interlat®

Centro del
Pensamiento
Digital
Latinoamericano

Internet Fortificada: Seguridad Digital y Certificados Blockchain

Febrero 2022

Contenido

Fundador y Director
Luis Carlos Chaquea B.

Moderadora y Editora
Ingrid Arzolay S.

Renata Cabrales, Ejecutiva principal en Banco de desarrollo de América Latina (CAF)
Colombia
Hiddekel Morrison, Presidente & CEO en HM Consulting
República Dominicana

Héctor García, presidente de Camerfirma y Director Académico en la Pontificia Universidad Javeriana.
Colombia
Diego Alarcón, Gerente de Cuentas Estratégicas Fujitsu.
Colombia

Abstract

Una caída global de las redes sociales favoritas, con miles de millones invertidos, causó pérdidas considerables y caos social. La falla tuvo su origen en un error humano. ¿Cuánto es el verdadero costo de la Seguridad Digital? Más allá de la aplicación tecnológica: ¿De quién es la responsabilidad? Son preguntas claves.

Informes detallan que el mayor riesgo se encuentra en el ser humano. Entonces, la inversión en la capacitación del talento en materia de seguridad digital debería ser prioridad. Sin embargo, aún los estados y organizaciones no aprueban políticas que rijan las buenas prácticas en la materia.

En este documento resumimos el debate que los especialistas en seguridad digital tuvieron en torno al tema en el Centro del Pensamiento Digital Latinoamericano, en el marco de los 9nos Premios #LatamDigital by Interlat Digital Enterprise Intelligence

Palabras clave:
Seguridad Digital, Capacitación, Fake News, BlockChain, MetaVerso, Seguridad Digital, Tecnología, Ciberseguridad, Ciberdelincuencia, Marco Legal.

Desarrollo

1.- Fake News y la generación de caos social

Las *Fake News* están en el punto de mira por ser causa de inestabilidad política, social y económica. Son un verdadero peligro cuando son usadas como instrumentos para generar caos social. Pueden enardecer a las personas y causar pérdidas económicas considerables. Su rango de acción es tan amplio y diverso como la sociedad misma; son capaces de afectar desde la macroeconomía de un país, hasta el emprendimiento de un usuario en Instagram.

El impacto más grande se encuentra en el ciudadano pues “inciden en nuestras decisiones” y en los efectos sobre “la Ideología”, afirma Hiddekel Morrison, Presidente & CEO en HM Consulting. Renata Cabrales, Coordinadora de proyectos en Fundación Gabo, profundiza en el tema: “Una información falsa puede afectar la salud, el buen nombre y la honra de una persona e incluso provocar la muerte”. Los efectos de una *Fake News* pueden ser de intensidad leve, media o alta. Existen dos tipos: las fabricadas y las espontáneas. Estas últimas son parte de estrategias con objetivos personales o de grupos de poder que desean generar ciertos efectos en la sociedad.

Las consecuencias de las *Fake News* son tan negativas que es urgente que los ciudadanos presionen a los poderes privados y públicos para que apliquen medidas de control. “Las plataformas de redes sociales deben evitar ser utilizadas para tales fines”, indica Morrison. Sin embargo, la acción tomada por Twitter y Facebook durante el periodo 2020 y el suceso de la pandemia, obtuvo cierta fricción y dió paso a otros debates. Entre esos debates surgieron dos cuestionamientos: Uno, el poder de limitar o no la libertad de expresión de las personas, influyentes o no. Dos, el poder en sí que tienen las redes sociales para afectar a la sociedad y su responsabilidad sobre esa afectación.

En el foro se destacaron algunas herramientas tecnológicas que ya están en implementación. Las cuentas verificadas, entre ellas. Además, indicaba Morrison: “Existen ya algoritmos que permiten que se denuncie la información falsa o el caso de WhatsApp que limita la cantidad de reenvíos.” ¿Son medidas escasas? Habrá que seguir discutiendo.

Aplicar la tecnología Blockchain “garantizaría la realidad del origen inviolable de la información y lo puedes aplicar muy fácil”, asevera Diego Alarcón, Gerente de Cuentas Estratégicas Fujitsu.

2.- El usuario es el eslabón más débil

Morrinson hace énfasis en que en materia de ciberseguridad son las personas “el eslabón más débil”. De allí que lo más importante sea educar al usuario. “Evangelizar” es la palabra que aplica Alarcón. Es importante que cada uno de los profesionales que tienen el conocimiento, compartan con los otros la importancia de tener buenas prácticas de ciberseguridad. Como bien indicaba Alarcón, no sólo en la difusión de información, sino al momento de gestionar la seguridad de sus acciones en Internet.

Los análisis de eventos donde se ha presentado un quiebre de la seguridad en internet demuestran que la plataforma, el encriptado y el algoritmo no tienen fallas. “En muchos de los grandes casos de filtraciones de seguridad o de ataques quien falla es la persona que ejecutó la acción. Por lo general la arquitectura del sistema no ha sido vulnerada”, afirma Morrinson.

Son conocidas las buenas prácticas que se desarrollan en las diferentes organizaciones para evitar la difusión de informaciones falsas. Sin embargo, queda un trecho largo en materia de buenas prácticas de ciberseguridad. La aplicación tecnológica es el camino, pero las personas deben recorrerlo, conocerlo e internalizar cuál es la importancia de tener buenas prácticas en sus procesos de digitalización.

Sobre las Fake News la recomendación básica y fundamental es conocida. “Antes de difundir una información se debe comprobar el origen y la veracidad de la misma”; afirma Hector García, presidente de Camerfirma. La importancia de conocer estas buenas prácticas es apenas el inicio del trabajo a realizar para enfrentar el peligro que representan.

Las plataformas ya tienen diferentes herramientas de denuncia que los usuarios pueden utilizar. Nuevamente queda en manos de las personas la capacidad de frenar o no estos procesos que vulneran la seguridad de Internet y que ponen en riesgo la sana convivencia ciudadana. Renata Cabrales hace énfasis en que una noticia falsa puede ya ser juzgada como un delito de calumnia o injuria y ser llevada ante la ley.

Alarcón hace énfasis en que “la educación nos toca a todos. Eso va a hacer que haya menos resistencia a todas estas tecnologías y que seamos más conscientes. Cuando tú eres consciente de que conducir a alta velocidad es un riesgo, entonces no lo haces. En el caso de la tecnología, no todos los usuarios saben que si vas a un cibercafé y usas un computador para abrir tu cuenta de Facebook, debes cerrar la sesión. De lo contrario el siguiente usuario que se siente en esa máquina tendrá acceso a toda la cuenta y datos de esa persona”.

Para saber qué tan expuesta está la sociedad actual, Diego Alarcón recuerda el evento de la caída global de Facebok, Whatsapp e Instagram. Indica que la causa de tal situación fue “por algo tan sencillo, como los cambios de unas políticas de unos routers de conectividad en California. Resulta que un usuario cometió un error en los switches de conectividad de Facebook, ahora llamada “Meta” y por eso cayó todo el planeta”. Esto para que se tenga una idea de lo vulnerable que es nuestro sistema social actual.

3.- La responsabilidad del algoritmo

En el otro lado de la moneda, Renata Cabrales indica que existe responsabilidad en las grandes compañías y la programación de sus algoritmos. “La tecnología puede ayudarnos mucho a proteger la información y a proteger la verdad”, indica Cabrales. Pero el robustecimiento de los algoritmos es un requerimiento que se debe hacer y en los que todos los actores de la sociedad deben estar de acuerdo.

García de Camerfirma revela que ya existen tecnologías que alertan sobre una información que tenga más de 25.000 views, pero que el desarrollo tecnológico requiere de estudios que fundamenten la necesidad o la importancia de generar una Internet Fortificada. Faltan estudios que validen el impacto que una Fake News tiene en la sociedad. De nuevo, la exigencia por parte de la ciudadanía es muy importante.

Morrinson insiste en que una gran parte de la responsabilidad sobre Fake News está en manos de las plataformas. Él expone: “Si las dos o tres plataformas por las que se difunden el 80% de noticias falsas toman las medidas, veremos cómo mejora la situación. Ya se ha comprobado esto cuando se limitan las posibilidades de enviar un mensaje en whatsapp o cuando se limitan las publicaciones que tienen términos identificados como noticias falsas”. Todo esto tiene detrás algoritmos tecnológicos capaces de reducir el problema. La pregunta es: ¿Se tiene el interés de reducirlo?

4.- Internet fortificada más allá de las Fake News

Alarcón llama la atención sobre la importancia de ver la seguridad como una prioridad o como una inversión necesaria. Lograr una internet fortificada va más allá de evitar la difusión de noticias falsas. En su experiencia, la tecnología que existe para proteger los sistemas de grandes compañías o instituciones públicas no es aplicada porque no existe una conciencia de la necesidad de tener ecosistemas seguros.

“El segmento corporativo y empresarial tiene que asumir responsabilidad. Hay excelentes soluciones tecnológicas y de seguridad. Existe la detección con inteligencia artificial del comportamiento típico de una organización para saber cuando puede haber un acceso remoto tendiente a secuestrar la información. Pero esas compañías ven la seguridad como un gasto que no genera dinero. Y por eso no se aplica”, refiere Alarcón. Por fortuna ya es mayor la aceptación de la importancia de proteger los ecosistemas digitales, aunque aún no es suficiente.

La cultura de seguridad digital ha recibido un impulso debido a la multitud de casos de empresas que no invierten en su seguridad y luego sufren un ataque o un quiebre en sus ecosistemas. ¿Es suficiente esta aceptación? No. Es muy poco y muy lento. Los riesgos aumentan de forma exponencial y en la medida que se acelera la transformación digital; se acelera el riesgo de caer en ciberdelincuencia o en qué sectores o intereses particulares influyen en las ideologías de los estados.

“La tecnología cuesta y hay que invertir, es necesario”, afirma Alarcón. Dentro del evento anual *Fujitsu Activate Now 2021,* el Expresidente de Estonia Toomas Hendrik Ilves, expuso cómo la digitalización de todos los ciudadanos en Estonia, le permitió al Estado generar un beneficio del 2% del producto interno bruto. Alarcón narra que “un ciudadano Estonio ya tiene una versión digital de su seguridad social, de su identificación y de toda su historia clínica. ¿Cómo se hace? Invirtiendo en esa tecnología”.

5.- Invertir en tecnología

Álvaro Guzman, ganador de los 9nos Premios #LatamDigital destacó la crisis de confianza que existe. “Ahora mismo lo que está pasando en la humanidad es que estamos viviendo una crisis de confianza. No es necesario pensar en validar si la noticia es falsa o no. La crisis de confianza viene por la pregunta: ¿A quién le creemos? ¿Y quién es responsable de validar que algo es cierto o no es cierto? Lo que surge es que la confianza ha perdido su institucionalidad. Ahora necesitamos tecnología Blockchain”, indica.

La tecnología llega como un soporte de esa confianza resquebrajada. Pero se debe recordar que no es un tema nuevo. Las noticias falsas existen desde que la humanidad existe. Con otros nombres y otras formas. Lo relevante hoy es que existe la tecnología para manejar esas situaciones. Existen formas de regular, normar y certificar la información. Incluso rastrear el origen. Allí hay que trabajar.

El dolor está allí, la medicina también; sin embargo, aún se requiere de mucho esfuerzo para conversar sobre Seguridad Digital. Para que las personas comprendan la importancia de crear contraseñas seguras. Aún falta para que las empresas inviertan en Seguridad Digital, tal y como se invierte en la Seguridad laboral o industrial, por ejemplo.

Todas las organizaciones tienen que estar alineadas para invertir en tecnología. Es la única forma de poder generar confianza en la red. Generar estándares similares de protección que aseguren todo lo que la industria digital comprende. Los estados tienen que mirar el “marco regulatorio" de los desarrollos, actitudes y manejo de datos, afirma Morrinson. “Los gobiernos deben ser proactivos porque la tecnología va delante de la readecuación social”, continúa.

La subestimación de las consecuencias y el pensamiento muy común de “a mí eso no me va a pasar” incide en que exista una resistencia a invertir en tecnología de seguridad. Hay que demostrar el impacto financiero de no hacer la inversión, expone Alarcón. Casos abundan de empresas que han perdido más al sufrir un caso de ciberdelincuencia que aplicar las medidas preventivas. ¿Por qué esto sigue pasando?

Es importante que la seguridad digital se mire como la inversión de un seguro. La inversión lo que garantiza es que las compañías se encuentren protegidas. La medida es preventiva, y al igual que en un seguro, es mejor que no ocurra ningún accidente grave.

Conclusiones

Para tener una Internet Fortificada es clave evitar la difusión de noticias falsas, explica Hector García. También se debe asegurar de informar a la sociedad. “Evangelizar” es el verbo más adecuado sobre la responsabilidad que tiene cada usuario al manejar su información personal, corporativa o noticiosa.

Cada actor debe tener responsabilidad sobre la seguridad en internet. En especial el tema de propiedad de datos está pendiente y es una conversación que debe darse. El marco regulatorio sobre cibercriminales es una deuda de casi todos los estados. La educación de los empleados por parte de las grandes organizaciones, es otra tarea sin realizar. La responsabilidad legal sobre las grandes compañías que lanzan sus algoritmos y no miden su impacto social, es otra discusión pendiente.

“Los gobiernos deben ser más proactivos, porque la tecnología va delante de la readecuación social. Primero viene la realidad del ciberdelito y luego vienen las legislaciones que lo combaten. En un futuro vendrá el metaverso y con él vendrán los versos legales. Otras realidades, otros desafíos. El componente regulatorio es determinante, Cuando los gobiernos en cada país establezcan leyes que le digan a facebook, que le digan a google, si por sus plataformas se difunden noticias falsas hay una penalidad, entonces tendremos otras conversaciones”, asegura Morrinson.

Lo cierto es que no se trata del desarrollo tecnológico. Allí, ya no está el obstáculo. Lo que en realidad hace falta es la disposición de los actores para tomarse la fortificación de internet en serio. Crear sistemas de confianza, ética y responsabilidad es fundamental. Decidir hacerlo es la clave, la tecnología ya existe.