizás nunca se entere de ello, hasta que se convierte en una víctima de las trampas del internet, tratamos de confiar en nuestras adquisiciones tecnológicas, imaginamos que el robo o secuestro de datos es un problema que incluye a algunas personas y que tales hechos nunca nos van a suceder, pero tenga cuidado.

Recordemos películas como: La Red, Disconnect, Antitrust, entre otras muchas más, y observemos que todo aquello que parecía parte de la ficción, ahora ha superado a la realidad, un caso similar de estas representaciones cinematográficas salió a la luz a principios de este año, medios de información estadounidense denunciaron las irregularidades en el manejo de información de aproximadamente "90 millones de usuarios de la reconocida red social Facebook por parte de la ex firma británica Cambridge Analytica, en las pasadas elecciones presidenciales de 2016" (El Espectador, 2018, párr. 4).

De manera ilegal se filtró información de carácter público y privada de personas con capacidad de voto en los Estados Unidos, "mediante la aplicación Pig. Gi, que ofrecía recargas gratuitas a los usuarios que llenaran encuestas o vieran anuncios" (Semana, 2018, párr. 8). Con los datos obtenidos se logró establecer formas de pensar, sentir y actuar de cada persona y luego el equipo de investigadores de Cambridge Analytica llegaron a establecer "cual debía ser el contenido, tema y tono de mensaje para cambiar la forma de pensar de los votantes de forma casi individualizada" (BBC, 2018, párr. 21).

Hechos como el anterior se producen diariamente, somos parte de un gran laboratorio social de investigaciones avanzadas a nivel tecnológico, nuestra realidad es moderna, pero es importante cuestionarnos lo siguiente: ¿Qué tan modernos somos nosotros? ¿Somos tan desarrollados como las maquinas que hemos construido? Goodman (2015). Esto nos demuestra que "nuestra subjetividad es muy frágil" (p. 34), el mínimo accionar nos afecta, nos puede llegar a destruir lamentable e irreparablemente, cuantos ataques se han producido a la información privada de las personas por parte de crackers informáticos sin que estemos atentos a ello, como el caso de Cambridge Analytica.

El concepto de "seguridad" que emerge desde la perspectiva de Goodman es un asunto de responsabilidad social, ¿Quiénes se encargan de la protección de la información de millones de usuarios alrededor del mundo? ¿Quiénes son esos policías virtuales? Ningún sistema informático es confiable, ninguna contraseña nos puede brindar la seguridad anhelada, ninguna persona puede borrar su historial de na-

vegación y estar completamente segura que sus acciones en la virtualidad han quedado olvidadas, todo se guarda con una intención sea buena o sea mala.

Goodman enfatiza en la importancia de explicar la ciencia, "las consecuencias del analfabetismo científico son mucho más peligrosas en nuestra época que en cualquier anterior" (Sagan, 1997, p. 23), los creadores de la ciencia deben brindar a la humanidad la información necesaria de las consecuencias positivas y negativas de sus invenciones, ese es el primer paso para generar estrategias de formación encaminadas a la protección y al moderado consumo tecnológico, advertir sobre los posibles riesgos u amenazas es una forma de minimizar los impactos de la tecnología en la población, especialmente en la juvenil.

Las tecnologías de la información y la comunicación son escenarios alternativos donde niños y niñas menores de 18 años acceden a internet en busca de nuevas relaciones a través de la creación de perfiles personales en cuentas virtuales como Facebook, Twitter, Instagram, etc. Generalmente, navegan bajo el control de una persona; los cuales, directa o indirectamente crean mecanismos de protección primarios o simples. Estas formas, no previenen de los riesgos que pueden ser objeto la población juvenil, puesto que carecen de vigilancia de los contenidos consultados por internet, persistiendo un desconocimiento de las actividades que hacen los menores de edad cuando se conectan en internet.

Estoy de acuerdo con Marc Goodman cuando infiere que una de las ventajas que ha contribuido a que muchos ciberdelicuentes entren a nuestros hogares, trabajos y en nuestras vidas, es gracias al desconocimiento técnico que poseen las personas alrededor del mundo, en América Latina estos procesos permanecen bajo un velo oscuro de dudas e incertidumbres, este llamado no consiste en que todos los usuarios se conviertan en expertos en seguridad informática, pero sí de poseer algunos conocimientos básicos que contribuyan a generar más seguridad en tiempos donde la tecnología que empleamos avanza y se transforma, también avanza y se transforman las acciones ciberdelictivas.

El autor nos presenta una caja de herramientas orientadas a la protección de la información, opción excelente para ejecutarlas desde nuestros entornos más inmediatos. Multiplicar y compartir estas acciones entre más usuarios seguramente nos convertirán en esos vigías virtuales con capacidad de ejecutar la tecnología que llega a nuestras manos con mayor sentido de responsabilidad. La "tecno utopía" nos invita a crear espacios virtuales equitativos y sostenibles, limpios de virus, que le salgan al paso a los que secuestran y destruyen información atentando contra nuestros derechos de comunicarnos y expresarnos libremente en el mundo de la virtualidad. A continuación te invitamos a seguir estos pasos sencillos:

1. Actualizar es dejar atrás todo aquello que nos puede hacer frágiles, es recomendable "renovar o actualizar permanentemente el software del sistema operativo de computado-

res, tables, celulares, etc." (Goodman, 2015, p. 605). Los softwares de estos dispositivos tecnológicos contienen errores que los crackers informáticos emplean al máximo para localizar, identificar y extraer información relacionada con sus propósitos delictivos.

2. Anteriormente habíamos mencionado que ninguna contraseña es segura, pero podemos disminuir las probabilidades de ser objeto de los crackers informáticos dedicados a este plano de la tecnología virtual, tenga presente que cotidianamente se crean softwares encargados a develar el contenido de millones de contraseñas. En primer lugar, lo correcto es cambiar periódicamente las contraseñas, está comprobado que dejarlas por tiempos largos, contribuye a un fácil descifrado y acceso a cuentas virtuales. En segundo lugar, deben ser alfanuméricos y poseer como máximo veinte caracteres entre símbolos, números y letras mayúsculas y minúsculas. En tercer lugar, si eres de las personas que emplean generadores de claves y contraseñas, trata de consultar uno de confiabilidad, por ejemplo: Dropbox, Evernote, PayPal, entre otros muchos más.

3. Cuando necesites descargar algún software es importante revisar su origen de contenido, es recomendable seguir los sitios aptos y calificados para estas operaciones, por ejemplo: App Store de Apple, garantiza un software limpio de virus que pueden llegar el lugar donde tengas almacenada la información, "desconfía de los softwares gratuitos, que se encuentren en redes P2P, logrando reducir un mayor riesgo de infección" (Goodman, 2015, p. 607).

4. Mantener apagado el ordenador cuando no se emplea para alguna actividad, este al estar prendido y con conexión a internet se convierte en una puerta de acceso a diversos ciberdelincuentes, igualmente el celular es objeto de constantes ataques, se recomienda cuando no se emplea desactivar "bluetooth y Wi-Fi, el acceso inalámbrico al móvil en todo momento proporciona vías adicionales de ataque que ladrones pueden utilizar para poder vulnerar tu teléfono, propagar software malicioso y robar datos" (Goodman, 2015, p. 608).

5. Encriptar la información es algo comúnmente empleado entre usuarios, ayuda a proteger información de cada usuario relacionado con su vida personal y de trabajo "encriptar tu disco duro implica que los demás no puedan acceder a su contenido si lo pierdes o lo roban, encriptar el tráfico por internet utilizando una red privada virtual (VPN), especialmente cuando usas red Wi-Fi pública" (Goodman, 2015, p. 609).

Estas son algunas de las reflexiones que salen en torno a las dinámicas y las lógicas por las cuales opera el tema de la información y la seguridad en internet, tema recurrente, oportuno y más que sugerente a la hora de entender que un porcentaje significativo de nuestras obras en el mundo, tienen que ver con el uso de la tecnología de la información y las comunicaciones.

## BIBLIOGRAFÍA

BBC (2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. Recuperado de https://www.bbc.com/mundo/noticias-43472797

El Espectador (2018). *Cambridge Analytica se declara en quiebra en Estados Unidos.* Recuperado de https://www.elespectador.com/economia/cambridge-analytica-se-declara-en-quiebra-en-estados-unidos-articulo-789187

Goodman, M. (2015). *Los delitos del futuro*. Colombia: Ariel.

Sagan, C. (1997). *El mundo y sus demonios: La ciencia como una luz en la oscuridad*. México: Editorial Planeta.

Semana (2018). *Cambridge Analytica, involucrada en escándalo por uso de datos de Facebook, cerró sus operaciones.* Recuperado de https://www.semana.com/tecnologia/articulo/cambridge-analytica-involucrada-en-escandalo-facebook-cerro-sus-operaciones/565643

Seguridadpc.Net. (sf). *¿Qué son los ciberdelincuentes?* Recuperado de http://www.seguridadpc.net/conceptos/los-ciberdelincuentes.html

Singularity University (sf). *Marc Goodman*. Recuperado de https://translate.google.com/translate?hl=es&sl=en&u=https://su.org/about/faculty/marc-goodman/&prev=search