CIBER SEGURIDAD

Una publicación del Córdoba Cyber-Security Hub

Los principales desafíos que enfrenta el sector de la ciberseguridad en Córdoba y la Región a través de reportajes, artículos y opiniones de expertos.

Córdoba
Cyber-Security Hub

Índice

CIBERSEGURIDAD
Una publicación del Córdoba Cyber-Security Hub.

Coordinación general: **Luciano Crisafulli**
Producción periodística: **Natalia Riva**
Diseño Gráfico: **Victoria Monguillot**

Para Comunicarte con Córdoba Cybersecurity Hub, escribinos al mail
cbacybersecurityhub@gmail.com

A través de las redes sociales del Córdoba Cyber-Security Hub

Córdoba Cybersecurity Hub

Córdoba, Argentina - Julio de 2022

“El sector de la ciberseguridad es estratégico para el desarrollo de la Córdoba del futuro”

Dr. Martín Llaryora - Intendente de la ciudad de Córdoba

En los últimos años se ha puesto en relieve la dependencia que tenemos los ciudadanos respecto de las nuevas tecnologías. La vida diaria gira alrededor de actividades cada vez más digitalizadas y, por consiguiente, más sensibles a amenazas cibernéticas.

En la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio. El bajo costo y riesgo que conllevan estos delitos han sido factores clave en su crecimiento. Con el simple uso de un celular conectado a Internet, los ciberdelincuentes pueden causar grandes daños. Según un informe del BID, “el crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo”.

Si bien los gobiernos de la Región somos conscientes de la necesidad de proteger el espacio digital, la ciberseguridad no ha ganado hasta el momento presencia destacada en la agenda política con prioridad. Pero esta realidad irá cambiando en el corto y mediano plazo a medida que cada vez más ciudadanos y empresas sean víctimas de nuevos ciberdelitos.

Los esfuerzos para abordar los ciberataques deben ser de naturaleza multidimensional e integral, porque se requiere una variedad de factores para construir una cibersociedad resistente. Debemos trabajar mancomunadamente para crear una cultura de ciberconciencia y formar cada vez más profesionales calificados. La puesta en práctica de políticas integrales de ciberseguridad permitirá a las ciudades disfrutar de los beneficios de la transformación digital, protegiendo a sus ciudadanos y potenciando su actividad económica.

Con este objetivo es que, desde la Municipalidad de Córdoba, hemos tomado la decisión de conformar un Hub de Ciberseguridad en Córdoba con visión internacional, pensado para toda la Región. Participa un conjunto de más 40 organizaciones entre empresas, startups, universidades y áreas de gobierno que ya comenzaron a trabajar colaborativamente para posicionar a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad que brinda productos y servicios de alta calidad a organizaciones públicas y privadas.

Particularmente para nuestra ciudad de Córdoba, estamos convencidos que el sector de la ciberseguridad es estratégico, ya sea por su gran dinamismo dentro del propio sector tecnológico y por ser clave para el crecimiento de la Economía del Conocimiento, motor de las futuras generaciones, como para mejorar la calidad de vida de los ciudadanos.

De Córdoba a la Región: un hub de ciberseguridad para fortalecer un sector estratégico de la economía

Conformado a finales de 2021, el Córdoba Cyber-Security Hub tiene como objetivo posicionar a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad. Lo integran instituciones públicas, empresas privadas y especialistas en la materia. En las primeras reuniones con los miembros del hub, ya se delinearon las principales líneas de acción y se detectaron las fortalezas y debilidades del sector.

Proteger los activos digitales frente a las amenazas que existen en la red y la seguridad de la información, software, datos y sistemas se ha convertido en una obligación para todas las organizaciones privadas y públicas y se vuelve un tema cada vez más relevante en la vida de las personas. Dentro del sector tecnológico, la ciberseguridad es una de las verticales con mayor crecimiento, ya que representa una de las claves para el crecimiento sostenible del sector.

En este contexto, y con el objetivo de posicionar a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad que brinda productos y servicios de alta calidad a organizaciones públicas y privadas, un grupo de empresarios, emprendedores, académicos e instituciones referentes en la temática, coordinados desde la Secretaría de Planeamiento, Modernización y Relaciones Internacionales de la Municipalidad de Córdoba, formó el Córdoba Cyber-Security Hub.

Actualmente el Hub está conformado por 44 miembros entre los que se encuentran organizaciones públicas y privadas del sector del conocimiento. En los últimos meses se han venido realizando encuentros de co-creación y planificación en donde se definieron los principales desafíos que enfrenta el sector en Córdoba y se propusieron las primeras líneas de trabajo para promover su crecimiento.

Sobre la conformación y puesta en marcha del Hub de Ciberseguridad, Alejandra Torres, secretaria de Planeamiento, Modernización y Relaciones Institucionales de la Municipalidad de Córdoba destacó la creación de este espacio y se comprometió a trabajar en este sector clave de la economía del conocimiento que es la ciberseguridad.

> **Es muy importante que sigamos trabajando conjuntamente, articulando lo público y lo privado para seguir posicionando a Córdoba regionalmente. Las condiciones están dadas para que el sector pueda crecer apalancado en el talento de nuestros emprendedores y programadores.**
>
> **Alejandra Torres**

Por su parte, Luciano Crisafulli, director de CorLab, remarcó que el sector de la ciberseguridad es estratégico para la ciudad de Córdoba, al menos, por tres razones. “En primer lugar, gracias a la ciberseguridad, pueden prevenirse incidentes personales o familiares, mejorando la calidad de vida de las personas. Además, genera un impacto positivo sobre la competitividad de las empresas asegurando el correcto funcionamiento de sus recursos y herramientas digitales. Finalmente, este es uno de los sectores más dinámicos dentro del sector tecnológico y contribuye en forma directa con el crecimiento sostenible del mismo”, enumeró.

Para Carlos Aguirre, presidente de la Asociación Argentina de Derecho Informático (Adiar), “plantear el estudio, análisis y creación de una organización como el Hub que maneje la ciberseguridad desde el campo público como del privado es super importante”. En esta misma línea, Ignacio Casanovas, cofundador Capazeta, una empresa que brinda soluciones de ciberseguridad, aseguró que el hecho de que exista “que exista un Hub de Ciberseguridad en la ciudad de Córdoba es muy importante sobre todo por el apoyo del sector público que permite que todo esto funcione de una forma mancomunada y coordinada”.

El especialista en Ciberseguridad y director de Proofpoint Argentina, Guillermo Colsani, también celebró la decisión de crear un Hub de Ciberseguridad, ya que lo considera un espacio “clave” para generar interés en la comunidad estudiantil y en las empresas y, de esta forma, posicionar a la ciberseguridad como una opción más cotidiana en las vidas de las personas. “El Hub también va a elevar el nivel de exposición de los participantes, aumentando la inteligencia colectiva para la defensa; creando así un círculo virtuoso autosustentable y con perspectivas de negocio muy prometedoras”, completó.

Principales líneas de acción del Hub

En las reuniones que se vienen realizando con los miembros del Hub, se planteó, como el principal desafío, generar mayor conciencia y cultura sobre ciberseguridad en la ciudadanía en general, lo que implica el diseño e implementación de acciones de sensibilización y formación para posicionar en organizaciones públicas, privadas y en la comunidad la importancia de la ciberseguridad.

Asimismo, otro de los ejes que se estableció como prioritario, tiene que ver con la necesidad de promover la demanda por servicios de ciberseguridad por parte de organizaciones públicas y privadas e incrementar el nivel de inversión que realizan en este tema.

El último desafío que se planteó, que no es un tema menor, conlleva el desarrollo de acciones para promover la generación de nuevos talentos especializados en ciberseguridad para atender a los requerimientos del sector.

De esta manera, para atender las problemáticas y desafíos mencionados, desde el Hub se establecieron algunas líneas de acción y trabajo entre los que se destacan: la organización de un congreso regional de Ciberseguridad, de jornadas de concientización con diferentes sectores, de competencias de seguridad informática (CTF) y de talleres y capacitaciones especializadas, la creación de un directorio de empresas y emprendimientos de ciberseguridad, la generación de un equipo de respuesta ante emergencias informáticas (CERT) y la creación de canales de comunicación y difusión especializados en la materia.

Fortalezas y debilidades

La confección de un listado de fortalezas y otro de amenazas en el sector de la ciberseguridad en Córdoba fue otro de los resultados de los encuentros de los miembros del Hub. Estas definiciones y puestas en común sirven para delinear líneas de acción, trabajar para modificar los aspectos negativos y potenciar los positivos.

En este sentido, según enumeran los especialistas en el tema, las fortalezas del sector en Córdoba capital son varias, comenzando con que se cuenta con recursos humanos (profesionales) capacitados y con experiencia; también se destaca la existencia de universidades con programas de estudios en ciberseguridad; se cuenta con un número significativo de empresas especializadas en ciberseguridad; y por último, existe una red consolidada de trabajo interdisciplinario y networking.

Sin embargo, también existen debilidades en el sector que son las principales cuestiones hacia donde el Hub tendrá que orientar sus esfuerzos. Ellas son: falta de concientización y cultura social en ciberseguridad (en empresas e instituciones); poca inversión en ciberseguridad por parte de empresas y gobiernos; falta de coordinación y de trabajo en comunidad por parte del sector; desconexión academia- empresas; falta de capacitaciones en ciberseguridad, en especial en español; falta de retención de recursos humanos capacitados; falta de apoyo estatal para auditorías y falta de visión e integración internacional del sector.

Nota de Tapa

Académicos, empresarios, Emprendedores e instituciones referentes en ciberseguridad, coordinados desde la Secretaría de Planeamiento, Modernización y Relaciones Internacionales de la Municipalidad de Córdoba, formaron el Córdoba Cyber - Security Hub.

Actualmente el Hub está conformado por 44 miembros entre los que se encuentran organizaciones públicas y privadas del sector del conocimiento.

La importancia de un Hub de Ciberseguridad

Para contextualizar el peso que hoy tiene contar con un espacio de este tipo, cabe destacar que los incidentes de inseguridad informática en la Argentina se duplicaron en el último año, según los datos registrados por el equipo de respuesta a emergencias informáticas (Cert.ar) dependiente de la Dirección Nacional de Ciberseguridad.

Según el reporte del año 2021, "en el año 2020 la cantidad de incidentes reportados fue de 226", mientras que "en el año 2021, fueron 591"; y de ellos el 55,24% corresponden a casos de phising (robo de identidad), seguido por la modificación no autorizada de la información (15,20%) y por el spam, en cerca del 10%.
Otro informe de Avast, una de las empresas líderes a nivel mundial en ciberseguridad, destaca que en el país la probabilidad de que una empresa se encuentre con cualquier tipo de malware para PC es del 19,07%. En comparación con el promedio mundial, los argentinos tienen un mayor riesgo de toparse con todo tipo de amenazas informáticas, lo que conlleva pérdidas económicas cada vez mayores.

Por último, según la principal conclusión de la Encuesta Global Digital Trust Insights 2022 de PwC, realizada a 3.600 CEO y otros directivos a nivel global, el 30% de los ejecutivos argentinos no comprende en su totalidad el riesgo de filtraciones de datos a través de terceros; y un 20% muestra poca o nula comprensión de ese riesgo. "Estos hallazgos son alarmantes, en especial en un contexto en que más del 41% de los ejecutivos argentinos encuestados esperan un aumento de los delitos informáticos para 2022", destacó PwC.

Cuáles son los miembros del

Córdoba Cyber-Security Hub

Empresas Tecnológicas

- Accefy
- ACsoft Soluciones informáticas
- Apex America
- Arcor
- ARTSSEC
- Capazeta
- Caylent
- Cedi Consulting
- Cloudshine
- Daitek
- Danka
- Digital Content Machine
- Eclypsium
- Ecogas
- Fortinet
- Gates consulting
- Jemersoft
- Konecta
- Mobbex
- Pabex
- Pagos 360
- Patagonia Security
- ProofPoint
- Punto Net Soluciones SRL
- RAM IT
- Sello de Competencia Digital
- Tedicom
- Vectus
- Vicino Software Factory
- VU Security
- Xecur IT

Cámaras y Agrupaciones Empresariales

- Asociación Argentina de Derecho Informático (ADIAR)
- Cluster Córdoba Technology
- Córdoba Hacker Space
- Laboratorio de Redes y Ciberseguridad (LARYC)
- CIIECCA
- Colegio de Abogados de Córdoba.

Instituciones Educativas y Universidades

- Universidad Blas PascalUniversidad Siglo 21
- Universidad Nacional de Córdoba
- UTN Facultad Regional Córdoba
- Instituto Universitario Aeronáutico

Organizaciones Públicas

- Ministerio de Ciencia y Tecnología de la Provincia de Córdoba
- Dirección de Ciberseguridad. Presidencia de la Nación
- Municipalidad de Córdoba

Con un fuerte llamado a la concientización y ante más de 800 personas, se realizó el "1er Congreso de Ciberseguridad, desde Córdoba Capital para toda la Región"

Este multitudinario encuentro marca un hito para la ciberseguridad en Córdoba, no sólo por su impacto en el sector tecnológico, sino también en el sector productivo y en la ciudadanía en general. Disertaron más de 20 especialistas representantes de universidades, empresas, startups y organismos públicos, quienes se enfocaron en los desafíos y oportunidades en materia de seguridad informática.

La participación de más de 800 personas en "1er Congreso de Ciberseguridad, desde Córdoba Capital para toda la Región" superó ampliamente las expectativas. Participaron asistentes presenciales y otros conectados vía streaming desde distintos puntos de la Región. De esta manera, el Congreso marca un hito en la ciudad de Córdoba para el sector tecnológico y de la ciberseguridad. Además, demuestra el interés por la concientización sobre la relevancia de la seguridad informática.

El Congreso fue organizado por el Córdoba Cyber Security Hub, una iniciativa de la Municipalidad de Córdoba que reúne a empresas, universidades y otras organizaciones públicas, y que tiene como objetivo posicionar en la Región a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad.

En el Congreso disertaron referentes tecnológicos especialistas en ciberseguridad. Lo hicieron en diferentes paneles donde se analizaron los principales desafíos que enfrentan las empresas y la ciudadanía en términos de seguridad informática. También se abordaron temas vinculados a la formación de talentos en el sector y se contó con un panel para debatir aspectos normativos y jurídicos relacionados a la ciberseguridad.

El secretario de Economía y Finanzas, Guillermo Acosta, abrió el Congreso destacando la importancia de la conformación de un Hub de Ciberseguridad en donde participan empresas, organizaciones, universidades y sector público. "Gestionamos con mesas de trabajo, que son un espacio colaborativo donde trabajamos conjuntamente con otros sectores y, a través del diálogo, buscamos consenso para diseñar e implementar políticas públicas. Una de esas mesas es la de Ciberseguridad, un tema fundamental y estratégico para la ciudad."

A su turno, Alejandra Torres, secretaria de Planeamiento, Modernización y Relaciones Internacionales de la Municipalidad de Córdoba, realizó el cierre del encuentro moderando el panel donde se presentaron los desafíos del Córdoba Cyber Security Hub y destacó que "no se puede abordar la transformación digital de la ciudad de Córdoba sin tener en cuenta la ciberseguridad". Sobre la conformación y puesta en marcha del Hub, indicó: "Es muy importante que sigamos trabajando conjuntamente, articulando lo público y lo privado para seguir posicionando a Córdoba regionalmente. Las condiciones están dadas para que el sector pueda crecer apalancado en el talento de nuestros emprendedores y programadores".

¡Podés revivir el Congreso!

Para quienes quieran revivir todas las charlas o para quienes no pudieron participar, pueden hacerlo a través del canal de YouTube de la Municipalidad de Córdoba (www.youtube.com/user/cordobagovar). Allí está todo el contenido del Congreso.

Convocatoria de Artículos de Divulgación

Otra actividad que se realiza en el marco de este Congreso es la convocatoria a Artículos de Divulgación dirigida a profesionales del área que quieran transferir sus conocimientos sobre casos, experiencias, buenas prácticas, tendencias e investigaciones relacionadas a la ciberseguridad en general. Los que estén interesados pueden ingresar al sitio del Córdoba CyberSecurity Hub (https://cybersecurityhub.cordoba.gob.ar/) y allí encontrarán las bases y condiciones para participar.

Principales definiciones de las exposiciones y paneles

“Los desafíos de la seguridad informática en Córdoba y la Región”

Estuvo a cargo de Enrique Dutra, consultor especialista y referente en ciberseguridad, fundador de PuntoNet Soluciones. Las principales definiciones del panel fueron:

“No existen estadísticas reales sobre los ataques de ciberseguridad en Córdoba porque las organizaciones no se animan a decir cuando sufrieron un ataque (les da una mala imagen), pero está comprobado que luego de la pandemia han crecido muchísimo. Las personas hoy confían ciegamente en la tecnología porque no son conscientes del riesgo que conlleva. Tenemos que trabajar en la formación de la gente en esta temática, trabajar en comunidad y preparar a las empresas”.

“Hay que salir del estado de confort en el que se encuentra cada uno y empezar a trabajar en comunidad. Sin ese concepto no vamos a avanzar nunca como sociedad: en el nicho de la ciberseguridad no se comparten muchos conocimientos y hay que romper con esa estructura porque hoy hay trabajo para todas las especialidades”.

“Las problemáticas de ciberseguridad son las mismas en todas partes del mundo. Pero lo que más preocupa de Córdoba es que no tenemos un extranjero tratando de vulnerar la privacidad, sino que tenemos gente local que vulnera las compañías y trata de obtener un rédito económico por ello”.

“A la gente se le ha dado acceso a muchas herramientas tecnológicas pero nunca se hizo un trabajo de concientización que explique los riesgos que conlleva el uso de ellas”

“Smart City, ¿Cómo hacerlo correctamente?”

A cargo del experto en ciberseguridad, César Cerrudo, Director de Investigación en Strike (Uruguay). El especialista profundizó en los desafíos de las ciudades inteligentes en materia de seguridad para los vecinos y enumeró las principales cuestiones para mejorar:

“Una smart city es una ciudad que utiliza tecnología para automatizar y hacer más eficientes los servicios con el objetivo de mejorar la calidad de vida de sus ciudadanos. Es decir, la ciudad decide brindar mejores servicios para ser más eficiente a través de la tecnología”.

“La mayor parte de las tecnologías usadas en ciudades inteligentes es muy insegura, fácil de hackear y muy expuesta a ciberataques. Esto sucede, en la mayoría de los casos, porque cuando los gobiernos deciden implementar tecnologías no se hacen testeos previos para confirmar que esa nueva tecnología sea realmente segura y no ponga en riesgo y cause problemas a los ciudadanos. Es un gran desafío para todas las ciudades testear y hacer una auditoría previa a las tecnologías que incorporen y asegurarse que cumplan las funciones que tiene de una manera segura para evitar ciberataques fácilmente. No sólo es importante testear la funcionalidad, sino también es imprescindible testear la seguridad”.

“Hay mucha falta de concientización sobre ciberseguridad y falta de conocimiento en general. Es necesario que todas las personas que intervienen en la adquisición e implementación de tecnología tengan conocimientos específicos en la materia para asegurar que lo que se implementa sea seguro mediante testeos”.

“Hoy somos muy dependientes de la tecnología y cada vez vamos a depender más y más. Entonces se hace necesario que todo el mundo conozca de ciberseguridad aunque sea de temas básicos y los vaya profundizando a medida que lo necesite. No hay que utilizar tecnología sin antes comprobar su seguridad y que tenga encriptación, autenticación, etc”.

“¿Cómo afecta un ciberataque a las personas?”

A cargo de Matias Koller de Grupo Vectus y Jorge Karim Hitt de Bancor, moderado por Joaquín Varela de Patagonia Security. Aquí aseguraron que si bien la falta de datos estadísticos no permite tener precisiones, el “phishing” (ataques a través de correo electrónico) es lo más recurrente como delito hacia las personas.

“Si bien no hay estadísticas en la Argentina, uno de los ataques más conocido a las personas es a través de la utilización del correo electrónico, y más en el ámbito empresarial es el ransomware y el malware en donde se restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción”.

“En cuanto a los ataques bancarios, se puede decir que, en definitiva, todos confluyen en quebrar la voluntad del cliente a través de la ingeniería social o ‘hacking social´ que hace referencia que el cliente apague su racionalidad y de alguna forma interactúe con el delincuente dando datos de seguridad de sus productos bancarios, datos que en un estado de plena conciencia no hubiera divulgado. Esto es lo que históricamente se conocía como el cuento del tío”.

“La reputación personal es otro de los objetivos usuales. Algo que realizan con plataformas de phishing, que imitan el sitio web de alguna empresa o entidad, para acceder de forma ilegal tanto a las cuentas de un usuario como a sus redes sociales. En estos casos, se emplean excusas como “alguien te ha mandado un mensaje privado” y “por motivos de seguridad es necesario que se cambien las claves”. Esto solo es una estrategia para lograr que introduzcas tus claves y conseguir tus datos para suplantar tu identidad”.

“Es muy difícil quebrar la seguridad de las plataformas digitales de los bancos porque todas funcionan bajo ciertos parámetros de seguridad (como la doble autenticación) que dan, en cierto modo, un nivel de seguridad que no llega a afectar la transacción del cliente”.

“Se debe trabajar enérgicamente en la educación y capacitación del cliente bancario. La digitalización de los distintos servicios y productos generó un ´gap´entre la conciencia y educación del cliente y la tecnificación de estos productos. Esto aumentó mucho durante la pandemia en donde la mayoría de los clientes comenzó a operar a través del home banking”.

“Nuevas tecnologías para una mayor ciberseguridad de las empresas”

En el siguiente panel se avanzó con las “Nuevas tecnologías para una mayor ciberseguridad de las empresas”, y estuvo a cargo de Edgardo Enrique Schunk de Grupo Arcor, Ignacio Casanovas de Capazeta y Germán Parisi de Pabex (moderado por Daniel Daniele, de Córdoba HackerSpace). Entre varios conceptos, sobresalió la importancia de desarrollar softwares más seguros, lo que muchas veces implica ir en contra de la usabilidad. Las principales definiciones, fueron:

“Con la pandemia, las empresas pasaron de tener sólo un pequeño porcentaje de gente trabajando de forma remota a tener la totalidad de los colaboradores trabajando en esta modalidad. Eso fue un gran desafío porque las empresas tuvieron que ampliar los sistemas de conexiones sin exponer los datos”.

“Lo que hoy se visibiliza, sobre todo después de la pandemia, es la transversalidad que adquirió la ciberseguridad: ya no sólo es de interés de los profesionales, sino que pasó a un ámbito más mundano que hasta, incluso, trasciende el ámbito laboral y las generaciones. El cambio más grande tiene que ver con el uso de software, hoy es usado por todo el mundo por lo que el desafío es hacer softwares más seguros que muchas veces implica luchar contra la usabilidad. Se trabaja mucho actualmente con la experiencia de usuario (UX), pero se deja de lado el costado de la seguridad”.

“En cuanto si una empresa tiene que tener sus propios especialistas en ciberseguridad o tercerizar este servicio, lo ideal es general un esquema híbrido. Tener la seguridad delegada te da un segundo puto de vista lo cual es fundamental y necesario; sin embargo la seguridad tiene que estar contemplada desde el minuto cero de una empresa y que todo el equipo de trabajo tenga consciencia de la importancia de esta temática”.

“Formación de competencias para desempeñarse en ciberseguridad”

De la mano de Eduardo Casanovas del Instituto Universitario Aeronáutico y fundador de Capazeta, Miguel Solinas de la Universidad Nacional de Córdoba, y Fabián Gibellini de la Universidad Tecnológica Nacional, moderados por Ileana Barrionuevo de Naranja X. En el mismo se destacó la importancia de que las Universidades comiencen a tener carreras específicas sobre ciberseguridad y que dejen de ser módulos o materias optativas en el marco de otras carreras. Otros conceptos que se abordaron fueron:

“Es necesario incorporar la temática de la ciberseguridad en el ámbito académico en los distintos niveles. En este momento en muchas carreras de varias universidades se está trabajando en la implementación de contenidos relacionados y también tomar el tema de la ciberseguridad como habilidades blandas. Hay que incorporar el tema de la ciberseguridad en los planes de estudios no solo de carreras afines y hay que trabajar en conjunto entre todas las universidades para plantear una carrera específica. Ese es un gran desafío”.

“Hay que empezar desde los niveles más bajos con la concientización. Los estudiantes tienen que entender que se empieza por la defensa, es decir, con el desarrollo seguro. Es ahí donde hay que hacer fuerza y es el desafío más grande con los cambios tecnológicos asociados a nuevas aplicaciones y desarrollos. Si no hacemos que esos desarrollos sean seguros, por más que concienticemos, no va a alcanzar”.

“Sobre la formación en ciberseguridad, es importante destacar que se trata de un conocimiento consolidado, no se debe caer en la tentación de redescubrir o redefinir el conocimiento sobre ciberseguridad. Está acordado a nivel global, ya existe una documentación que nos permite acceder a cuáles son los ítems del dominio de la ciberseguridad y está íntimamente relacionado a la formación en ingeniería de software y a ciencias de la computación. Revisando esos dominios nos vamos a dar cuenta cuáles son las temáticas que debemos impartir en las carreras de grado y posgrado para formar profesionales en el área de ciberseguridad”.

“Desafíos para promover la generación de nuevos talentos en ciberseguridad”

A cargo de Guillermo Colsani de Proofpoint y de Carolina Marconetto de Apex América, moderado por Antonella De Caro, de Salesforce. Se destacó la importancia del rol de las empresas en la formación de talentos especializados en ciberseguridad. Otros conceptos que se abordaron, fueron:

“En este último tiempo, en las empresas está sucediendo una evolución en ciberseguridad similar a lo que sucedió con la innovación. Primero había un experto en innovación, después un departamento específico y luego todas las áreas de la empresa debían innovar. Ahora veo que está sucediendo lo mismo con la ciberseguridad. Hoy las empresas necesitan que todos participen en la capacitación y concientización de esta temática para familiarizarse con la problemática y convertirse en protagonistas para resolverla”.

“Para ser un colaborador crítico en ciberseguridad no es necesario pertenecer a un nicho de gente super experta, sino que hoy se está expandiendo hacia otras áreas. Se habla mucho de la importancia del testing, una persona puede testar sin ser un experto. Y si alguien aprende cómo trabajan los atacantes, puede emular esos ataques y agregar valor”.

“Con respecto a la conformación de equipos de ciberseguridad en las empresas, es recomendable que existan equipos híbridos con personas tercerizadas que no están embebidas en la problemática de la compañía. Muchas veces pasa que las personas que desarrollan el software in house pueden estar un poco viciadas lo que genera puntos ciegos. Es bueno que los equipos tercerizados sean contratados esporádicamente para que hagan testeos y armen un backlog de vulnerabilidades”.

“Aspectos normativos y jurídicos en ciberseguridad”

El panel sobre “Aspectos normativos y jurídicos enciberseguridad” estuvo a cargo de Franco Pilnik del Ministerio Público Fiscal de Córdoba, Carlos Dionisio Aguirre de Adiar y Segundo Carranza Torres del Estudio Carranza Torres. Aquí quedó demostrado el aspecto fundamental relacionado con los tiempos de legislación y procedimientos para que el marco regulatorio no quede tan desfasado respecto a la velocidad de los cambios tecnológicos y de los hábitos de consumo sobre dichas tecnologías.

“El derecho suele correr detrás de los hechos. En el ámbito de la tecnología, esta brecha entre realidad y ley usualmente es mayor, principalmente debido a la velocidad exponencial del desarrollo tecnológico”.

“Hoy, ningún país está bien en materia de ciberseguridad. Argentina está bastante más atrás si se tiene en cuenta que las leyes corren detrás de la realidad; recién ahora se está empezando a trabajar muy bien en algunos aspectos. Los temas tecnológicos evolucionan tan rápido y hay que estar permanentemente al tanto de las últimas novedades trabajando a la par de los informáticos para poder entender y, de esta manera, generar seguridad desde lo jurídico”.

“Entre las principales normativas nacionales e internacionales vigentes respecto al área de seguridad informática se encuentran la ley de Delito informático; la ley de Protección de datos personales; la ley de Firma digital; la ley de Grooming”.

“Principales ejes de trabajo del Córdoba Cyber-Security Hub”

Finalmente, Alejandra Torres hizo el lanzamiento formal del Hub y fueron presentados los tres ejes principales de trabajo por Victor Stronati de Naranja X, Luciano Crisafulli de CorLab y Guillermo Colsani de Proofpoint. Estos ejes obedecen a desafíos de la seguridad informática en cuanto a la ciudadanía, las empresas y la formación de talentos.

“El eje Ciudadanía responde al desafío: ¿Cómo podríamos generar mayor conciencia y cultura sobre ciberseguridad en organizaciones públicas, privadas y en la ciudadanía en general?. Implica el diseño e implementación de acciones de sensibilización y formación para posicionar en organizaciones públicas, privadas y en la comunidad en general la importancia de la ciberseguridad”.

“El eje Pymes (o demanda) responde al desafío: ¿Cómo podríamos hacer que se incremente la inversión en ciberseguridad de parte de organizaciones públicas y privadas?”. Implica el diseño e implementación de acciones que incrementen la demanda por servicios de ciberseguridad”.

“El eje Recursos Humanos responde al desafío: ¿Cómo podríamos generar una mayor cantidad de talentos especializados en ciberseguridad? Implica el diseño e implementación de acciones para promover la generación de nuevos talentos especializados en ciberseguridad”.

“La ciberseguridad en el sector público debe ser tenida en cuenta por sobre todas las cosas”

El especialista en ciberseguridad, Enrique Dutra, advierte sobre el gran impacto que tienen los ciberataques en las áreas gubernamentales y recomienda que se definan planes de trabajo reales. Y considera que la conformación del Cyber Security-Hub vino a sacar del estado de confort a todos: sector público, universidades, organizaciones públicas y privadas.

Al igual que las empresas y las personas, las áreas gubernamentales también son muy vulnerables a los ataques cibernéticos. La transformación de base hacia el gobierno electrónico y digital en la Argentina trae consigo nuevas realidades y aspectos a tener en cuenta. Para Enrique Dutra, especialista el ciberseguridad y fundador de PuntoNet, la ciberseguridad en el sector público debe ser tenida en cuenta por sobre todas las cosas: “No nos olvidemos que una ciudad funciona con servicios que son usados por la ciudadanía, y si es víctima de un ciberataque, podría afectar a miles de personas”, destaca.

A modo de ejemplo, Dutra recordó que en plena pandemia unos ciberdelincuentes dejaron fuera de servicio la red de distribución de agua de la ciudad de Curitiba en Brasil, sobre todo en la zona donde estaban los hospitales con mayor cantidad de pacientes con Covid-19 y el impacto fue muy alto.

“La ONU tiene una gran preocupación sobre la seguridad de los servicios esenciales (agua, gas, energía, bancos, salud, etc), son unos de los focos principales en las ciudades del mundo y ante un ciberataque el impacto es importante por ser muy masivo y seguramente no es fácil de reemplazar”, indicó el especialista

Por otro lado, advirtió que la complejidad del sector público y “cierta inmadurez en protecciones ante un ciberataque”, siempre provocan que un ciberdelincuente logre su objetivo. Para esto, aconseja que se definan planes de trabajo reales, ya que “lineamientos y normativas existen desde hace años”.

- ¿Por qué considerás que la ciberseguridad es central hoy para los negocios, empresas e individuos?

Las organizaciones o las personas seguramente tienen información que, sí es obtenida por un tercero de alguna manera, éste puede sentirse beneficiado. Los años pasaron y efectivamente tener información es tener poder. Hoy ya no podemos hablar sólo de antivirus o backup, términos frecuentes cuando se plantean aspectos de seguridad y de protección. El escenario se ha complejizado desde el momento en que todos estamos hiperconectados. Internet ya forma parte de nuestras vidas, por lo que hay que empezar a protegernos desde el momento cero en el cual nos conectamos.

Los delincuentes o estafadores que usan la tecnología como medio para lograr sus objetivos se han convertido en ciberdelincuentes. Para protegernos debemos utilizar mecanismos, procedimientos y conductas que estén alineados a la seguridad de cara a Internet, de allí que mencionamos ciberseguridad. Para dar un ejemplo simple, si hablamos del celular, éste se ha convertido en nuestra plataforma de trabajo (correo, contactos, mensajes, etc), contiene nuestros datos privados (datos de salud, fotos, aplicaciones, etc) y ahora se ha convertido en nuestra billetera.

Por último, y no es un dato menor, las organizaciones empezaron a entender que la información tiene un valor como un activo más. Si un ciberdelincuente cifra esa información y no hay como restaurarla, hay que pagar un rescate que ronda los USD 40.000. Además, surge el problema de cómo dejamos estipulado en los libros contables que se usó ese dinero para pagar un secuestro de información. Pero más impacto tiene si esa información el ciberdelincuente la expone a Internet, ya que la reputación de la organización se vería seriamente afectada.

- ¿Cuáles son los ataques más frecuentes en el ámbito corporativo y en el personal?

Las amenazas con las que se enfrentan las personas y las organizaciones no difieren mucho entre sí. Las personas siempre son foco de ataques de personas inescrupulosas, que intentan mediante alguna técnica de engaño lograr el objetivo. Antes de la pandemia hablábamos constantemente del correo que trataba de que el usuario accediera a un sitio y pusiera sus datos de tarjeta de crédito (phishing). Cuando comenzó la pandemia, este tipo de ataque creció y lo sigue haciendo de

manera importante. Ahora tenemos mensajes de texto (smishing), llamadas telefónicas o mensajes de Whastapp (vishing). Crece porque el usuario confía demasiado en los dispositivos electrónicos y no piensa que del otro lado puede existir una persona que intentará engañarlo para robarle.
En las organizaciones ocurre esto mismo, pero el foco no siempre es robarle al usuario, si no que con alguna acción termine haciendo algo que pueda debilitar el sistema de seguridad de dicha organización. Si el ciberdelincuente no logra el objetivo de esta manera, realiza un ciberataque directo, como viene ocurriendo en estos últimos meses, en donde están extorsionando a las organizaciones una vez vulneradas y si no logran obtener el beneficio, publican en la Web los datos obtenidos.

- ¿Cómo ve el desarrollo en Córdoba de profesionales en materia de ciberseguridad? ¿Qué potencial tiene?

Hoy el mundo está necesitando cada vez más profesionales en ciberseguridad. Hay muchas áreas para cubrir (es como la medicina, los estudiantes pueden profesionalizarse en diferentes áreas, hay para todos los gustos) y Córdoba, concentrando a una gran masa de estudiantes de todas las provincias, es el lugar propicio para el desarrollo de profesionales en materia de ciberseguridad. Es cierto, que la oferta de capacitaciones por el momento es pobre para la demanda que existe. Pero es algo por lo cual todos estamos trabajando en el Hub.

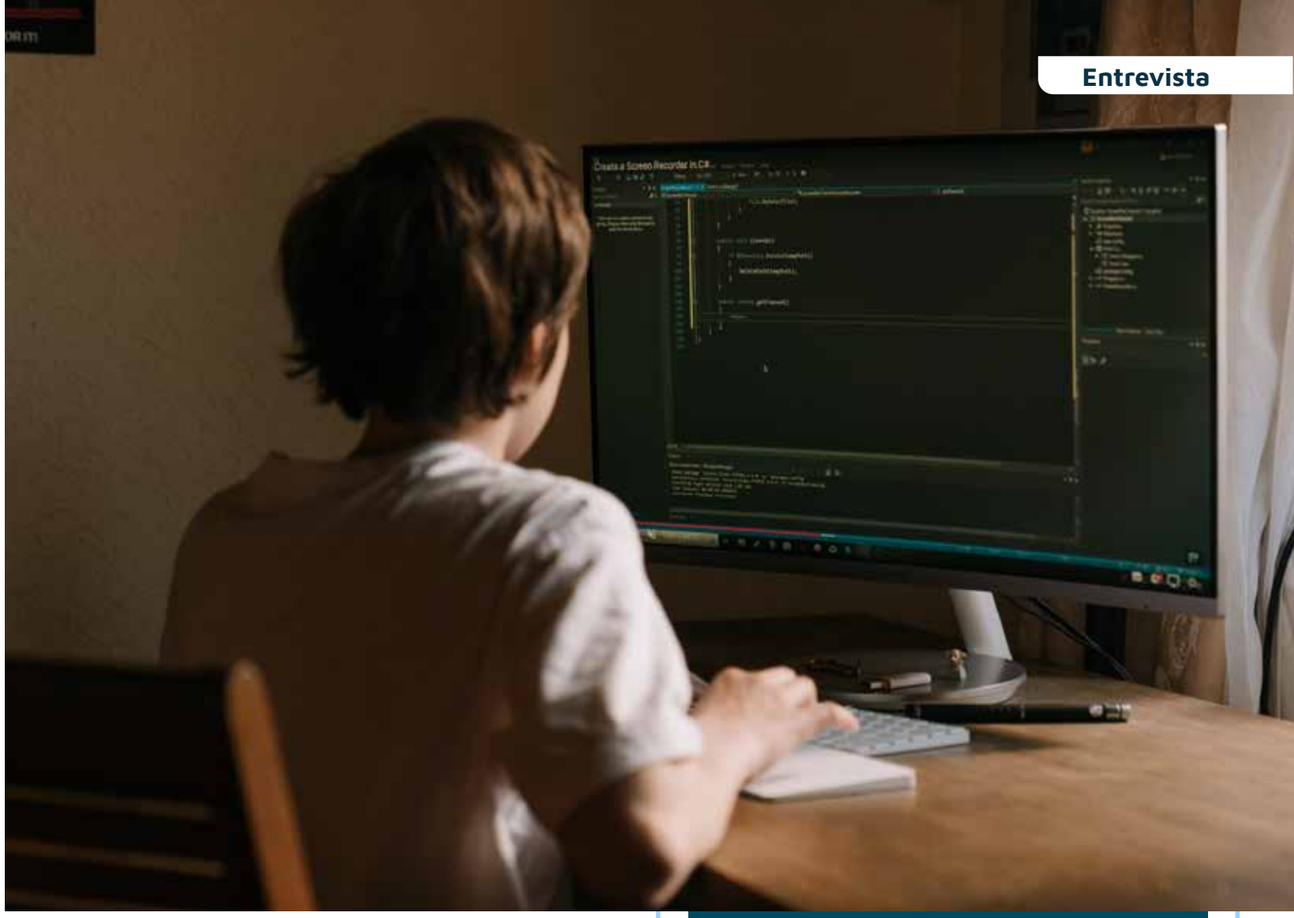
- ¿Cuáles cree que son los principales desafíos en materia de ciberseguridad?

Pensando en la Norma ISO 27000 y en los procesos de las organizaciones, la ciberseguridad debe velar por la disponibilidad (la información siempre accesible), integridad (que no esté adulterada en ninguna de las maneras) y confidencialidad (sólo accedido por las personas a quienes se les dieron los permisos).

Ahora bien, ¿qué sucede con las personas? Es necesario capacitarlas, que tomen conciencia que el ciberespacio (Internet) es maravilloso y así como podemos conectarnos para ver una película, si lo hacemos con una red Wifi compartida con el vecino, éste puede tratar de acceder a nuestros dispositivos y acceder a nuestros datos. Siempre comento en mis disertaciones que debemos analizar el riesgo al momento de hacer algo.

Toda nuestra vida lo venimos haciendo, por ejemplo, si vamos a cruzar la calle miramos el semáforo, así y todo verificamos que nadie lo pase en rojo y nos atropelle. Lo mismo debe hacer el usuario, ¿Por qué debe darle el usuario y password de acceso al banco?, ¿Por qué darle el SMS del PIN?, ¿Conozco bien mi vecino como para compartir el Wifi?, ¿Creo una cuenta para acceder a otra red o uso Facebook?, ¿Por qué debería dejar el celular sin bloquear? Preguntas que debemos hacernos al momento de analizar situaciones que pueden comprometer los datos del usuario. Cuidemos nuestros datos.

Entrevista



- ¿Existen estadísticas de ciberataques en la ciudad de Córdoba?

- Entendemos que al no existir regulaciones en la Argentina sobre denuncias de ciberataques como en otros países, uno se entera de los incidentes cuando requieren asesoramiento personal o un colega nos comenta. En Estados Unidos, por ejemplo, existe la Ley HIPAA que se aplica a planes de salud, oficinas de compensación para atención médica y algunos proveedores de atención médica que transmitan en forma electrónica información de salud. Cuando surgió el Ransomware Wannacry, por cumplimiento legal los hospitales se vieron obligados a reportar que por cuestiones de infección los pacientes no podrían llegar a ver sus historias clínicas (recordemos que las historias clínicas son del paciente no de la organización de salud). Por eso, en ese momento se obtuvieron estadísticas, hoy por razones de impacto y otras cuestiones no son públicas. Hace poco fue atacado Globant, se hizo público y sus acciones cayeron hasta 13% en Wall Street. Por eso muchas empresas no reportan y tratan de que esa información no sea pública. Víctimas en la ciudad de Córdoba, hay más de cientos que conocemos.

- Según su experiencia, ¿Qué importancia tiene la conformación de un hub de ciberseguridad?

La conformación del Cyber Security-Hub vino a sacar del estado de confort a todos: sector público, universidades, organizaciones públicas y privadas. Es una iniciativa de enorme valor que, de mantener los objetivos definidos, con un trabajo en equipo y comunidad interdisciplinario, podemos lograr que la sociedad y las organizaciones logren el nivel de madurez deseado.

Como todo, lleva tiempo y esfuerzo. Un niño no puede subirse a los cuatro años a una moto de alta cilindrada, debe primero usar andador, triciclo, bicicleta con rueditas, bicicleta más grande, moto baja cilindrada hasta llegar a la moto deseada. El Hub está en el “andador”, pero con grandes iniciativas del equipo que lo conforman y con ganas de hacer muchas cosas. Será responsabilidad del Hub mantener las mismas y con el esfuerzo de todos vamos a lograr excelentes objetivos. Hoy es

una necesidad muy fuerte de la sociedad (lo vemos a diario) y hay una necesidad de acompañar, con este espacio que debe ser cubierto por todos trabajando de manera comunitaria. Si logramos trabajar en comunidad, vamos hacer un excelente trabajo

Recomendaciones para prevenir el fraude, según Dutra

- **Desconfiar siempre**.
  "La mejor forma de prevenir estos ataques es ser totalmente desconfiado. Nunca ceder ningún dato personal a un tercero o desconocido y, si debemos hacerlo, validar que la persona quien nos solicita la información sea el que dice ser o de la organización a la que pertenece. Nunca ceder datos como usuarios, contraseñas o pins de validación. Si alguien debe hacernos una transferencia solo facilitar el alias o CBU, no deben acceder a las cuentas nuestras".

- **Nunca acceder a enlaces sospechosos.**
  "Si reciben un correo, por más que asuste el contenido al leerlo, no acceder a los links o sitios que suelen venir en el cuerpo. Si tienen dudas, por ejemplo un correo que les pide datos de la tarjeta por que se les está por bloquear la cuenta, entrar por el navegador o la aplicación como lo hacen habitualmente, pero no usando los links de los correos".

- **No dar datos por teléfono.**
  "Para aquellas llamadas que recibimos, no dar ningún tipo de dato, más bien, pedir y cortar la llamada. Tratar de denunciar los números de teléfono o Whastapp".

- **Cambiar regularmente las contraseñas.**
  "Como hay una importante cantidad de robo de cuentas de redes sociales, configurar bien las contraseñas. Es decir, cambiarlas regularmente y si desean pueden usar un esquema interesante para acordarse, el de la frase. Por ejemplo, si quiero poner una contraseña larga y no quiero olvidarla puedo crear la frase "Me gusta vivir en Córdoba en el 2022". Si tomamos las iniciales de cada palabra, tendremos la contraseña "MgveCee2022".

- **Doble factor de autenticación.**
  "Algo que refuerza de manera importante la seguridad de acceso es el proceso en el cual el usuario define su teléfono en la cuenta que usa, por ejemplo, Facebook. Esto permitirá definir lo que se denomina doble factor de autenticación. Es decir, una vez que ponemos en la aplicación el usuario y contraseña, recibiremos un código de acceso al celular que dura muy poco y debemos ingresarlo en el sitio a donde deseamos ingresar. Este código nunca debemos cederlo".

Algunas de las estafas virtuales más frecuentes

- **Alquileres fraudulentos:**
  Casas o departamentos que se publican en las redes sociales, piden una seña. Se sugiere validar telefónicamente y analizar si hace pocos días ha sido publicado, si no existe otra publicación similar o contactar directamente una inmobiliaria.

- **Bonos o subsidios del gobierno:**
  Usuarios reciben llamadas por personas que se hacen pasar por el ANSES u otro organismo, piden datos bancarios (datos de acceso a la cuenta) para depositar el dinero. Si alguien quiere transferir, sólo debemos pasar el alias o CBU de la cuenta.

- **Ventas:**
  Publican algo para vender y un supuesto comprador pide el CBU y dice que se equivocó y transfirió más plata de lo que debía. Pide los datos para acceder a la cuenta o llama otra persona haciéndose pasar por el Banco para resolver el problema. Verifiquen cuánto depositó y si el dinero ingresó realmente. Nunca den acceso a las cuentas del banco.

HackerSpace

“Es muy importante que exista en Córdoba un hub de ciberseguridad, nos da visibilidad en el resto de la Región”

Carlos Garay es uno de los fundadores de Hacker Space, el primer espacio nacido en la Ciudad que busca concientizar sobre la importancia de resguardar los datos y auditar los sistemas. Considera que es el momento de demostrar que Córdoba tiene un alto potencial tecnológico.

En 2019 surgió en la ciudad de Córdoba un nuevo espacio con el objetivo de concientizar a las empresas y al sector público sobre la importancia de resguardar sus datos y auditar los sistemas que tienen tanto su información como la de todas las personas. Con ese propósito nació Córdoba Hacker Space, “un lugar para aprender, para charlar, para debatir, para jugar, para investigar”, asegura Carlos Garay, uno de sus fundadores junto con Antonella de Caro, Joaquín Rodiguez Varela, Marcos Oviedo, Victor Stornatti, Daniel Daniele y Dan Borgono.

Creemos que un hackerspace es una fuente de educación y colaboración dentro de la seguridad informática, contribuyendo al desarrollo de esta área de conocimiento. Las actividades del hackerspace se realizan con un espíritu de compartir información y de diseminar el conocimiento. Esto permite que el campo de la seguridad informática crezca, se desarrolle y continúe su camino hacia la excelencia del conocimiento

-¿Cuál fue el disparador para la conformación del Córdoba Hacker Space?

En 2019 junto a Marcos Oviedo pudimos realizar en conjunto con la UTN, con mucho esfuerzo, “Bsides Argentina”, el capítulo argentino del framework de conferencias de USA “BSides”. Fue un éxito, llenamos el auditorio de la UTN y fue en ese momento que dijimos “acá hay mucho potencial, sólo falta reunirnos”. Entonces pensamos en una JAM, donde la idea principal era juntarse para hablar sobre Hacking. Luego fue tomando forma como Hacker Space y recibimos la ayuda de McAfee que en ese momento se encontraba con operaciones en Córdoba. Nos cedieron el espacio físico y empezamos a juntarnos a charlar, a jugar, a estudiar... En 2020, en pandemia, migramos a la modalidad virtual y todos los meses dábamos charlas sobre distintas temáticas.

- ¿Cómo viene creciendo este espacio y qué proyecciones tienen a mediano y largo plazo?

El 2020 fue muy productivo, tuvimos muchos eventos. Este año (2022) tenemos varios proyectos en mente, entre ellos la Municipalidad de Córdoba nos invitó a formar parte del Hub de Ciberseguridad y nos acompañará para conformarnos como ONG sin fines de lucro. Además, seguiremos realizando eventos on line y, a medida que se pueda, alguno presencial. Como es de público conocimiento McAfee ya se retiró de Córdoba por lo que estamos sin lugar físico para juntarnos, pero ya encontraremos nuestro lugar para poder seguir dándole a la comunidad hacker un espacio donde pueda ir.

- Según la experiencia en el ámbito de la ciberseguridad, ¿Cuáles son los ataques más frecuentes y cuáles son las mejores formas de prevenirlos?

Sin duda en el ámbito corporativo está de moda el "Ransomware", un ataque dirigido hacia empresas que descuidan alguna puerta de acceso a su infraestructura, donde los cibercriminales encriptan información de la empresa y piden rescate en criptomonedas y es prácticamente imposible de rastrear. No se recomienda el pago por la información; se recomienda que la mejor forma de prevenir es realizando auditorias de seguridad, buscan-

do el punto débil que deberían cubrir, capacitación y concientización a los colaboradores.

- ¿Cómo es la situación actual en el sector público con los ciberdelitos?

El sector público en todos los niveles, en mi opinión, es un sector muy sensible. Los organismos públicos no toman las medidas necesarias para evitar estos ataques, claro ejemplo fue el ataque a RENAPER y al Senado de la Nación.

- Desde la pandemia, ¿han crecido las estafas virtuales?

Si, por supuesto... Los cibercriminales están a la vanguardia del día a día, en esta pandemia nos tuvimos que quedar en casa y adoptar nuevas metodologías de compras on line, comprar desde el supermercado o algún insumo que nos haga falta. La única modalidad de pago eran las tarjetas de crédito. Los cibercriminales generan algún pretexto para "engancharte", lo que se llama un phishing.

- ¿Cómo ves el desarrollo en Córdoba de profesionales en materia de ciberseguridad?

¡Lo veo muy bien! Desde que hicimos el evento BSides en 2019 descubrimos que había potencial, muchos chicos y chicas interesados en InfoSec (seguridad de la información); muchas empresas del rubro se fueron radicando en la ciudad dándole oportunidades. Ahora, con la propuesta de la Municipalidad de Córdoba de conformar un Hub Regional, la idea es que se potencie la actividad en la región, formar nuevos talentos, fomentar la seguridad de nuestros ciudadanos para que estén atentos a presuntas estafas.

- ¿Qué impacto tendrá, según tu criterio, la conformación de un Hub de Ciberseguridad?

Es muy importante que exista un espacio como el hub de ciberseguridad; nos da visibilidad en el resto de la Región y el mundo, nuevos negocios, nuevos talentos, nuevas oportunidades para demostrar que Córdoba es potencial en tecnología. Tenemos Smart Cities y mientras estemos implementando tecnología que utilizan nuestros vecinos, tenemos que tener el resguardo y que sus datos estarán seguros, tenemos que saber que estamos expuestos al mundo y los cibercriminales pueden sacar provecho de eso.

- ¿Cuáles son los principales desafíos de ciberseguridad por estos días?

Mantener a los cibercriminales fuera de los intereses de nuestros ciudadanos, que ellos se encuentren seguros, que se sientan acompañados en caso que sufran un fraude.

Más información sobre
Córdoba Hacker Space:
https://www.cordobahackerspace.org/

Proofpoint Argentina

"Córdoba tiene un potencial altísimo para convertirse en generador de talentos en el área de ciberseguridad"

Guillermo Colsani, especialista en Ciberseguridad y director de Proofpoint Argentina, asegura que sigue en crecimiento la afluencia de estudiantes de sistemas y que los roles de ciberseguridad son muy demandados. Asegura que la conformación de un Hub de Ciberseguridad es "clave" para consolidar este sector.

Proofpoint es una empresa de ciberseguridad que tiene oficina central en Sunnyvale, California (Estados Unidos). Actualmente cuenta con cerca de 4000 empleados en todo el mundo y hace un año que decidió desembarcar en la ciudad de Córdoba y se convirtió en la primera oficina orgánica que abrió Proofpoint fuera de su país. ¿Por qué eligió esta ciudad para crecer? "Córdoba es una ciudad que genera talento año tras año, y donde la industria de tecnología es un fuerte motor de la economía", cuenta Guillermo Colsani, director de la firma en Argentina.

Para el especialista, Córdoba tiene un potencial altísimo para convertirse en generador de talentos en el área de ciberseguridad. "Por un lado, la afluencia de estudiantes de sistemas sigue creciendo; pero, además, la ciberseguridad también puede nutrirse de otros perfiles que les interesa ampliar sus áreas de conocimiento como quienes estudian lenguas, administración de empresas, educación, psicología, abogacía, entre otros", destaca Colsani y agrega que, actualmente, los roles de ciberseguridad tienen un alto impacto en el mercado, por lo tanto es un perfil que tiene una posibilidad de ingresos muy alta.

> **Un hub de ciberseguridad es un espacio clave para generar interés en la comunidad estudiantil y en las empresas y, de esta forma, posicionar a la ciberseguridad como una opción más cotidiana en las vidas de las personas.**
>
> **Guillermo Colsani**

"El Hub también va a elevar el nivel de exposición de los participantes, aumentando la inteligencia colectiva para la defensa; creando así un círculo virtuoso autosustentable y con perspectivas de negocio muy prometedoras", completó Colsani.

Según tu experiencia en el sector, ¿Cuáles son los principales desafíos de ciberseguridad?

La industria de ciberseguridad tiene el gran desafío de aumentar la cantidad de talento para gestionar la ciberdefensa; se estima que se necesitan entre 2 y 3 millones de personas más en roles de ciberseguridad a nivel mundial.

¿Cuáles son los ataques más frecuentes en el ámbito corporativo?

Los ataques más frecuentes están centrados en las personas, principalmente ataques o engaños que llegan a través de email, conocidos como Scam, Spam o Phishing; y también los ataques producidos por empleados que, sin advertirlo o intencionalmente, filtran información crítica para la empresa. Las líneas de productos desarrollados por Proofpoint son la mejor manera de prevenir estos ataques, y requieren de una atención permanente por parte de los equipos de seguridad como también de todos los empleados.

¿Cómo han crecido las estafas virtuales desde la pandemia?

La ciberseguridad ha cobrado una relevancia mucho mayor luego de la pandemia, hoy es un tema que preocupa a nivel C-level (jefes de área) de las empresas ya que el potencial impacto es altísimo, desde una pérdida por pedido de recompensa (el afamado ransomware) por parte de los atacantes, como también la inutilización de las operaciones son ejemplos muy cotidianos y que afectan directamente a la rentabilidad y reputación de las empresas.
En este contexto, Proofpoint desarrolló un esquema de clasificación de Phishing, solamente para poder darle nombre a la variedad de ataques; y ese esquema de clasificación muestra cómo los atacantes han aprovechado la pandemia para enmascarar engaños. También están apareciendo engaños relacionados con el reciente conflicto entre Ucrania y Rusia, lo que muestra que los atacantes están constantemente en la búsqueda de la actividad social para poder enmascarar sus ataques.

Proofpoint en Córdoba: "Tenemos muchas oportunidades para sumarse y crecer en la carrera profesional"

El equipo de Proofpoint de Córdoba está compuesto por dos organizaciones: Customer Success y el equipo de Ingeniería de producto.

La empresa desarrolla productos de ciberseguridad para el segmento corporativo, es decir que los clientes son empresas de todo el mundo que utilizan sus productos para defender los activos de la empresa y a sus empleados. El eje es que "La protección empieza por las personas". Los productos más importantes se agrupan en los siguientes pilares: Protección en email y en ataques avanzados; protección de la información y de aplicaciones corporativas en la nube; entrenamientos y ejercicios de seguridad para los empleados; aseguramiento de regulaciones de utilización de información digital.

"En Proofpoint tenemos muchas oportunidades para sumarse y crecer en la carrera profesional, invito a quienes estén interesados a que exploren los puestos requeridos en este enlace https://proofpoint.wd5.myworkdayjobs.com/ si la ciberseguridad les interesa y quisieran ver cómo empezar", puntualiza Colsani y agrega: "Nuestro equipo tiene el foco puesto en construir una cultura de trabajo que sea inclusiva, diversa y que potencie el crecimiento en un ambiente de bienestar personal".

Opinión

Concientizar sobre ciberseguridad: La mejor defensa contra los ciberdelincuentes

Por Esp. Ing. Fabian A. Gibellini (*)

Quién no ha recibido mensajes, correos o llamados en donde ganamos fortunas, dólares, premios, viajes, etc..., que alegría genera, una adrenalina por ser ganadores de algo, pero;¿así de fácil?, ¿sin hacer nada?, o sólo haciendo un clic o contestando un mail, o bajando un archivo adjunto, es una emoción inconmensurable. Sin embargo, cuando vemos la realidad de lo que hay detrás de esta acción que ejecutamos, nos encontramos con un verdadero monstruo de la virtualidad que sólo consigue que nos frustremos, que tengamos miedo, impotencia y una pérdida de confianza en los medios utilizados.

Tener que hablar del secuestro de los archivos, perdiendo todo tipo de acceso a nuestra información y dependiendo de un ciberdelincuente que quiere cobrar por regresarnos lo que es nuestro, es decepcionante y parece de película.

Estamos hablando de los "ransomwares"(código malicioso que secuestra datos), uno de los ataques cibernéticos más frecuentes que hoy podemos encontrar y que en muchos casos se podría evitar con solo informar que no se haga clic en enlaces que sean sospechosos o descargar archivos adjuntos de correos que no conocemos o que no esperábamos.

Pero, ¿cómo es posible esto en la actualidad? Hemos tenido avances tecnológicos increíbles que nos llevan a contar el día de hoy con herramientas eficientes, muy sofisticadas y consideradas seguras, tales como cortafuegos (firewalls), sistemas de detección de intrusos, reconocimiento de la identidad por huella o faciales, sistemas de protección digitales y muchos otros sistemas de protección. ¿Cómo puede un usuario residencial o empleado sufrir algún inconveniente de ciberseguridad si cuenta con todas estas herramientas?

Por supuesto que estas herramientas son necesarias y debemos contar con ellas en los dispositivos que usamos diariamente ya que disminuyen de manera considerable los riesgos, brindando protección a la información abundante que generamos en nuestra rutina personal, laboral y social. Sin embargo,la implementación excesiva también puede generar malestar, debido a que muchas de estas herramientas tienen opciones muy prohibitivas, o que al monitorear las acciones o eventos que llevan a cabo en los dispositivos, su productividad se ve disminuida y sus actividades se ven afectadas considerablemente por la necesidad de incurrir en más tiempo para desarrollarlas.

Teniendo en cuenta que es el usuario el que tiene en sus manos la gestión de la información, puede llevar a cabo acciones que represente un riesgo por desconocimiento, por no estar correctamente informado o por no cumplimentar con las políticas de seguridad orientadas a proteger la información.

Pero, ¿cómo se informa el usuario? Hoy en día con las redes sociales, internet y todos los medios de comunicación debería ser un experto en el tema, claro está que el mar de información nos lleva a la desinformación y a la posibilidad de que estemos leyendo datos falsos.

Así como la tecnología de protección de los datos avanzó, también aumentó la sensibilidad de los datos que las personas almacenan digitalmente: billeteras virtuales, datos de salud, datos personales, datos de geolocalización, documentos de trabajo y de identificación personal, entre otros.
Esto generó que los ciberdelincuentes preparen y diseñen engaños cada vez más sofisticados como el phishing, extorsiones virtuales, malwares, ataques de ransomware, etc.

Aquí entran en juego todos los ámbitos: el educativo (escuelas y universidades), las pymes (sensibilizando a sus empleados), el gobierno en todas sus jurisdicciones, y los especialistas en la temática.

La conformación de un Hub de Ciberseguridad en la ciudad de Córdoba, integrando todos los ámbitos nombrados anteriormente, puede ser la clave para lograr objetivos claros de concientización de los usuarios. Este conglomerado de universidades, empresas, organizaciones sin fines de lucros y gobierno pueden brindar la mejor herramienta para defenderse de los ciberdelincuentes: "La concientización en materia de ciberseguridad".

Concientizando en el uso de las herramientas digitales, es el mismo usuario el que tiene la posibilidad de disminuir los riesgos potenciales aplicando acciones básicas de seguridad, tales como no ingresar claves en sitios no oficiales, no acceder en equipos desconocidos, no descargar y ejecutar archivos de fuentes desconocidas y realizando copias de seguridad de sus datos.

(*) Responsable Laboratorio de Ing. En Sistemas de Información UTNFRC
Coordinar Equipo de Seguridad del CIDS (Centro de Investigación, Transferencia y Desarrollo de Sistemas de Información)

La importancia de los datos en la era de la ciberseguridad

Por Luciano Monchiero (*)

Cuando hablamos de datos, hablamos que los encontramos en todos los lugares, ya sea con simples usuarios a través de sus teléfonos inteligentes, profesionales, industrias y todo tipo de organización.
En consecuencia, pensar en el gran volumen de datos que día a día se genera en diferentes ámbitos es algo inimaginable. Ahora pensemos qué sucede desde el enfoque de la ciberseguridad.

Cuando hablamos de datos, hablamos que los encontramos en todos los lugares, ya sea con simples usuarios a través de sus teléfonos inteligentes, profesionales, industrias y todo tipo de organización. En consecuencia, pensar en el gran volumen de datos que día a día se genera en diferentes ámbitos es algo inimaginable. Ahora pensemos qué sucede desde el enfoque de la ciberseguridad.

Para ello, tengamos presente algunos números que nos pueden hacer comprender un poco mejor sobre este fenómeno. En efecto, para el año 2025 se espera más de 200 zettabytes (es decir 1 zettabyte equivale a 20 billones del papel de árboles) almacenados en la nube en todo el mundo, eso ya nos sumerge en la realidad que nos encontramos. Por lo tanto, cada vez más esos datos se convierten en un incremento de valor sobre todo para las empresas y organizaciones. Y esto lo decimos, ya que, en el proceso diario de estas organizaciones y sus actividades, lleva a considerarse si la misma se encuentra en dirección a los objetivos planteados, o tener en cuenta cuáles áreas son las que mejor están generando valor o en su defecto implementar mejoras para que aquellas que requieren lograr ese objetivo buscado. Esto claramente le da un poder de ayuda a cada departamento dentro de cada organización para lograr mejorar sus procesos, sobre todo usar esos datos para generar un beneficio para sus clientes, consumidores, empleados y en especial a su propio negocio.

Ahora bien, como se observa, son innumerables los casos en que esos datos nos aportan beneficios. El punto clave en este contexto se encuentra en que, a mayor rendimiento, mayor son las necesidades de contar con infraestructuras de seguridad sobre esos datos. En efecto nos lleva aquí a adentrarnos en un terreno que poco a poco comienza a tomar partido sobre la importancia de la ciberseguridad en empresas y organizaciones.

Pensemos por un momento si en cada industria, cada empleado sabe desde el primer día cómo mantener seguros el volumen de datos que maneja, es decir la cantidad de correos que recibe, los archivos adjuntos, la cartera de clientes, las imágenes que le llegan de correos externos, los usuarios y contraseñas a diferentes sistemas, las planillas excel con un sin número de información importante para esa firma y que no puede ser revelada a terceros. Es ahí donde tenemos que dar una respuesta desde el enfoque de la Ciberseguridad y si tomamos a referentes de organizaciones internacionales como el NIST, ISACA, INCIBE, entre otros, **todos coinciden en que el activo más importante de toda organización es el dato y que el principal foco está en reducir el riesgo en todo negocio, sobre todo si sabemos que el usuario -empleado- es el eslabón más débil de la cadena.** En consecuencia, hablamos de que, si bien es importante contar con una ley que nos obligue a implementar medidas técnicas de ciberseguridad y organizativas a fin de reducir los riesgos, también es importante que un ente autárquico e independiente ejerza los mecanismos de control para que la cadena de seguridad y de valor continúe intacta hacia todas las partes de este proceso.

Ahora nos detengamos a pensar por un momento cuántas veces compartimos información de la empresa por medios de mensajería como Whatsapp, la pregunta es si ese medio es adecuado y si esa organización cuenta con una política de seguridad, entre otros puntos claves en esa cadena.

Sin lugar a dudas que nos encontramos en una era donde los bits y bytes seguirán ocupando gran parte de nuestros negocios y de nuestras vidas, el punto será tomar conciencia del trabajo que debe ocupar cada organización para proteger los intereses no sólo propios sino de sus clientes ya que si consideramos que un ataque de ransomware hoy a una empresa le cuesta 116 mil dólares en promedio a nivel mundial, entre identificación del problema, horas de técnicos trabajando en el problema, tema de reputación con clientes que se van porque no creen ya en la seguridad de su empresa, las demandas que eso acarrea y otras consideraciones, el dolor de cabeza termina siendo mucho mayor.

En este último ejemplo, lo importante a resaltar es la toma de conciencia de si esos empleados se encontraban capacitados para comprender sobre este nuevo fenómeno que ataca al activo más importante de la organización -los datos-, si cuenta con medidas organizativas y técnicas.
En conclusión, es un cambio de paradigma que hoy en día no podemos dejar de lado ya que lo tenemos encima de nuestros propios intereses.

(*) Director de la especialización en Cibercrimen de la Universidad Empresarial Siglo 21.

No tengo nada que esconder, ¡Pero quiero mi privacidad de vuelta!

Por Javier Jorge y Miguel Solinas (*)

En esta era de hiperconectividad y de explotación de datos personales, la privacidad es un factor muy relevante. La tecnología interviene en todos los aspectos de nuestras vidas y se acentúa cada día más. Los registros que se generan de cada uno de nuestros movimientos significan que nuestra privacidad está cada vez más amenazada. Significa que cada vez tienen más datos de nosotros como individuos, como grupos y como sociedad.

Todo parece sacado de una película de ficción. Las formas en que podemos ser rastreados e identificados se han disparado, junto con los tipos y la escala de información disponible sobre nosotros.

¿Qué es la privacidad? Según la RAE es "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión." Ahora bien, por analogía, la privacidad en el ciberespacio debe ser también un ámbito de nuestra vida privada que **tenemos derecho a proteger** de cualquier intromisión. Quizás nos deberíamos preguntar ¿Por qué las empresas que nos brindan servicios en el ciberespacio les interesa avanzar sobre nuestros datos ? Sabemos que es por una cuestión absolutamente comercial. Mientras más datos tengan de nosotros, mejor nos conocerán, podrán hacer una mejor calificación como individuos, grupos y sociedades y los algoritmos que utilizarán para orientar nuestras decisiones serán más efectivos. Obviamente eso los beneficiará económicamente como en algún momento ocurrió con el conocimiento de las rutas marítimas para recorrer el mundo minimizando riesgos. Mientras tanto, nosotros como individuos, grupos y sociedades veremos que esos beneficios no impactan de modo significativo sobre nuestras vidas. La relación es asimétrica.

La privacidad es un derecho que como tal también nos permite disfrutar de otros derechos, **y la interferencia con nuestra privacidad a menudo proporciona la puerta de entrada a la violación del resto de nuestros derechos.** No las violaciones a este derecho derivan en casos escandalosos como el de Cambridge Analítica y sus efectos en el mundo y en Argentina[1].

Una forma simple de empezar a fortalecer nuestra privacidad es eligiendo una mejor plataforma de mensajería instantánea e invitar a nuestros contactos a usarla. Las plataformas de mensajería más populares no siempre son las que más respetan la privacidad de las personas.

¿Cómo elegir la mejor plataforma?
A continuación mencionamos algunos puntos.

1. ¿Es de código abierto?
Las aplicaciones de código abierto se pueden auditar y es posible saber exactamente qué es lo que hacen con nuestros datos.

2. ¿Soporta encriptación de extremo a extremo?
Esto significa que solo el emisor y receptor del mensaje pueden verlo, algo obvio pero que no se cumple en todas las plataformas, algunas dicen cumplirlo pero es imposible verificarlo.

3. ¿Cómo se sostiene económicamente el proyecto?¿Existe alguna corporación que me lo "regala"? ¿Debo pagar por el servicio?
Existen proyectos que se sustentan mediante donaciones o aportes de sus usuarios, por lo que no necesitan vender información para sustentarse.

4. ¿La plataforma estuvo implicada en alguna fuga de datos, ya sea intencional con la justicia/agencias de inteligencia o "accidental" por algún "error"?
Algunas plataformas dicen que ofrecen encriptación de extremo a extremo, sin embargo muchas veces se encuentran noticias de empresas que abren información de sus usuarios a terceros.

5. ¿Es necesaria la presencia de un servidor para poder comunicarme ? ¿Qué pasa si la empresa desaparece o decide dejar de prestar servicios o empezar a cobrar por ellos?
Existen aplicaciones capaces de funcionar sin un servidor de un tercero para comunicarse.

Factores/ Aplicaciones	Whatsapp	Signal	Jami	Telegram	Tox
Código abierto	No	Si	Si	Solo el cliente	Si
Encriptación de extremo a extremo	Declara que si, pero no se puede verificar	Si	Si	Si, pero no por defecto	Si
Financiamiento	No	Donaciones	Fundación GNU	No por el momento[2]	Donaciones
Fugas de datos	Si[3]	No	No	No	No
Centralizado en un servidor	Si	Si	No	Si	No
Cantidad de datos personales asociados a tu cuenta	15[4]	1	0	3	0

Uno de los temas que falta mencionar es la cantidad de personas que usan cada plataforma. En ese sentido las plataformas que son menos usadas son Jami y Tox. La decisión de la plataforma a elegir queda a criterio del lector. De la lista mencionada anteriormente puede observarse que Signal es una alternativa que va ganando cada vez más usuarios y que realiza un tratamiento respetuoso de nuestros datos.

Este artículo es el primero de una serie de acciones tendientes a mejorar nuestra privacidad

(*)
Javier Jorge, Ingeniero en Computación en Instituto Nacional de Tecnología Industrial (INTI)
Miguel Solinas, Sub Director Departamento de Computación FCEFyN - UNC

[1] *https://noticias.perfil.com/noticias/general/2019-09-06-el-pro-y-el-caso-cambridge-analytica.phtml*
[2] *https://t.me/durov/142*
[3] *https://www.business-standard.com/article/technology/whatsapp-doesn-t-break-end-to-end-encryption-to-review-messages-propublica-121090901162_1.html*
[4] *https://www.xataka.com/basics/signal-vs-telegram-vs-whatsapp-cuales-diferencias-cual-cuida-tu-privacidad*

Córdoba Cyber-Security Hub

accefy · ACsoft · @diar · apex · Arcor

arts·sec · capazeta · CAYLENT · CEDI TECHCONSULTING

CIECCA · Colegio de Abogados Córdoba · Córdoba Technology Cluster 20 años · Cloudshine · daitek

DANKA · eclypsium · ECOGAS · FORTINET · Gates CONSULTING · HACKERSPACE

JemerSoft Tech Solutions · Konecta · mobbex · mundosE

Pabex Desarrollo de software · PAGOS360 · PATAGONIA SECURITY · proofpoint.

puntonet soluciones · RAM .IT Soluciones Informáticas · SMARTFENSE

vectus · Vicino SOFTWARE FACTORY · VU · XECUR.IT IT Solutions for Organizations

SIGLO 21 · UBP · UNC · UTN · Argentina Presidencia · CÓRDOBA entre todos

CorLab · Secretaría de Planeamiento, Modernización y RRII · Secretaría de Economía y Finanzas · Municipalidad de Córdoba