Internet, **la nueva sangre** de la tecnología

Las tecnologías emergentes, aquellas que están conectadas a internet, traen múltiples beneficios, pero es necesario tomar precauciones para usarlas con seguridad porque los cibercriminales están al acecho.

Imagen: Thomas Breher (Tbit) en www.pixabay.com (https://goo.gl/UvuVMT). Licencia CCO Creative Commons.

Big data, blockchain, internet de las cosas (IoT), internet del valor (IoV), industria 4.0, ciudades, hogares y redes inteligentes (*smart*) y *fintech* son nombres que aparecen cada vez con más frecuencia en la vida ordinaria de las personas. Estas tecnologías emergentes, conectadas a internet, proporcionan velocidad, eficiencia y otras múltiples ventajas, pero pueden comprometer la privacidad y la seguridad.

La palabra *blockchain* se asocia con criptomonedas, ese medio para hacer transacciones virtuales que alcanza precios astronómicos y del que bitcóin es el más conocido. Pero, en realidad, esta tecnología es mucho más, pues da pie a nuevas modalidades de negocio, a partir de tres de sus características fundamentales: la información se produce en bloques y así se garantiza su integridad; es pública, lo que aumenta la transparencia y la confiabilidad, y múltiples mineros la generan de forma distribuida, con lo cual es difícil de manipular.

Gracias a esas condiciones, hoy se habla de contratos inteligentes, una variante empresarial en la que los computadores conectados a internet —si se cumplen ciertas condiciones— toman decisiones automáticas sobre las acciones que deben seguirse.

También es recurrente la palabra *smart* combinada con *cities*, *homes* y *grids,* que no son otra cosa que ciudades, hogares y redes inteligentes; o empieza a ser familiar la industria 4.0, en la que se automatiza casi por completo la producción industrial mediante computadores que controlan procesos y máquinas.

Todas ellas son tecnologías emergentes, cuya característica es la conexión a internet, y que, sin duda, están revolucionando la sociedad, de la mano del acelerado crecimiento de las posibilidades de conexión de los seres vivos entre sí y con las máquinas.

Los beneficios y riesgos que en materia de seguridad y privacidad plantean estos temas fueron el centro del "4.º Foro en seguridad de la información. La seguridad ciudadana ante el reto de las plataformas tecnológicas emergentes". Este se llevó a cabo el 20 de septiembre del 2017 en la Universidad de los Andes y fue organizado por el Departamento de Ingeniería de Sistemas y Computación (DISC).

En el panel que se desarrolló dentro del evento se habló de varias de estas tecnologías, de sus beneficios y de los riesgos que representan para la sociedad.

A continuación, un resumen de lo tratado por los panelistas y algunas conclusiones recogidas por la profesora del DISC Sandra Rueda sobre las conferencias.

Blockchain y criptomonedas

Hubo consenso entre los conferencistas sobre la urgencia de estudiar el fenómeno para decidir cómo encararlo y si, eventualmente, debe ser objeto de regulación estatal, pues en Colombia es alegal.

"La banca tradicional, definitivamente, no ha venido atendiendo esas nuevas necesidades —dijo Yenny Tatiana Rodríguez, jefe de Seguridad de la Información del Banco Itaú, al responder una pregunta del público en el panel—. Colombia debe abrirse a estos temas y pensar qué sucedería si adoptáramos las monedas virtuales, que no responden a una banca centralizada. Debemos usar nuestra experiencia en temas como lavado de activos y no devolvernos en el tiempo".

Imagen: Michael Weenscht, en www.pixabay.com (https://goo.gl/cVU3T5). Licencia CC0 Creative Commons.

Bitcóin es la más popular de las criptomonedas. Estas plataformas no están reguladas por el sistema bancario.

A su vez, el coronel Fredy Bautista, director del Centro Cibernético de la Dijin, resaltó que las criptomonedas son plataformas alternativas para hacer transacciones, que le dan vida al IoV (internet del valor), pero, a diferencia de los sitios de pagos en línea, no están certificadas por una franquicia o por un sistema bancario. De ahí, recalcó, se derivan diversos riesgos: además, de lavado de activos y financiación del terrorismo, se usan para pagar extorsiones producto de ataques de *ransomware* (programa malicioso que encripta la información con el fin de pedir rescate) o de denegación del servicio; o para acceder a servicios vía *streaming* que reproducen en vivo abusos sexuales a niños.

Eddy Williems, evangelista principal de G Data, añadió que los inversionistas pueden resultar estafados cuando ponen su dinero en una especie de esquema piramidal, en el que desconocen quién está detrás.

Internet de las cosas (IoT) y *smarts*

El IoT conecta los dispositivos y aparatos que usamos en la vida diaria mediante sensores para que interactúen entre máquinas o con seres vivos mandando o recibiendo información a través de internet. Da pie, entonces, a las *smarts* (hogares, ciudades y redes inteligentes, son las principales).

"Ayuda a reducir costos y a aumentar la eficiencia; por ejemplo, si la Policía sabe cuáles son las vías más congestionadas, puede controlar los semáforos —dijo en el panel Martha Liliana Sánchez, asesora nacional de Seguridad Digital de la Presidencia de la República—. Los riesgos surgen porque estamos pasando del internet de la información, al internet de valor, en el que podemos transar monedas, acciones o cualquier otro dato para tomar decisiones y no fue diseñado para eso".

Por otro lado, los conferencistas concluyeron que se requiere compromiso serio entre la utilidad del internet de las cosas y la privacidad de las personas. Como los objetos están conectados a sensores que recopilan información, quienes la recogen deben informarle al usuario cuál es el fin que persiguen y, además, garantizar que su almacenamiento sea seguro, para evitar que sea *hackeada*.

"Si la gente quiere beneficiarse de estas tecnologías, tiene que ceder datos a cambio, pero debe saber para qué van a usarlos", afirmó la profesora Rueda y al entregar las conclusiones mencionó ejemplos poco éticos, como el de un fabricante de juguetes sexuales que recogió datos íntimos de sus clientes sin siquiera contarles que los sensores de los dispositivos enviaban detalles de cómo los usaban.

Fintech

Son *start-ups* que proveen aplicaciones que prestan servicios financieros, pero no corresponden a empresas financieras ni tecnológicas tradicionales y están por fuera del

Los expositores

Los conferencistas fueron los siguientes: Eddy Williems, evangelista principal de la compañía de seguridad alemana G Data; AJ Singh, director de Servicios Globales y Soluciones en Inteligencia de la estadounidense FireEye; Rafael Londoño, subdirector de Estándares y Arquitecturas de MinTIC; John Fabio Giraldo, contralmirante del Comandado Conjunto Cibernético, y Gina Pardo, directora de Seguridad y Operación Bancaria de Asobancaria.

También contó con la participación especial de Michael Bock, embajador de la República Federal de Alemania, y de Alexander von Bila, presidente del Consejo directivo de la Cámara de Industria y Comercio Colombo-Alemana.

De igual forma, hubo un panel, en el que, además de Eddy Williems y AJ Singh, estuvieron los siguientes expertos: Fredy Bautista, coronel de la Policía y director del Centro Cibernético de la Dijin; Martha Liliana Sánchez, asesora nacional de Seguridad Digital de la Presidencia de la República, Yenny Tatiana Rodríguez, jefe de Seguridad de la Información del Banco Itaú, y Sandra Rueda, profesora del DISC, como moderadora.

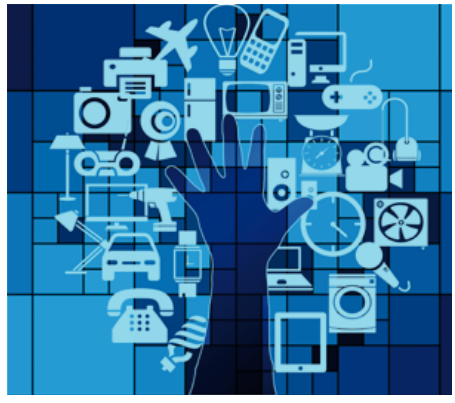


Imagen: Gerd Altmann (Geralt) en www.pixabay.com (https://goo.gl/6fMVfr). Licencia CC0 Creative Commons.

La conexión digital de objetos que usamos a diario facilita la vida de las personas, pero plantea retos en cuanto a la privacidad.

mercado regulado. Dentro de ellas, Yenny Tatiana Rodríguez, del Banco Itaú, destacó el *crowdfunding*, una modalidad de financiamiento colectivo para esas empresas, e identificó los siguientes riesgos:

1. Lavado de activos y financiación del terrorismo. Dado que no hay trazabilidad de los recursos para financiar estas empresas, no se sabe si realmente se quiere crear una *start-up* o si se pretende ingresarlos al sistema legal amparados en máscaras.
2. El impago. La iniciativa puede no llegar a feliz término y, por lo tanto, se pierde la inversión. En otros negocios, ese riesgo lo asume el sector financiero, pero aquí solo hay dos personas haciendo la transacción y la posibilidad de que se materialice es alta.
3. El operacional. En él intervienen tres actores: a) la persona que requiere la inversión, b) el dueño del capital y c) la plataforma a través de la cual se hacen las inversiones. Entre ellos pueden surgir conflictos de intereses relacionados con el número de créditos, con las ganancias esperadas, con la posibilidad de lavado de activos y acciones similares.

Industria 4.0

Eddy Williems, de G Data, destacó la industria 4.0, un protocolo que está empujando la completa automatización de los ambientes industriales mediante el uso de computadores conectados a internet. La intranquilidad surge de la vulnerabilidad de las redes usadas para controlar los procesos porque puede comprometerse no solo la parte física de la planta, sino que los productos pueden encarecerse o no estar disponibles en el mercado.

Vehículos automatizados

AJ Singh, director de Servicios Globales y Soluciones en Inteligencia de FireEye, resaltó los vehículos automatizados que, por ejemplo, podrían mitigar los problemas de tráfico y reducir las emisiones de CO_2.

"Como ciudadanos, no deberíamos confiar en que el Gobierno nos protegerá de todo en el ciberespacio, porque —enfatizó—, a diferencia de los otros escenarios, en este no sabe quién es el enemigo ni cómo va a llegar y tampoco tiene las herramientas para estar pendiente de todo el mundo. A nosotros también nos toca colaborar".

Cloud computing

Esta tecnología provee servicios computacionales en la nube que pueden usarse sin necesidad de instalar equipos en las empresas.

La profesora Sandra Rueda recogió tres conclusiones de las conferencias: 1) es importante verificar el nivel de confianza de los proveedores de las soluciones, 2) hay que encriptar los datos que se suben a la nube y 3) no deben almacenarse allí documentos que puedan comprometer la seguridad de las instituciones o de las personas.

Sobre este último punto, el coronel Fredy Bautista contó sobre un microempresario que pidió ayuda al Centro Cibernético de la Policía porque digitalizó documentos sensibles de su sociedad y los subió a la nube; le comprometieron la contraseña y, cuando se dio cuenta, la mitad de su empresa estaba en poder de un tercero. "El problema no fue de la tecnología, sino de la configuración de las contraseñas para el acceso y, sobre todo, del nivel de información que había subido", dijo el oficial.

Imagen: Gerd Altmann (Geralt) en www.pixabay.com (https://goo.gl/6fMVTr). Licencia CCO Creative Commons.

La industria automotriz avanza en la automatización de los vehículos.

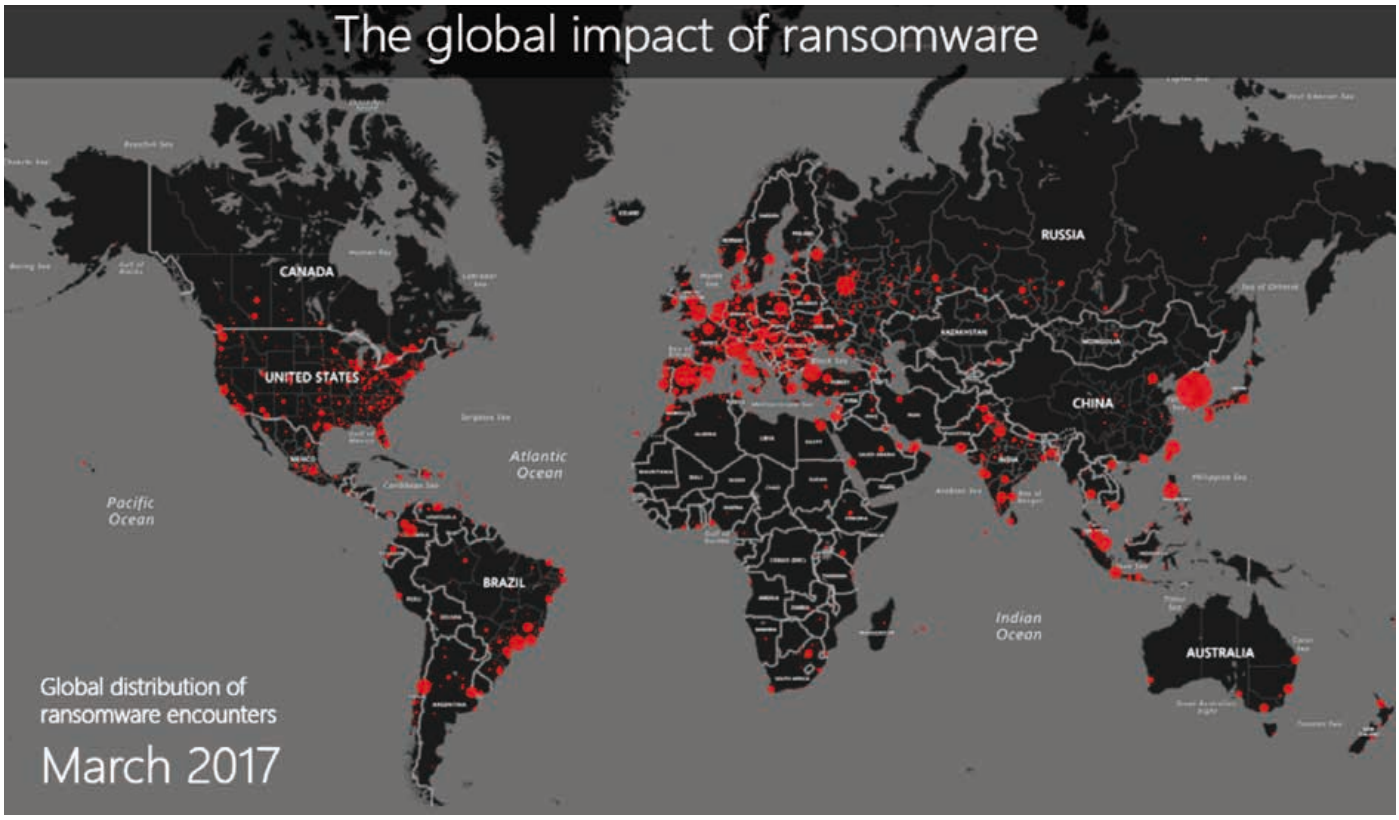
Imagen: Gerd Altmann (Geralt), en www.pixabay.com (https://goo.gl/NHKCJc). Licencia CCO Creative Commons.

Los usuarios del *cloud computing* deben tener en cuenta que es importante encriptar la información que suben ala nube.

Imagen: Gerd Altmann (Geralt), en www.pixabay.com (https://goo.gl/7Fgz3u). Licencia CCO Creative Commons.

La industria 4.0 ha sido denominada la cuarta revolución industrial o la ciberindustria del futuro.

La verdad sobre el ***ransomware***



Fuente: Microsoft Security Blog (https://goo.gl/vd88Mi)

Distribución global de encuentros de *ransomware* por mes. En el blog TechNet, de Microsoft, se puede consultar el mapa mes por mes, entre enero y junio del 2017.

La encriptación de datos para exigir rescate es un problema muy visible y que puede afectar a cualquier ciudadano, pero hay amenazas mucho más peligrosas, según Eddy Williems, evangelista principal de la firma alemana G Data, cuya función es explicar en palabras sencillas conceptos complejos de seguridad.

En la medida en que la gente se familiariza con las tecnologías conectadas a internet, ¿los riesgos para los ciudadanos son mucho mayores?

Sí, el problema con el internet de las cosas (IoT) es que los aparatos y objetos que se conectan a internet deberían ser seguros por diseño y por metodología, pero, desafortunadamente, y ese es el mayor riesgo de esos dispositivos, es que no se están desarrollando de forma segura.

¿Por qué sucede eso? ¿Porque los desarrolladores no están capacitados, porque no se invierte lo suficiente, porque el conocimiento tecnológico es insuficiente?

Es una combinación de factores. Integrar seguridad en los dispositivos podría demorar su salida al mercado o afectar sus precios. También es difícil encontrar la gente adecuada, pues el que sabe fabricarlos, probablemente no sabe asegurarlos, y cuando el fabricante busca ayuda en la industria de la ciberseguridad, se topa con que ella enfrenta sus propias limitaciones, porque faltan recursos humanos. Se requiere que la academia trabaje en la formación de ese tipo de expertos.

En su conferencia habló de contar la verdad sobre el *ransomware*, ¿a qué se refiere?

Mostré una imagen que evidencia las exageraciones de los medios de comunicación y de la industria de seguridad, porque se piensa que el *ransomware* es lo único; en realidad, en términos porcentuales es muy pequeño, pero, como es muy visible, nos olvidamos de amenazas como el *spyware* y el *adware* que espían nuestras actividades, o las que apuntan hacia nuestras cuentas bancarias o información personal. El *ransomware* está poniendo millones de dólares en los bolsillos de los cibercriminales y

no deberíamos subestimarlo, pero estas otras son más extendidas y potencialmente más peligrosas porque podrían afectar infraestructuras críticas o gobiernos y son las que realmente se constituyen en armas de guerra.

¿A quiénes van dirigidos los ataques de *ransomware*?

Son para obtener dinero fácil. Los bancos no son su objetivo real, las instituciones educativas sí, porque usualmente carecen de presupuesto suficiente para comprar defensas de calidad; es tentador atacarlas porque no pueden detenerse y son más proclives a pagar rescates costosos y sin mucha resistencia. Por otro lado, debemos separar dos tipos de *ransomware*: el indiscriminado cuyo fin es conseguir la mayor cantidad de dinero de las víctimas, y el que apunta directamente a alguna entidad. Un ataque dirigido es muchísimo más complicado y muchísimo más caro; para obtener dinero rápido es más fácil o eficiente lanzarlo al público general.

¿Qué tipo de información le encriptan al ciudadano y cuánto le piden en promedio para rescatarla?

Los costos dependen de variables como el precio del bitcóin, debido a que se exige el pago del rescate en moneda virtual, y también del poder adquisitivo de los países. Recuperar la información puede costar desde 100 dólares y el promedio es de 500 dólares. Lo que encriptan depende del *ransomware* en sí mismo; normalmente no se cifran programas, sino documentos de oficina, fotos, hojas de cálculo. También pueden

> "Los dispositivos que se conectan a internet deberían ser seguros por diseño y por metodología, pero no se están desarrollando de esa forma".
>
> Eddy Williams

tomar posesión del sistema e incluso las copias físicas de respaldo (*backups*) pueden ser cifradas. Probablemente, la mejor defensa reside en el uso de tecnologías muy nuevas como la supervisión de conducta, que consiste en analizar el comportamiento del *software* de cualquier aplicación que corra en el sistema, para, con base en criterios preestablecidos, determinar si se asemeja a un *ransomware*. También hay que contemplar productos específicamente diseñados contra esta amenaza y las tecnologías de protección contra *exploits* (fragmentos de *software* o datos que aprovechan vulnerabilidades de seguridad para que el sistema se comporte de manera errada).

¿Cómo sabe un ciudadano del común, que compra equipos y programas legales, si estos cuentan con esas protecciones?

Actualmente no existen pruebas comparativas especializadas en *ransomware*. Represento a la AMTSO (Anti-malware Testing Estándar Organization), una entidad independiente que fija los estándares para analizar los diferentes productos *antimalware* y ver cuáles funcionan bien, cuáles no y cuáles son mejores. Debido a su complejidad, es muy difícil simular el *ransomware*, estudiarlo para estandarizar pruebas, pero se está trabajando en eso.

Foto: Felipe Cazares

Eddy Williams, de G Data.

¿Qué recomendaciones puede darnos a los ciudadanos para protegernos?

El problema fundamental siempre será el factor humano. Los usuarios hacen clic irresponsablemente y una práctica sana es ser precavidos en el uso de los clics. Además, somos negligentes en la instalación de las actualizaciones en las aplicaciones; en gran medida si los sistemas operativos y las aplicaciones se mantuvieran al día, no habría que apoyar la responsabilidad en las soluciones antivirus. El aprendizaje es muy lento, pero las amenazas se hacen cada vez más sofisticadas y más rápidas.

¿Podemos vivir tranquilos conectados a internet?

Sí, podemos, pero hay tener ciertas precauciones básicas; la industria de la ciberseguridad está avanzando y cada vez es posible cubrir nuevos frentes. Es como caminar en el bosque: usted se aplica repelente porque los mosquitos pueden atacarlo; eso ayuda, pero siempre puede haber una serpiente y tenemos que ser muy cuidadosos.

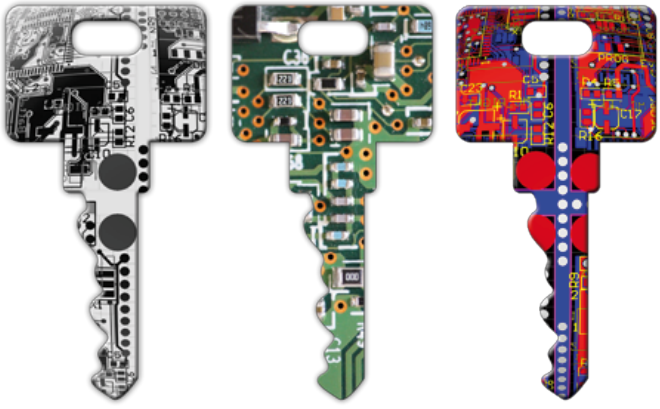


Imagen: Gerd Altmann (Geralt) en www.pixabay.com (https://goo.gl/H4Fj6P). Licencia CC0 Creative Commons.

Las llaves de la ciberseguridad están en manos de cada ciudadano. Prácticas sencillas como actualizar las aplicaciones ayudan a disminuir los riesgos.