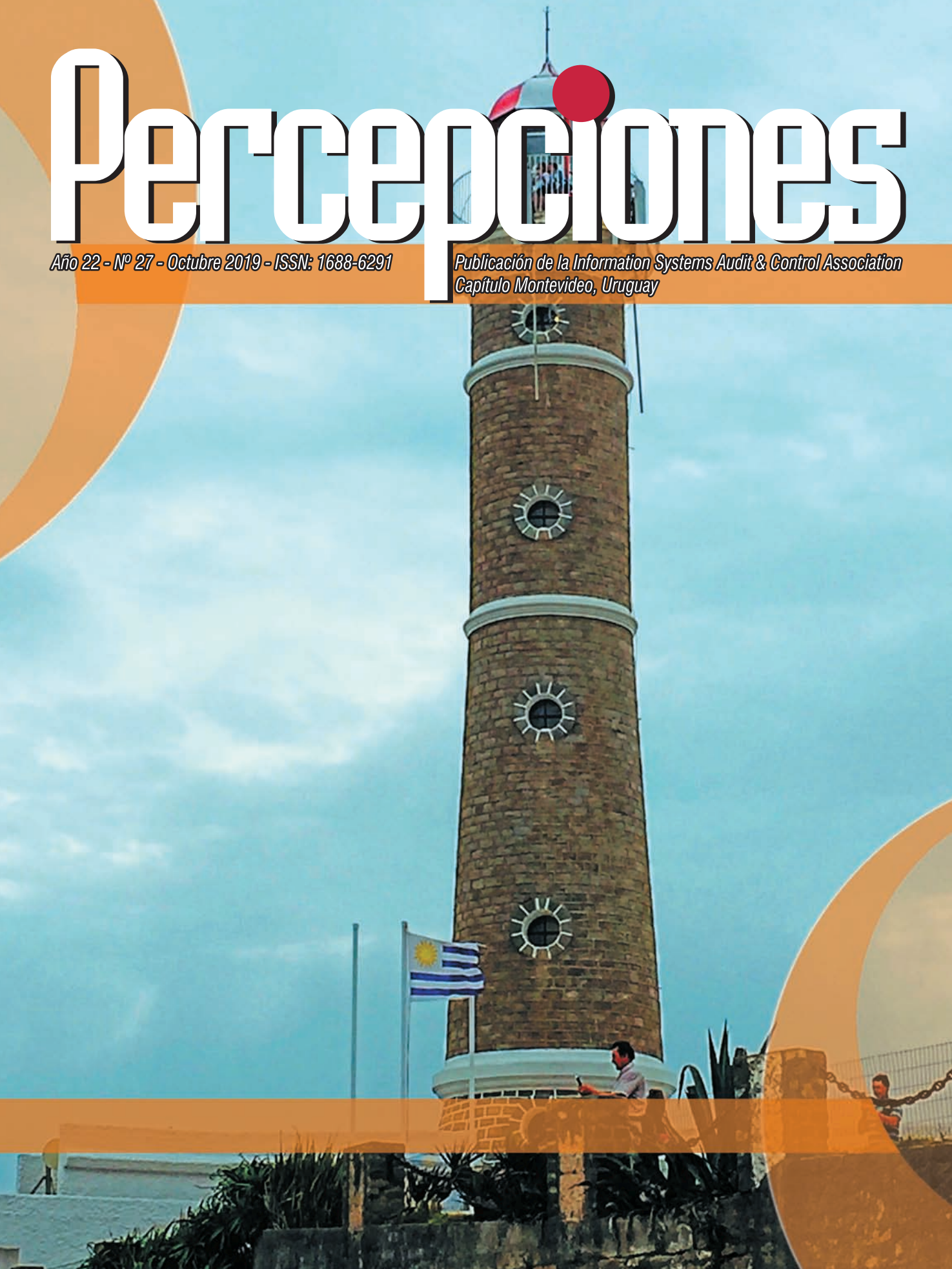
Percepciones

Año 22 - Nº 27 - Octubre 2019 - ISSN: 1688-6291

Publicación de la Information Systems Audit & Control Association
Capítulo Montevideo, Uruguay



GlobalSUITE

OPTIMICE SU EMPRESA CON UN **SOFTWARE INTEGRAL DE SISTEMAS DE GESTIÓN**

Obtenga un **40% de ahorro de costes** en la implantación de diferentes **sistemas y normas de forma integrada**

RISK | SECURITY | CONTINUITY | COMPLIANCE

Solicite más información en: www.globalsuitesolutions.com

Percepciones
Publicación de la Information Systems Audit & Control Association
Capítulo Montevideo, Uruguay

Año 22 Nº 27 - Octubre 2019
ISSN: 1688-6291

Percepciones es una publicación de

ISACA®
Confianza en, y valor de los sistemas de información
Montevideo Chapter
200 CHAPTERS STRONG

ISACA - Capítulo Montevideo, Uruguay
Cerrito 420 of. 505
Telefax: 29150319
CP 11000 - Montevideo, Uruguay
E-mail: info@isaca.org.uy
Internet: www.isaca.org.uy
www.facebook.com/isacamontevideo

Registro en el Ministerio de Educación y Cultura según Art. 4º, Ley 16.099, Tomo XI, Fojas 243

Sumario

"ISACA - Capítulo Montevideo, Uruguay es una Asociación sin fines de lucro de miembros profesionales dedicados a la práctica de la Auditoría, Control y Seguridad de Sistemas de Información, y comprometidos con la Educación, la Certificación y los Estándares"
"Nuestra visión es ser el líder global reconocido en Gobernabilidad, Control y Aseguramiento de la Tecnología de la Información."

Editorial

Estimados lectores,

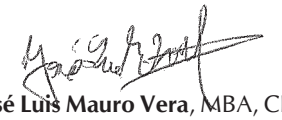
Desde nuestra Comisión Directiva del Capítulo Montevideo de ISACA, es un honor acercarles esta XXVII edición de la revista Percepciones. Bajo la consigna "Honorando nuestro pasado, innovando nuestro futuro", ISACA celebra sus 50 años, desde su fundación en Los Ángeles, California bajo la denominación EDPAA (Electronic Data Processing Auditors Association), que a partir de 1994 fue modificada a la actual denominación. Por ese entonces también se creaba nuestro Capítulo, que desde hace más de 25 años viene fomentando, aportando y facilitando conocimientos y metodologías para los profesionales vinculados con el Gobierno Corporativo, Auditoría, Riesgo Tecnológico y Seguridad de la información.

En esa línea, les acercamos en esta revista técnica, artículos que fueron seleccionados a través de un llamado que oportunamente realizamos para la presentación de artículos, y a partir del valiosísimo aporte de profesionales de Uruguay y de la región. Aprovechamos la oportunidad para agradecerles la gentileza de participar de nuestra revista y de compartir sus Percepciones con nuestra comunidad.

Desde hace ya 10 años, este año los invitamos a participar de la décima edición del congreso CIGRAS, que denominamos para la ocasión como "CIGRAS X". Contaremos con ponencias de expositores provenientes de distintas latitudes, procurando actualizarnos con las nuevas tendencias en los temas centrales para nuestra Asociación. En este sentido, continuando con nuestro interés de sumarnos al programa SheLeads Tech de ISACA, proponemos paneles y conferencias que abordarán la temática de la diversidad e inclusión de la mujer en las actividades de liderazgo en tecnologías de la información y ciber seguridad. También proponemos aportar nuevas perspectivas desde el punto de vista de ciber seguridad, a través del panel sobre cómo los hackers uruguayos logran aprovechar los programas de Bug Bounty ofrecido por distintas empresas. Esta edición será una excelente oportunidad para reencontrarnos, actualizarnos y hacer networking con profesionales y líderes en las áreas de conocimiento de nuestra Asociación.

Este año 2019 nos encuentra acercándonos al final de la segunda década de este siglo, en períodos electorales en la región, y nos encuentra enmarcados con distintos desafíos y oportunidades en un mundo volátil, incierto, complejo y ambiguo. La transformación digital se presenta como una oportunidad para lanzarnos definitivamente en los nuevos paradigmas que definirán la educación, la economía, los modelos de negocio y el estilo de vida de las personas para la próxima década que se viene. Según el Barómetro de Transformación Digital de ISACA de 2018, 9 de cada 10 organizaciones tienen planes para avanzar en las iniciativas que conforman la transformación digital. Sin embargo, el 60% de las organizaciones no confía en que puedan valorar adecuadamente los niveles de seguridad de sistemas basados en inteligencia artificial o Machine Learning. En los tiempos que vivimos y en los que se vienen, es imposible dejar de lado los riesgos (positivos y negativos) que nos trae esta transformación, y la necesidad de gestionarlos y gobernarlos. En ese camino, desde nuestro Capítulo y desde ISACA, pretendemos facilitarles a través de publicaciones como Percepciones, eventos, cursos y conferencias como el CIGRAS, darles la oportunidad de mirar hacia adelante, ayudarlos y ayudarnos a sacar el mayor valor posible de las tecnologías y de la información,

Los saluda Atte.



Ing. **José Luis Mauro Vera**, MBA, CISA
Presidente, ISACA – Montevideo Chapter.

ISACA - Capítulo Montevideo, Uruguay || Comisión Directiva 2019

Presidente
Ing. Jose Luis MauroVera, MBA, CISA

Vice- Presidente
Sr. Maximiliano Daniel Alonzo, CISM

Secretario
A/P Ethel Kornecki, CISA, CISM

Tesorero
Cra. Alexandra Moyal, CISA, CRISC

Vocal
Lic. César Ganduglia

Comité de Membresía
A/P Fernando Yurisich, CISA, CIA, CRMA

Comité de Programación
Ing. Cristina Ledesma, CISA, CISM, CRISC

Comité de Publicaciones y Publicidad
A/S Miguel Galán, CISA, CRISC

Comité de Nominaciones
Ing. Felipe Sotuyo, CISA, CISM, CRISC, PMP

Comité de Educación
Ing. Evelyn Antón, CISA, CISM, CGEIT, CRISC

Comité de Auditoria
Ing. Susana González, CISA, PMP

Comisión Fiscal
A/P Cristina Borrazas, CISA, CRISC, PMP
Ing. Fernanda Molina, MBA, CISA, PMP
Ing. Reynaldo de la Fuente, CISA, CISSP, CRISC, MBA

Los desafíos éticos del manejo de datos

Carlos Petrella

Somos una sociedad tecnológica globalizada, que está replanteando drásticamente las reglas de juego de su comportamiento político, económico y social de manera vertiginosa, como consecuencia directa de la introducción ciertas máquinas que potencian lo que podemos pensar y lo que podemos hacer.

"Durante los últimos treinta años, el estado evolutivo y la trayectoria de la especie humana han sido cuestionados por los rápidos avances conseguidos en el campo de la nanotecnología, la biotecnología, las tecnologías de la información y la ciencia cognitiva." (Miah, 2012: 1),

Como muy bien anticipara en su momento Luis Joyanes: "La tecnología es un factor de cambio, que se manifiesta en el cambio tecnológico. El cambio tecnológico suele decirse que es, a la vez, cambio social y se puede ya decir que la tecnología encarna a los valores dominantes de la cultura industrial." (Joyanes, 1997: 1)

Entonces hablar de tecnología no es sólo hablar de artefactos tecnológicos, cualesquiera estos sean. Estos cambios tecnológicos generan además cambios políticos y sociales, que usualmente reflejan los valores dominantes de la cultura y por lo tanto, no son lo que se pueda decir neutros.

Debemos prepararnos para enfrentar ciertos desafíos éticos, que hasta hace muy poco no estaban en la agenda de los políticos, los empresarios y los trabajadores. Esos procesos están poniendo en duda los paradigmas legados, a un rimo que dificulta las adaptaciones.

En un mundo globalizado que opera sobre bases capitalistas, los procesos de "destrucción creativa" tienen efectos imponentes. Gran parte de las tecnologías emergentes son fuente de oportunidades para aquellos que planean entrar al mercado sin condicionamientos y también de amenazas, para aquellos ya consolidados.

Las teorías de Schumpeter (1997) reafirman ciertas formas del desarrollo de los ciclos económicos, que están revalorizando la importancia de la capacidad de renovación constante tan propia del modelo de referencia, lo que ha interpelado no sólo los sistemas productivos y comerciales, sino los sistemas políticos y sociales legados.

Los cambios tecnológicos tienen que ver con las reglas de juego con las que los seres humanos se desarrollan en la sociedad. Lo que aprendemos y lo que decidimos está muy influenciado por determinadas fuentes de información y conocimiento, a las que circunstancialmente los ciudadanos tenemos acceso.

A su vez esas fuentes de información y conocimientos, están cambiando aceleradamente sus formas de soporte, dando lugar a nuevas formas de registrar, organizar y presentar determinados contenidos, haciéndose cada vez más presentes en la vida diaria de las personas.

Mirando en el contexto mundial, se aprecia que la tecnología (en sus tres dimensiones instrumentos, recursos técnicos y procedimientos aplicados) ha profundizado su penetración en el entramado político, económico y social en todo el planeta de la mano de un impulso globalizador muy fuerte del uso de la Internet.

Actualmente un conjunto de tecnologías emergentes están operando como factor de cambio de las formas de informarse, fundamentalmente a partir de la disponibilidad de enormes cantidades de datos y de ciertas plataformas que potencian opciones de intercambios a gran escala, atravesando las fronteras de los Estados.

Por otra parte, la "tercera ola" potencia la trilogía: personas, procesos y contenidos, con la tecnología de la información y las comunicaciones como un sustento clave de las transformaciones. (Esains, 2011: 2) Se trata de un proceso drástico de replanteo de las formas de informarse y relacionarse, de una enorme envergadura e impacto.

Se ha producido una combinación explosiva de inventos e innovaciones que han cambiado la forma en que trabajamos, estudiamos y nos entretenemos. La creación de loa computación personal, la telefonía móvil, los motores de búsqueda, las aplicaciones móviles y el manejo de "big data" entre otros. (Friedman, 2018)

A partir de la disponibilidad de Internet y la World Wide Web y de la evolución de plataformas Web cada vez más interactivas, la humanidad dio un paso enorme para integrar redes de personas con intereses comunes, sin las limitaciones físicas que imponían referencias a un tiempo y a un lugar, para cada uno de los agentes.

No cabe duda de que el desarrollo de nuevas modalidades de intercambio sobre todo derivadas del uso de redes sociales globales, han ampliado las opciones de manejo de una enorme cantidad de datos que actualmente están siendo manejados por los administradores de plataformas tecnológicas.

No sólo cambian los agentes y la forma de relacionarse. Las propias formas de producir el conocimiento están cambiando. Michael Gibbons entre otros sostienen que una nueva forma de producción de conocimiento está emergiendo paralelamente al modelo tradicional organizado por especialidades.

Como en todo conjunto de tecnologías durante su aparición, han surgido confusiones en cuanto a los nuevos conceptos manejados y sobre todo, en lo referido al alcance de su aplicación en términos de las capacidades que deben tener los agentes para poder capitalizarlas.

Han surgido gran cantidad de portales webs de la mano de los beneficios de desarrollar una economía colaborativa portátil y ubicua que fomenta la participación económica y social de muchos agentes, para construir formas de producir y comercializar bienes o servicios a escala global de manera muy flexible.

Se están afirmando un conjunto de servicios creando un sistema que facilita la posibilidad de intercambiar y compartir bienes o servicios a través de plataformas electrónicas generando nuevas opciones para el desarrollo de modelos de economía colaborativa que plantea nuevos procesos de intermediación disruptivos.

Los ejemplos ya presentes muestran que han cambiado las reglas de juego en negocios claves como el transporte de pasajeros o el alquiler de viviendas, por retomar ejemplos totalmente consolidados como UBER y Airbnb donde algunos agentes se están adueñando de las reglas de juego de esos negocios.

Estas plataformas se han convertido en fuentes de creación de grandes beneficios y perjuicios para muchos agentes que han visto comprometerse sus modelos de negocio o sus fuentes de trabajo. Entre los ganadores están los emergentes poderes administradores de esas grandes plataformas.

Todos estos cambios en los intercambios entre grades grupos de interés plantean desafíos políticos y organizativos impensados hasta hace unos pocos años. (Winner, 2008) No cabe duda de que el agente que maneje la información que se comparte y la forma de compartirla tendrá una posición dominante cuasi monopólica.

Hoy ya se han afirmado un conjunto de servicios creando un sistema que facilita la posibilidad de intercambiar y compartir bienes o servicios a través de plataformas electrónicas. La economía colaborativa plantea nuevos procesos de intermediación disruptivos que han cambiado las reglas de juego en negocios clave.

La tecnología aplicada en las organizaciones - como un recurso humano utilizado por humanos por más desarrollo que haya tenido en el pasado - mantiene ciertas limitantes. La aplicación de la tecnología en las instituciones y las organizaciones depende de factores tales como la cultura.

Pero no sólo la cultura es un aspecto importante. Asoma primero tímidamente y luego con mayor vigor la necesidad de separar la paja del trigo. Esto es definir qué es lo bueno y que es lo malo respecto a los reacomodos de poder derivados del uso de estas tecnologías. Aparecen finalmente los aspectos éticos.

"De todas las creencias que nacieron en Silicon Valley, sin duda la más extraña es el tecnopopulismo; es decir, hacer falsas promesas sobre la base de la transformación digital." En especial promesas relacionadas con que el usuario obtendrá un poder inmediato con el uso de ciertas plataformas. (Morozov, 2018: 1)

Esas nuevas plataformas han aportado algunos beneficios directos de ciertos procesos de desintermediación, de la mano de acercar agentes que requieren por ejemplo un auto para trasladarse o una habitación para resguardarse. Pero también han generado condicionamientos muy fuertes en el manejo de las cadenas de valor.

Nos referimos a la posibilidad de que los administradores que controlan la infraestructura para administrar determinadas redes, monopolicen el uso de una enorme cantidad de datos y la posibilidad de desarrollar subsidios cruzados entre los diversos usuarios, manejando los modelos de negocios derivados. (Srnicek, 2018)

Todo parece indicar que la utopía del desarrollo digital en el que el mercado se autorregulaba con beneficios equitativos para todas las partes, está llegando a su fin a partir de una web, que opera de una manera cada vez más centralizada y en manos de unas pocas plataformas dominantes. (Morozov, 2018)

Aparecen entonces necesidades de desarrollar aportes prescriptivos sobre el "debe ser" en términos éticos respecto de lo que hacen o pueden hacer estas plataformas, para condicionar las decisiones de los agentes que la utilizan, sin que estos agentes tengan real conciencia de estos procesos de manipulación.

Estas plataformas manejan enormes cantidades de información sobre quiénes somos los usuarios, que es lo que más nos interesa, lo que estamos actualmente aprendiendo, qué necesitamos comprar o vender, de qué manera nos entretenemos y qué orientaciones políticas o religiosas tenemos.

Alguien que maneja toda esta información tiene en sí mismo un enorme poder para orientar las decisiones políticas, económicas o sociales y religiosas de los agentes e incluso para generar replanteos de las mismas solamente presentando el lado circunstancialmente más conveniente de determinados datos que maneja.

En la actualidad ese poder de manejo de enormes cantidades de datos de los usuarios de los motores de búsqueda de información y de manejo de las relaciones dentro de las grandes redes sociales a escala global, se ejerce de manera casi discrecional, con fines que no son conocidos por los agentes afectados.

Pensamos que además de ciertas declaraciones de principio que siempre son buenas como orientación, respecto de cómo deberían manejarse esas grandes plataformas y la información que manejan, también hay que abordar cuestiones instrumentales relevantes de cómo se administran las relaciones, que todavía no están claras.

Los desafíos éticos del manejo de datos, sobre todo en lo relacionado con el enorme poder de algunas plataformas globales, debe aparecer en la mesa de discusiones de manera que las potencialidades libertarias y desintermediadoras de la Internet, no se vean tan constreñidas por el dominio de un conjunto de poderosas corporaciones.

Aparece la necesidad de replantear ciertas reglas de juego relacionadas con la discrecionalidad de gobierno con la que se mueven los administradores de las redes y con la confiabilidad de los datos que manejan. Es necesario generar las condiciones para un buen gobierno corporativo y para un manejo de los datos mucho más transparente.

Parece que debería insistirse en establecer cuáles son las reglas de ese buen gobierno corporativo en relación con cómo se manipulan por parte de los administradores los modelos de negocios, cuando estos están dirigidos a manipular la competencia entre los diferentes grupos de interés que operan sobre redes muy globales de uno genérico.

Además es importante afinar los mecanismos de denuncia cuando se constata que los datos que administra una plataforma son usados con otros fines que aquellos con los que fueron solicitados a los usuarios o bien cuando son manipulados o cambiados para influir en las conductas de manera de cambiar lo que deciden.

Ya hay muchas ideas contrapuestas puestas sobre la mesa a partir de los intereses en pugna y los efectos del manejo de las plataformas. Están en juego aspectos muy relevantes que hacen a las decisiones de los ciudadanos sobre la elección de sus representantes o sobre aquello que quieren comprar o vender en las grandes redes.

Recién estamos comenzando a entender el enorme poder que tienen actualmente los administradores de plataformas tecnológicas de relacionamiento. Tal vez sea prematuro anticipar cuáles serían las mejores soluciones a desarrollar. Pienso ahora es el tiempo de los debates de ideas, pero sin ser ingenuos.

Está claro que lo que hagamos o dejemos de hacer sobre la forma en que son gobernadas y gestionadas las grandes plataformas tecnológicas que operan sobre la Internet, seguramente afectará centros de poder que actualmente tienen una posición dominante sobre lo que se presenta como información y sobre lo que se decide.

Referencias

Esains, Victoria. (2011), La Gestión del Conocimiento pasó la etapa infantil de las falsas expectativas. Entrevista a Domingo Valhondo, Disponible en: (http://www.learningreview.com/gestion-del-conocimiento/articulos-y-entrevistas/366-la-gestiel-conocimiento-pas-etapa-infantil-de-las-falsas-expectativas).

Friedman, Thomas. (2018), Gracias por llegar tarde. Cómo la tecnología, la globalización y el cambio climático van a transformar el mundo los próximos años, Buenos Aires, Editorial Paidos.

Gibbons, Michael; Limoges, Camilla; Nowonty, Helga; Schwartzman, Simon; Scott, Meter y Trow, Martin. (1994), The New Production of Knowledge. The dynamics of science and research in contemporary societies, Londres, Sage Publications.

Joyanes, Luis. (1997), Cibersociedad, Madrid, Mc Graw Hill.

Miah, Andy. (2012), Cuestiones éticas derivadas del mejoramiento humano, Disponible en: (https://

www.bbvaopenmind.com/articulos/cuestiones-eticas-derivadas-del-mejoramiento-humano/)

Morozov, Evgeny, (2018), De Airbnb a Uber: la economía colaborativa está en manos del gran capital, Disponible en: (https://www.eldiario.es/theguardian/Airbnb-ciudad-economia-compartida-capital_0_840266844.html)

Schumpeter, Joseph. (1997) Teoría del desenvolvimiento económico, México, Fondo de Cultura Económica.

Srnicek, Nick. (2018), Capitalismo de Plataforma, Buenos Aires, Caja Negra Editores.

Winner, Landon. (2008), La ballena y el reactor, Barcelona, Gedisa Editorial.

Ing. Carlos Petrella, PhD

Investigador, docente, escritor y conferencista con más de diez libros y más de cuarenta artículos académicos publicados sobre su especialidad.

Docente e investigador grado 5 especializado en Dirección, estrategia y comunicación de la Facultad de Ciencias Económicas y Administración de la UDELAR.

Experto en estudios prospectivos, cambio organizacional, gestión del conocimiento, procesos de innovación, aprendizaje organizacional y coaching, con sustancial experiencia en procesos de desarrollo organizacional, estudios de escenarios de desarrollo y consolidación de grandes empresas y en el asesoramiento en situación de crisis.

CONFERENCIA:
"ÉTICA Y ADVANCE DATA ANALYTICS"

En los últimos años, con el advenimiento de los nuevos modelos de negocios basados en datos, las empresas han comenzado a utilizar información de las personas para poder modelar comportamiento pasados, y desarrollar modelos predictivos capaces de adelantarse a las necesidades de los clientes. Si bien esto se está dando cada vez más en todas las ramas de la economía, las que más generan, analizan y modelan datos, son las empresas relacionadas con el sector IT. Por su parte, hoy las personas generan un volumen enorme de datos, muchos de los cuales no son creados voluntariamente por ellas. Muchos menos, estas personas son conscientes de que estos datos terminan siendo materia prima para que las empresas conozcan su comportamiento, y en última instancia, descifrando cómo viven su día a día. Ya sea Google, Amazon, Microsoft, Facebook, o los propios supermercados, las telefónicas, los retails, entre otros grandes grupos de empresas, tienen información tal que permite entender cómo viven y qué pueden necesitar (o no) cada uno de los ciudadanos. El tema no es solamente si la persona ha dado su consentimiento para utilizar esta información, para lo cual es imprescindible comprender la regulación actual, sino también incorporar la visión ética del tema que complementa la visión legal del mismo. Y muchas veces, la utilización de esta información para el modelado de algoritmos puede llegar incluso a tener riesgos, no solo para las personas, sino para las propias empresas, y la sociedad en su conjunto, como se han identificado en ejemplos como el de Facebook y Cambridge Analytica.

Dirigido a:

Los conocimientos vertidos en la charla son de utilidad tanto a profesionales que se desempeñen en procedimientos relacionados con estas técnicas, como a estudiantes de las carreras de Seguridad, Auditoría y Tecnología.

FECHA:	9 de octubre de 2019
LUGAR:	Sede del capítulo Montevideo. Cerrito 420 of 505. Montevideo, uruguay
DURACIÓN:	2 horas
HORARIO:	18:30 a 20:30 hs.
PRECIO:	SOCIOS Y EST. DE UDELAR: SIN COSTO // CON CONVENIO: $300 // COSTO GENERAL: $400

Expositor invitado:

DIEGO VALLARINO

Diego es PhD en Apllied Economics/Cliometria de la Universidad Torcuato Di Tella de Argentina. Posee un MSc en Data Analytics en la Universidad de Barcelona y es MBA Full Time de la Universidad Adolfo Ibáñez de Chile. Es Licenciado en Administración de Empresas y Contador Público de la UdelaR de Uruguay. Además, tiene postgrados académicos en las universidades de Harvard, Babson y Wharton en EEUU.

Su área de especialización es el Análisis y Diseño de modelos analíticos avanzados enfocados en el ciclo de vida del cliente (prospección, originación, retención y collection), bajo una concepción de economía comportamental de los agentes. Su foco es generar valor diferencial a los clientes a través de combinar la Innovación con Data Engineering, Advance Analytics Modeling y Data Reporting.

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

FCEA FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN

ISACA Montevideo Chapter

Cerrito 420 of 505, Montevideo, Uruguay
Telefax: 29150319
E-mail: info@isaca.org.uy
Web: www.isaca.org/montevideo
Linkedin: Isaca Montevideo Chapter

Inscripciones:
http://isaca.org.uy/eventos

El desafío de ser “bueno”

Vasant Raval

El comportamiento moral es, quizás, fácil hablar, pero difícil de poner en práctica. La respuesta a la pregunta “¿Hice lo correcto?” puede que no sea inequívoca. Por otra parte, lo que yo podría considerar como lo fundamentalmente correcto de hacer, puede que no sea reflejado exactamente (por un acto intencional o no) en la acción siguiente. Existen, de hecho, varios factores en el trabajo que producen la diferencia entre un bien moral que hay que hacer y lo que finalmente se hace. En esta columna, voy a discutir algunas de las razones de esta brecha. Si bien esto no podría ser un examen exhaustivo sobre el desafío de ser bueno, un ejercicio puente entre “el deber” y “el ser” ilustrará lo que necesitamos para ver el futuro.

La cuestión moral

Para cualquier proyecto (o caso) que enfrentemos en el momento, la formulación de una cuestión moral puede no ser una tarea fácil. Si una situación se ha estado gestando desde hace algún tiempo, es probable que el tomador de decisiones haya tenido tiempo para pensar en el caso y construir posibles interrogantes morales. Si la situación es inminente y no dio ningún aviso previo, es difícil de resolver “en sus pies” lo que podría ser una respuesta moralmente apropiada. Además, si dos o más personas están involucradas en el caso, existe la posibilidad de que los individuos involucrados se transmitan su preocupación en relación con la parte ética del proyecto general. Sin embargo, a menos que el escenario sea frecuente, simple o familiar, uno puede encontrar que las respuestas a, o incluso las interrogantes de la acción moral son difíciles de encontrar.

Si hay espacio para la reflexión sobre el aspecto moral del problema en una etapa posterior en la secuencia de decisiones, ciertamente proporcionaría una oportunidad de volver a examinar la cuestión moral a la luz de los progresos realizados hasta el momento. Esto ayudará a determinar si el tomador de decisiones se siente cómodo con la forma en que se identifican y abordan las cuestiones morales y si existe algún espacio para el cambio en el planteamiento del problema y/o método para abordarlo.

Para aumentar la dificultad está el hecho de que las cuestiones morales (no materiales) no se identifican de forma aislada; ellas son inherentes al problema material y la forma en que se resuelven. Hay buenos argumentos

para indicar que la inmediatez y la importancia de los problemas materiales de la organización pueden consumir mucho tiempo y concentración de las personas que participan en la solución del problema, que no tienen recursos disponibles para explorar la ética de la situación[1]. Esta falta de atención puede llegar a ser aún más grave, como los componentes de un gran proyecto que se transmiten a los grupos encargados de resolver sólo la parte del rompecabezas proyecto. La tarea material asignada a un sub-equipo es guiada por las especificaciones detalladas que acompañan a la carga. Por el contrario, incluso si el equipo a nivel de proyecto determina las cuestiones morales y cómo deben ser abordados, el espíritu de la acción moral puede no llegar a los niveles más bajos en la implementación del proyecto. Por estas razones, es probable que los temas no materiales sean dejados atrás, mientras que la tarea material sea cumplida en el afán por ser el primero en el mercado.

En estos días, las batallas legales entre Uber y Airbnb por un lado y los gobiernos por otro, han escalado en diversas materias. Un argumento planteado por los reclamantes (gobiernos) es que los nuevos modelos introducidos por Uber y Airbnb no son compatibles con las normas existentes. Por ejemplo, Bloomberg News informó de que las reglas del Servicio de Impuestos Internos (IRS) de EEUU no son claras para la presentación de informes de ganancias mediante plataformas on-demand. Como resultado, Bloomberg informa, las empresas no retienen los impuestos sobre los ingresos que ellas pagan a los proveedores de servicios.[2] ¿Podrían Airbnb, Etsy y Lyft haber visualizado el problema en el ecosistema en que se estaban juntando? La respuesta, por supuesto, es que no sabemos. Es probable, sin embargo, que un cierto grado de intercambio de ideas podría haber disparado preguntas, si no respuestas, sobre el potencial de la falta de retención de impuestos para los contratistas independientes. Tal reflexión podría haber apuntado a la pregunta de cuales de las reglas existentes de la IRS son ambiguas y para cuáles la compañía necesita buscar mayor claridad desde la agencia. A la luz de las innovaciones de los habilitadores tecnológicos, preguntas sin precedentes han surgido; como resultado, la esperanza es que la preocupación de las organizaciones sea proactiva en la búsqueda de respuestas. Por ejemplo, el Instituto Americano de Contadores Públicos Certificados (AICPA) envió a la IRS una carta solicitando clarificación sobre la situación de los impuestos de temas relacionados con monedas virtuales (eCurrency[3]), incluyendo reglas para las donaciones en monedas digitales.

Un par de observaciones emergen desde el conflicto entre las nuevas plataformas emergentes tales como Uber y los reguladores. Primero, si la regulación es un indicador de la necesidad por mantener verdad y armonía en un sistema[4, 5], entonces la presencia de regulaciones en el actual ecosistema podría entregar algún entendimiento del legalmente mínimo mejor comportamiento. Después de filtrar que es irrelevante para el nuevo ecosistema, uno podría derivar una línea base de entendimiento de porque estas reglas actualmente existen y como ellas podrían impactar en la regulación futura de la nueva industria. Segundo, ambas modelos Uber y Airbnb dejan el componente de la sensibilidad humana (conductores, anfitriones) ampliamente fuera de sus propios perímetros. Dado que las cuestiones morales son inherentes a los problemas humanos, uno podría haber pensado sobre los nuevos modelos como aislados desde, o fuera del alcance de los problemas morales que preocupan a los colaboradores (conductores, anfitriones). Pero dado que la responsabilidad por aquellos a quienes encomiendan servicios presumiblemente descansa en la empresa propietaria del modelo de negocio, algún grado de análisis de las actuales prácticas en el entorno tradicional era garantizado. Una debilidad aquí ha impactado las reputaciones de Uber y Airbnb.

Dado que no existen respuestas infalibles para el desarrollo de cuñas entre progreso sobre los lados materiales y morales, ayudaría

tener medidas establecidas para un comportamiento responsable. Por ejemplo, un proceso integral donde preguntas morales sean realizadas, direccionadas y documentadas en conjunto con preguntas materiales, esto ayudaría a reconocer brechas, si existen, y a direccionarlas de manera oportuna.

"Ser 'bueno' tiene un aura de positividad por las razones correctas... Pero la acción moral exige costos de todo tipo."

¿Quién es el responsable?

Una buena interrogante moral debe claramente articular el problema y el estado de para quien es el problema. En una pregunta general sobre la aceptabilidad moral de un particular curso de acción o tecnológico, no identificamos necesariamente para quien es el problema[6]. El lugar de algunos problemas puede ser un individuo o una familia; para otros, puede ser una organización; y para otros incluso, puede ser la sociedad o las agencia del gobierno. A menudo, un eslabón débil al ejercer la responsabilidad recae sobre el responsable[7]. Por ejemplo, al proteger nuestra privacidad, tenemos que seguir ciertos pasos. De hecho, todas las seis condiciones asociadas con la privacidad (aviso, elección, uso, seguridad, corrección y aprobación) incluyen la frase "el individuo tiene el derecho a"; sin embargo, por varias razones, la gente prefiere hacer caso omiso de lo que tiene que hacer. El modo de pensar que domina la mayoría también determina el estado general de la integridad en el ecosistema. Una de las razones que la gente piensa de una manera y se comportan de manera diferente por razones éticas se llama "conciencia restringida".

"La 'inmoralidad de silencio' impregna a la sociedad más allá de una medida que uno puede imaginar."

El concepto puede explicarse como "la tendencia común de excluir información relevante de nuestras decisiones mediante la colocación de límites arbitrarios en torno a nuestra definición de un problema, lo que resulta en una falla sistémica para ver información importante"[8]. Además, se afirma que las personas también sufren de "condición ética limitada" o "restricciones sistemáticas sobre nuestra moralidad que favorecen nuestro propio interés"[9]. Como resultado, surgen deficiencias éticas, las cuales se agravan a nivel de organización. De hecho, las diferencias o brechas en la organización son más que la suma de las diferencias de los distintos miembros debido al fenómeno de pensamiento de grupo, que arrastra al grupo hacia la unanimidad e inhibe de diálogo abierto sobre cuestiones éticamente difíciles[10].

Puesto que los individuos y sus familias son responsables de ser "buenos" en sus vidas privadas, organizaciones (con y sin fines de lucro, así como el gobierno) son responsables de un gobierno responsable. En última instancia, que tan bien se abordan las cuestiones no materiales en las organizaciones depende en gran medida del clima de la organización. Si el clima esté incitando un comportamiento adecuado, lo más probable es que se hagan serios intentos proactivos para identificar y tratar las cuestiones morales que conllevan las cuestiones materiales.

Los investigadores advierten que debemos prestar atención a lo que no se está hablando dentro de una organización, ya que puede proporcionar información valiosa acerca de los valores informales[11], una poderosa fuerza en la conformación de la cultura de la empresa. Es responsabilidad del líder el establecer el tono en la cima de la organización. Sin embargo, también es necesario para la organización el evaluar continuamente la calidad del clima. A menos que algunos signos vitales sean monitoreados regularmente, será difícil buscar comodidad en el tratamiento de las cuestiones morales, como y cuando estas se presenten.

Costo de la moralidad

Ser "bueno" tiene un aura de positividad por las razones correctas. Se hace la vida útil y nos permite conservar nuestra paz interior.

Se propaga la calma en nuestra mente constantemente agitada y nos hace felices. Pero la acción moral exige costos de todo tipo (es decir, dinero, energía, pérdida de oportunidades). Por ejemplo, un estudiante puede obtener una baja puntuación en una prueba por no recurrir a la trampa. Sin embargo, para el progreso académico del estudiante, sus calificaciones podrían ser demasiado importante como para sacrificarlas. Actuar con honestidad podría costar la admisión a un programa de postgrado de prestigio.

Sea usted un gerente, un estudiante, un denunciante, un líder o un auditor, no es así de fácil hacer caso omiso de las posibles consecuencias de sus acciones voluntarias. El miedo al castigo, la amenaza de la pérdida del trabajo, otras amenazas a la persona o su familia, y la turbulencia esperada en la vida de uno, éstos están en juego al considerar una acción audaz. Sumando y ordenando todo contra de lo que uno podría obtener de esa acción a menudo deja a las personas poco dispuestas a "mover el bote". La observación pasiva de un hecho ilícito desde un costado es inmoral, pero ¿cuántos saltas y combaten contra el actor de ello? La "inmoralidad de silencio"[12] impregna a la sociedad más allá de una medida que uno puede imaginar. Por ejemplo, si nadie cuestiona irregularidades organizacionales, tales como una invasión de la privacidad, la práctica de violar el derecho de los demás a la privacidad podría convertirse en la norma.

El anonimato ha demostrado ser una medida de protección para alentar a la gente a hablar sobre hechos ilícitos. Si se utiliza el anonimato para preservar las libertades personales, proteger los secretos comerciales o mejorar la calidad de las respuestas, necesitamos sistemas diseñados para asegurar la desasignación[13]. La tecnología puede proporcionar soluciones, como los sistemas de denuncia de irregularidades, que ayudan a preservar la privacidad de los informantes.

La intervención moderada de la tecnología, si es percibida por el informante prospectivo como segura, puede resultar en la detección y tratamiento de la acción inmoral de forma oportuna y orgánica. Debemos tener en cuenta, sin embargo, que lo que funciona para proteger el anonimato de manera correcta también puede crear problemas en otros conceptos. Por ejemplo, el anonimato en las eCurrency puede engendrar actos ilegales de lavado de dinero. Incluso en ecosistemas que otorgan anonimato, siempre existe el riesgo de que alguien rompa el secretismo. El caso de los Panamá Papers[14] es sólo un ejemplo de cómo la tecnología puede revelar los generalmente invisibles malhechores y a sus socios.

Convicción en la causa

Los juicios éticos se basan en marcos formales e informales. Un marco de intuicionismo ético (intuitivist) ayuda a uno a identificar las acciones morales aceptables intuitivamente. Un marco de valor dominante identifica las acciones morales apropiadas mediante la generación de una convicción sobre el valor más dominante entre los valores que compiten en un dilema moral[15]. Independientemente del marco utilizado, la percepción de los diversos valores es un disparador importante para la acción moral. Sin una fuerte identificación con un valor, uno podría dejar de ver la importancia de una acción que elija para poner en práctica.

Una serie de ejemplos pueden ser observados aquí: en la política (Martin Luther King Jr. y Rosa Parks), sociología (Candace Lightener y Madres Contra Conductores Ebrios [Mothers Against Drunk Driving]), negocios (Blake Mycoskie de Tom's Shoes), y tecnología (Julian Assange y WikiLeaks, el caso de Edward Snowden relacionado con la vigilancia y la Agencia de Seguridad Nacional de Estados Unidos [NSA]). Independientemente de si usted cree en su causa, cada uno tenía una fuerte convicción de que algo estaba mal y la necesidad de corregir la situación. Es por ello que tomaron el riesgo y, tal vez en un gran esfuerzo, entregaron su opinión a los demás

para hacer que algo suceda. Si bien la convicción en la causa es fundamentalmente importante para la acción moral, es también necesario que la persona tenga la valentía de hacer lo correcto. Reunir la valentía no es una tarea fácil, debido a que las consecuencias mundanas de desafiar las irregularidades pueden ser devastadoras para la vida de uno. Por consiguiente, la valentía se menciona a menudo en paralelo con la causa y la primera (cuando se actúa) a menudo implica un comportamiento valiente.

La moralidad como una cualidad humana

Por definición, la moral se refiere a los seres humanos, no máquinas. Todos los sistemas son esencialmente una asignación de tareas entre personas y máquinas; algunos tienen incluso un papel mucho más importante para los seres humanos que las máquinas, otros están dominados por las máquinas. Entre los papeles que siguen siendo de los seres humanos está el papel del agente moral. En este papel, un profesional de TI no sólo se esfuerza por comportarse de manera ética, sino que también diseña las tareas automatizadas (la parte que corresponde a las máquinas) de una manera moralmente responsable. Por lo tanto, el entendimiento de lo que es moral en las máquinas es la responsabilidad de los seres humanos al hacerse cargo de la asignación de tareas hombre/máquina. Para ello, la consideración de los asuntos no materiales por adelantado es fundamental en la consolidación de un comportamiento responsable predecible en los sistemas automatizados.

"Desde los automóviles automatizados hasta los aviones no tripulados (drones), toda una serie de normas de comportamiento moral está programado en las máquinas."

Curiosamente, el desarrollo en el campo de la inteligencia artificial (IA) ha reducido el papel de los seres humanos en una asociación hombre-máquina en sistemas automatizados. El disminuido papel del ser humano en los nuevos sistemas puede parecer pequeña, pero no es insignificante; es la parte del sistema que aún necesita del juicio humano y opciones impulsadas por valores. Las decisiones que el diseñador humano hace en la creación del sistema automatizado tienden a ser implantadas de forma permanente en la vida de la máquina. Las máquinas pueden aprender a cambiar su comportamiento, pero sólo si el aprendizaje automático ha sido programado adecuadamente. El elemento humano en el impacto moral en general no puede ser subestimado o ignorado. Desde los automóviles automatizados hasta los aviones no tripulados (drones), toda una serie de normas de comportamiento moral está programado en las máquinas.

Cualquier error de juicio en la etapa de diseño presagia mayor riesgo de compromisos morales. Las cuestiones de comportamiento ético son fundamentalmente cuestiones humanas. Ya sea fuera o dentro del perímetro legal de una empresa, colaboradores humanos seguirán participando activamente en el ecosistema. En el contexto de 'automóvil para contrato', tal vez esta pregunta vaya a desaparecer o a cambiar drásticamente cuando Uber despliegue vehículos autónomos. Y para los drones, las reglas dominan su comportamiento; hasta que estén diseñados para aprender, la responsabilidad por la base moral de los drones corresponde a los tecnólogos. Con el tiempo, cuando las máquinas se vuelvan casi autónomas, la ética de la máquina se podrá extender a lo que los robots pueden aprender.

.

Notas Finales

1 Martin, K. E.; R. E. Freeman; "The Separation of Technology and Ethics in Business Ethics",*Journal of Business Ethics*, vol. 53, 2004, p. 353-364

2 *Bloomberg News*, "Billions From Airbnb and Others Go Unreported," as reported in the *Omaha World-Herald*, 24 May 2016

3 Saunders, L.; "The Latest Stumbling Block for Bitcoin: How to Tax It," *The Wall Street Journal*, 25 June 2016

[4] Kohlberg's moral stage development work includes compliance with the laws and regulations as one of the stages. See Kohlberg, L.; "Moral Stages and Moralization: The Cognitive Development Approach," December 1975.

[5] Kohlberg, L.; *The Psychology of Moral Development: The Nature and Validity of Moral Stages*, Harper and Row, USA, 1984

[6] Van de Poyel, I.; L. Royakkers; "The Ethical Cycle," *Journal of Business Ethics*, vol. 71, February 2007, p. 1-13

[7] Mims, C.; "In Securing Our Data, the Weak Link Is Us," *The Wall Street Journal*, 19 January 2016

[8] Bazerman, M.; A. Tenbrunsel, "Blind Spots: The Roots of Unethical Behavior at Work," *Rotman Magazine*, Spring 2011, p. 53-57

[9] *Ibid.*

[10] *Ibid.*

[11] *Ibid.*

[12] Das, G.; *The Difficulty of Being Good: On the Subtle Art of Dharma,* Oxford University Press, United Kingdom, 2010, p. 59

[13] Poore, R. S.; "Anonymity, Privacy, and Trust," *Information Systems Security*, vol. 8, iss. 3, 21 December 2006, p. 16-20

14 Stack, L. *et al.*; "The Panama Papers: Here's What We Know," *The New York Times*, 4 April 2006, www.nytimes.com/2016/04/05/world/panama-papersexplainer.html?_r=0

[15] *Op cit*, Van de Poyel and Royakkers, p. 6

Vasant Raval, DBA, CISA, ACMA

Es profesor de contabilidad en la Universidad de Creighton (Omaha, Nebraska, USA). Es co autor de dos libros sobre los sistemas de información y seguridad, sus áreas de enseñanza e intereses de investigación incluyen la seguridad de la información y la gestión empresarial. Las opiniones expresadas en esta columna son personales y no de la Universidad de Creighton. Él puede ser contactado en vraval@creighton.edu

CURSO:
"COBIT 2019 FOUNDATION"

Objetivos Generales:
Lograr que los participantes conozcan los principales conceptos del producto COBIT, así como las razones fundamentales por las que es utilizado como un marco de Gobierno para la Información y Tecnología. Preparar a los participantes para el examen COBIT 2019 Foundation.

Dirigido a:
Miembros del Consejo de las organizaciones.
Ejecutivos de negocios que deban participar en el análisis, el planeamiento y en la toma de decisiones estratégicas relacionadas con el uso de la tecnologías y de la información en la organización.
Profesionales de la organización y consultores en las áreas de Gobierno, Aseguramiento, Riesgos, Tecnologías de la Información, Auditoría, Control Interno, Operaciones, Privacidad y Seguridad.

Temario:

Está compuesto por 10 módulos:

1- Introducción al curso COBIT 2019.
2- Introducción al marco COBIT 2019.
3- Principios.
4- Sistema de gobierno y componentes.
5- Objetivos de gobierno y gestión.
6- Gestión de desempeño.
7- Diseñando un sistema de gobierno personalizado.
8- El caso de negocio inicial.
9- Implementando el Gobierno Empresarial de I & T.
10- Resumen del Curso.

FECHA:	22, 23 y 24 de octubre de 2019
LUGAR:	Sede del capítulo Montevideo. Cerrito 420 of 505. Montevideo, Uruguay
DURACIÓN:	20 horas
HORARIO:	22 y 23 de 9:00 a 13:00 y de 14:30 a 18:30, 24 de 9 a 13 hs
INVERSIÓN:	Socios: $8000 Con Convenio: $12000 Costo general: $15300

DOCENTE:

SYLVIA TOSAR

Ingeniera en Computación, UdelaR. M.Sc. en Información y Comunicación (Universidad Paul Valéry- Montepellier III, Francia).
Certificaciones: CGEIT, COBIT 5 Accredited, COBIT 2019 Accredited, ITIL Version 3 Foundation Examination,COBIT 2019 Approved Trainer, COBIT 5 Approved Trainer, PMP. Coordinadora CGEIT del Capítulo Mvdeo de ISACA, Miembro de ISO/IEC JTC 1/ SC40 IT Service Management and IT Governance, Miembro de la ISO/TC 309 "Gobernanza de las organizaciones", Miembro del Joint Working Group con SC 42 "Governance implications of AI", Docente de UNIT en Gobernanza de las Tecnologías de la Información, Delegada por la UDE en el Comité de Gobierno y Gestión de Servicios de TI de UNIT.
Amplia experiencia en cargos de Dirección, tanto en lo privado como en el Estado.

COBIT 2019

ISACA
Montevideo Chapter

Cerrito 420 of 505, Montevideo, Uruguay
Telefax: 29150319
E-mail: info@isaca.org.uy
Web: www.isaca.org/montevideo
Linkedin: Isaca Montevideo Chapter

Inscripciones:
http://isaca.org.uy/eventos

Por qué es importante el rol de ISACA para Ética en el Data Science

Diego Vallarino

Omnipresentes e invisibles, los algoritmos determinan cada vez más nuestro día: qué películas nos propone Netflix o cuánto nos cuesta una reserva de hotel. Gracias a ellos se pueden gestionar cantidades enormes de información de manera más eficiente. Pero también pueden terminar discriminando por cómo han sido desarrollados.

Un ejemplo que da Marta Peirano en *El enemigo conoce el sistema*[1] es el de David Dao, un pasajero al que sacaron a rastras de un avión en abril de 2017. Había pasado todos los controles de seguridad en el aeropuerto de Chicago y estaba esperando el despegue cuando las azafatas llegaron a echarle. Se negó y los agentes de seguridad terminaron sacándolo por la fuerza. United Airlines había vendido demasiados billetes y sobraba alguien. Un algoritmo había determinado que fuera Dao y no otro el expulsado. Él no era tan valioso para la aerolínea como un titular de la tarjeta de viajero frecuente. ¿Usaron también datos socioeconómicos, religiosos o raciales? Se desconoce, porque el algoritmo es secreto.

Hoy las empresas, e incluso los gobiernos, se han dado cuenta que tienen **un activo muy importante dentro de sus bases de datos, la Data**. Esta data permite a las empresas mejorar su competitividad. Por su parte, los gobiernos están entendiendo que el potencial de disponer de datos de los ciudadanos facilita la posibilidad de mejorar la calidad de vida de las personas, al igual de lo que está pasando en las empresas. Ya sea para brindar un conjunto de servicios, como para mejorar el diseño de las ciudades, la seguridad, entre otras tantas cosas que hacen al derecho humano de las personas.

Para lograr esto, **tanto el sector privado como el sector público debe comenzar a profundizar más cómo gestiona este activo tan determinante**. En tal sentido, en la última década la palabra algoritmo, un concepto que existe desde la época de los babilonios, ha comenzado a tomar grandes dimensiones en nuestro diario vivir. ¿Son los algoritmos realmente una cadena numérica solamente o inciden en el desarrollo ético del comportamiento humano? ¿Exclusivamente hacen su trabajo (en el periodismo sería 'informar') o inciden en la conformación de la opinión pública?

A nadie se le escapa la cantidad de algoritmos que pueblan nuestras vidas. Son ingentes. Los encontramos en multitud de si-

tuaciones cotidianas. Cantidad de desarrollos algorítmicos los vemos presentes a diario no solo en los ordenadores, en nuestros vehículos, en electrodomésticos, en los *call centers*, en la megafonía, en los sistemas de vigilancia…

Además, la inteligencia artificial (IA) se está introduciendo en un creciente número de tareas realizadas hasta la fecha por humanos. En ese nuevo escenario aparece, por ende, el *machine learning* donde las máquinas (el software que incorporan) van aprendiendo de sus errores, capacitándose mejor para próximas intervenciones. Es lo que Sherry Turkle ha definido como el 'horizonte robótico'.

Quizás el concepto máquina no sea el adecuado para definir a todo ese complejo mundo de los robots y los *cobots* (cuando tienen entidad física), pero tenemos los denominados asistentes personales inteligentes. ¿Quién no conoce a Alexa, Siri o Cortana, por ejemplo?) o también a los *bots* sociales y los *chatbots* (cuando se trata exclusivamente de concretar paquetes informáticos). Todos ellos albergan algoritmos que permiten múltiples funciones. Incluso la interacción humana a través del lenguaje.

Muchos algoritmos se han diseñado bajo unas determinadas concepciones éticas… o en ausencia de ellas. Y ello es potencialmente peligroso. Estamos frente a un nuevo contexto de organización donde la sociedad necesita establecer un conjunto de reglas para gestionar la dinámica de esas creaciones y su afectación al comportamiento humano y al desarrollo social.

Ya se han alzado algunas voces que tratan de concretar jurídicamente la existencia de las personas electrónicas (por contraposición a las físicas y a las jurídicas), de tal manera que puedan ser dotadas de derechos y deberes. **Ello posibilitaría, por ejemplo, la creación de impuestos y obligaciones tributarias, pero también la obligación de sus creadores de desarrollar algoritmos 'con alma', que respeten ciertas normas éticas, presentes en cada sociedad.**

¿Dónde está la línea que separa **un buen de un mal uso o abuso del poder de los datos** y los algoritmos?, se pregunta Rachel Botsman, madre filosófica de la economía colaborativa, en su último libro Who can you trust? How technology brought us together and why it might drive us apart[2]. Y todo esto antes de que saltara el *escándalo Facebook* por el uso de los datos de sus usuarios para, supuestamente, influir en campañas políticas.

La ética debe estar implícita en todo el ciclo de vida del Big Data.

Empezando por su **recolección**: por ejemplo, ¿son válidos los datos oficiales de una población si deliberadamente se ha excluido cierta etnia? Siguiendo por lo más complejo, el **algoritmo utilizado:** ¿Puede una simple traducción automatizada pecar de machista[3]? ¿Qué validez tendría un juicio apoyado en la alta probabilidad de volver a delinquir que apunta el rating criminal de ese individuo[4] [sistema muy utilizado en Estados Unidos] según unos datos sesgados? Estos ejemplos ilustran que es un error pensar que, frente a la subjetividad humana, los datos, el Big Data, son siempre acertados y objetivos. Y no necesariamente. Los **datos pueden estar sesgados, mal combinados, manipulados** o, simplemente, **mal interpretados** porque se basaron en algoritmos que resultan erróneos.

Pero vayamos al último eslabón de la cadena, el más sutil y poco evidente, el **propósito de los datos.** ¿Cómo califican el uso de datos personales en redes sociales para influir en campañas políticas? ¿Y cambiar los algoritmos para influir en las emociones de las personas, como reveló este experimento que difundió Facebook en 2014[5]?

"Las organizaciones que actúen con **ética y transparencia** en el uso de los datos tendrán una valoración positiva de la sociedad. Y al contrario, quienes no se rijan por esos parámetros sufrirán una enorme pérdida en su **reputación**", señala Eva García San Luis, socia responsable de Data & Analytics de

KPMG. Y subraya que, "en la era digital, la **confianza en una organización** no se mide solo por su marca, líderes, valores o empleados. También, y cada vez más, por **su forma de gobernar y gestionar los datos, los algoritmos**, las máquinas…".

Un ejemplo de lo que está pasando en el mundo lo puede ejemplificar Francia. En el Senado francés se está debatiendo estos días si se debe **exigir por ley que la Administración explique los algoritmos que utiliza en sus aplicaciones**. Miles de estudiantes se quejan de que la plataforma que gestiona su admisión en la enseñanza superior, Parcoursup, ha sido programada con criterios sesgados. Supuestamente, favorece a los estudiantes con más información y, en definitiva, con más recursos. Y, aunque hace dos años que la Ley Digital exige la transparencia algorítmica en Francia, esta no se da ni por parte del Gobierno ni de las empresas.

A modo de cierre, en este marco de desarrollo de sistemas inteligentes como lo son los algoritmos de aprendizaje dinámico, los profesionales que son integrantes del capítulo uruguayo de ISACA (*Systems Audit and Control Association*), deben ser conscientes que tienen mucho para aportar en esto de entender **cómo se desarrollaron esos algoritmos, qué data usan, cuáles son los objetivos que buscan, y que sesgos tienen implícitamente dentro de los outputs.** Esto redundará en un mayor valor para la ciudadanía y para las empresas en su conjunto. Igualmente, seamos claros, queda mucho por hacer…

Referencias:

1 El enemigo conoce el sistema. https://www.youtube.com/watch?v=WcP6yqf-3wc.

2 Who can you trust? How technology brought us together and why it might drive us apart. https://www.tendencias.kpmg.es/2018/04/entrevista-director-cnpic-ciberseguridad-infraestructuras-criticas/

3 Google Translate might have a gender problema. https://mashable.com/2017/11/30/google-translate-sexism/#pkhtgfpmksqa

4 There's software used across the country to predict future criminals. And it's biased against blacks. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

5 Así manipuló Facebook las emociones de sus usuarios. https://elpais.com/elpais/2014/06/30/icon/1404123574_764889.html

6 Eva García San Luis, KPMG. https://home.kpmg.com/es/es/home/servicios/advisory/risk-consulting/it-advisory/data-analytics.html

Diego Valarino

Es profesor e integrante del comité académico del Posgrado en Sistemas de Información de la Facultad de Ciencias Económicas y de Administración (UdelaR), PhD en Applied Economics/Cliometría de la Universidad Torcuato Di Tella de Argentina. Posee un MSc en Data Analytics en la Universidad de Barcelona y es MBA Full Time de la Universidad Adolfo Ibáñez de Chile.

Es también Licenciado en Administración de Empresas y Contador de la UdelaR de Uruguay. Además, tiene postgrados académicos en las universidades de Harvard, Babson y Wharton en EEUU.

Su área de especialización es el Análisis y Diseño de modelos analíticos avanzados enfocados en el ciclo de vida del cliente (prospección, originación, retención y collection), bajo una concepción de economía comportamental de los agentes. Su foco es generar valor diferencial a los clientes a través de combinar la Innovación con *Data Engineering, Advance Analytics Modeling y Data Reporting*.

Posee + 5 años en responsabilidad de C-Level en empresas multinacionales, + 8 años en Advance Data Analytics, + 18 años de experiencia en el Diseño e Implementación de Nuevos Proyectos con un fuerte componente de Innovación, Tecnología y Advance Analytics. Ha liderado equipos multidisciplinarios y multiculturales en Argentina, Bolivia, Chile, Paraguay, y Uruguay con logros destacados.

Es profesor invitado "Ética y Data Science" y "Data Value Innovation" en diferentes Escuelas de Negocios en América Latita. Es columnista habitual de la Revista Forbes (LatAm, desde 2014). Es autor del libro *"Innovando desde el Sur: Cómo las empresas de América Latina enfrentan la nueva competencia"* (2005). Es consultado habitualmente sobre temas relacionados con su profesión en radios y periódicos nacionales y extranjeros.

Certified Information Security Manager®

An ISACA® Certification

Certified Information Systems Auditor®

An ISACA® Certification

Certified in Risk and Information Systems Control™

An ISACA® Certification

Certified in the Governance of Enterprise IT®

An ISACA® Certification

Cinco claves para la implementación de su SGSI

Carlos Villamizar R.

Para la implementación de un **Sistema de Gestión de Seguridad de la Información**[1], la norma ISO27001:2013 establece los requisitos que debe cumplir una organización para la definición, implementación, revisión y mejora continua de seguridad de la información. Esto lo que busca es proteger apropiadamente la información frente a amenazas que puedan afectar su **Confidencialidad, Integridad y/o Disponibilidad**. Bajo este contexto, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Según las últimas estadísticas disponibles de la **International Organization for Standardization** (ISO) al finalizar el año 2017, 39.501 empresas en todo el mundo se habían certificado en la norma ISO27001:2013[2].

El top 10 de los países con mayor cantidad de empresas certificadas en ISO 27001 está liderado por Japón, seguido por China y el Reino Unido.

Top 10 - Países certificados en ISO 27001		
Posición	País	Certificaciones
1	Japón	9161
2	China	5069
3	Reino Unido	4503
4	India	3272
5	Estados Unidos	1517
6	Alemania	1339
7	Taiwán	994
8	Italia	958
9	Holanda	913
10	España	803

A nivel mundial, Colombia ocupaba en 2017 el lugar 35 (descendió desde la posición 29 que ocupaba en 2016) con 148 empresas certificadas, siendo el tercer país de LATAM en el ranking general (superado sólo por México y Brasil). La siguiente tabla lista el Top 10 de países con empresas certificadas en LATAM:

Top 10 - Países LATAM certificados en ISO 27001		
Posición	País	Certificaciones
23	México	315
34	Brasil	170
35	Colombia	148
50	Chile	64
52	Argentina	57
57	Perú	43
64	Uruguay	31
73	Costa Rica	21
83	Jamaica	11
87	Ecuador	8
88	Panamá	8

De acuerdo con la experiencia adquirida en los últimos 12 años en cientos de proyectos de definición e implementación de SGSIs en Latinoamérica y España (algunos de ellos con objetivo final de certificación), hemos identificado 5 aspectos básicos para la culminación exitosa de estas iniciativas:

1. **Compromiso de la alta dirección.** Para que la iniciativa entregue los resultados esperados, es requisito necesario el apoyo y la participación de la Alta Dirección de la empresa. Sin su apoyo formal real, es casi imposible desarrollar con éxito la iniciativa y demostrar el logro de la conformidad en la implementación del SGSI. Aquellas iniciativas que provienen desde los sectores operativos y/o tácticos y no cuentan con el respaldo de la Alta Dirección tienen mayor posibilidad de fracaso.

2. **Cada empresa es un mundo diferente.** Cada empresa es un mundo particular, así pertenezcan al mismo sector económico o a un mismo grupo empresarial. Cada una tiene su ambiente de control particular, un apetito de riesgo particular, y riesgos de seguridad de la información distintos. Lo que es bueno para una empresa, pueda que no lo sea para otra. Copiar tal cual de una empresa a otra NO es procedente. Luego se debe considerar un entendimiento de los requerimientos de seguridad y gestión de riesgos particulares de cada organización.

3. **Definición apropiada del Alcance.** Es importante definir un **alcance del SGSI** realizable. El esfuerzo para implementar el SGSI no es el mismo al definir en su alcance TODOS los procesos de la organización, a un alcance que incluya sólo 1 o 2 procesos misionales. En este sentido es mejor iniciar con pocos procesos y paulatinamente ir creciendo el alcance del SGSI a medida que se logra mayor madurez en seguridad de la información.

4. **Los controles no son todo.** Es un error creer que la implementación de los controles de seguridad incluidos en el Anexo A de la norma es "el todo", sin considerar los elementos clave de un SGSI como, por ejemplo, Objetivos de seguridad de la información, Declaración de aplicabilidad (SOA), métricas e indicadores de seguridad para evaluar el desempeño, información documentada, procedimientos de auditoría interna, no conformidades, acciones correctivas, etc., y por supuesto concienciar a los recursos humanos de la compañía mediante diversos medios: afiches, pendones, protectores de pantalla, videos, trivias, juegos, obras de teatro, etc.

5. **Automatizar el SGSI.** Tradicionalmente estas iniciativas se ejecutan con el apoyo de herramientas de ofimática. Sin lugar a dudas el uso del software **GlobalSUITE® Information Security**[3] ha sido factor crítico de éxito en la obtención de la certificación por parte de nuestros clientes ya que ha reducido la duración de la consultoría en por lo menos un 25% (especialmente en las actividades de **inventario de activos, gestión de riesgos y establecimiento de métricas e indicadores**), ha permitido que el cliente se involucre directamente en el uso de la herramienta conservando todos los registros y documentos del SGSI en un solo repositorio de información y sobre todo ha permitido dar autosostenibilidad al SGSI sin dependencia directa hacia el

equipo de consultoría, ya que lo hemos construido conjuntamente. En este sentido, **GlobalSUITE**®[4] cubre todo el ciclo PHVA de la norma ISO27001 y permite la mejora y sostenibilidad por parte del cliente de su SGSI.

Referencias:

1 Sistema de Gestión de Seguridad de la Información ISO 27001 https://www.globalsuitesolutions.com/es/seguridad-informacion-iso-27001/

2 Fuente: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

3 Software GlobalSUITE® https://www.globalsuitesolutions.com/es/seguridad-informacion-iso-27001/

4 GlobalSUITE® https://www.globalsuite.es/es/

Carlos Villamizar R.

Es Ingeniero de Sistemas y Especialista en Auditoría de Sistema de Información por la Universidad Católica de Colombia. Cuenta con las certicaciones CISA, CISM, CGEIT, CRISC, ISO27001 LA e ISO22301 LI. Tiene amplia experiencia como auditor y consultor en Gobierno de TI, Seguridad de la información, Continuidad y/o Aseguramiento de TI en las organizaciones. Es Director de Operaciones de GlobalSUITE en Colombia.

Pronósticos de seguridad/ ciberseguridad 2020

Jeimy J. Cano M.

Introducción

En un contexto digital asistido por la *desintermediación*, la *distribución*, la *desinformación*, la *deslocalización* y la *desinstalación*, los flujos de información y las plataformas tecnológicas operadas por terceros adquieren una mayor relevancia y atención, no sólo por los ejecutivos de las empresas, sino por los adversarios. Este nuevo escenario de negocios, que no es responsabilidad exclusiva del área de TI, establece nuevas relaciones y retos para crear experiencias novedosas en los clientes y abrir posibilidades inexistentes para las empresas.

Lo anterior exige crear un "retorno de la experiencia", es decir, un nuevo ROI (Retorno de la inversión) que consiste en mapear el viaje de compra de los clientes, aislar los puntos de contacto y los factores que impulsan la experiencia (Maxwell, 2019), de tal manera que se puedan crear patrones y condiciones particulares para todos los participantes, con lo cual la experiencia de compra sea conveniente, ágil y de valor para el comprador.

Este entorno donde se ha superado el uso de los navegadores, por el uso de aplicaciones móviles (de ahora en adelante apps), establece un escenario digitalmente denso donde la conectividad, los flujos de información, los datos personales y las personalizaciones hacen ahora parte de la cotidianidad del mundo actual. Sin perjuicio de que algunos estén o no de acuerdo con esa nueva realidad, es claro que habrá una mayor exposición de las características de las personas y sus gustos, así como el uso de algoritmos especializados para mantener la atención y potencial de compra activado en cada uno de los ciudadanos de internet.

Esta dependencia en aumento de los terceros de confianza, la necesidad de agilidad en el despliegue de soluciones, el uso de la inteligencia artificial para afinar las decisiones, la confiabilidad de la información y el ingreso de la tecnología 5G como habilitador de las futuras ciudades digitales, configura un entorno rico en propuestas de negocios y nuevos vectores de ataques que serán diseñados, para lograr sus objetivos, basados en la economía del adversario, donde se hacen los mínimos esfuerzos para obtener el máximo beneficio.

De esta manera, se presenta a continuación este documento con algunos pronósticos de seguridad/ciberseguridad para el año 2020, como una excusa académica y reflexión

práctica, posiblemente incompleta y limitada, que trata de explorar y conectar ciertos puntos inconexos en el espacio actual de posibilidades, con el fin de motivar reflexiones tanto en los profesionales de seguridad/ciberseguridad, así como en los ejecutivos de las empresas para visualizar escenarios adversos donde un agresor puede tomar ventaja y así estar preparados para cambiar su ecuación de riesgos.

A continuación se presentan las cinco (5) tendencias o pronósticos identificados para un contexto digital e hiperconectado donde más que probabilidades, se debe pensar en posibilidades.

1. Criptominería en IoT

La criptominería es una actividad que se ha venido consolidando desde hace algunos años como una forma de construir base monetaria, algunas veces de manera no autorizada o por debajo de los radares de los reguladores financieros. Para ello la capacidad de cómputo es un elemento fundamental, dado que la generación de criptomoneda demanda dicha capacidad para resolver los retos matemáticos que implica su producción.

"*Los mineros suelen crearse equipos de minería consistentes en múltiples tarjetas gráficas unidas a una misma placa base mediante extensores PCIe, y los fabricantes de placas base han estado aprovechando el boom de Ethereum para sacar modelos específicos para equipos de minería*" (Baños, s.f.). Sin perjuicio de lo anterior, los mineros cada vez más diversifican sus capacidades de procesamiento, con el fin de contar con mayores recursos en su reto por alcanzar nuevos registros de criptomonedas.

En este contexto, con una alta densidad digital cada vez más evidente y mayor conectividad de objetivos físicos con características inteligentes, se advierte una acción proclive de los mineros sobre dispositivos de internet de las cosas, que si bien son pequeños y con limitadas capacidades, es viable construir un *grid* de computación amplio y denso de tal forma que se puedan tener "*granjas de minería*" en segundo plano trabajando en la generación de criptomonedas nuevas o más maduras, como apoyo a otras estrategias ya consolidadas con servidores y equipos de computación caseros capturados mediante engaños a muchas personas.

Este nueva propuesta criptominera tiene la ventaja de poder utilizar capacidad de procesamiento posiblemente imperceptible para los dueños de los dispositivos, habida cuenta que no se cuenta con una práctica regular de medición y seguimiento de las capacidades de estos dispositivos de internet de la cosas, creando un escenario propicio para "robar" procesamiento de bajo perfil de forma no autorizada.

2. Engaños basados en terceros de confianza (Cadena de suministro y actualizaciones de firmware)

Con la transformación digital como fundamento de la propuesta de valor de muchas organizaciones a nivel global, los terceros de confianza se convierten en los aliados estratégicos de muchas de ellas, como base de la configuración y despliegue de soluciones y propuestas innovadoras para sorprender a sus clientes. En este ejercicio, tanto las empresas como los terceros despliegan productos y servicios digitalmente modificados, que por lo general se basan en los fundamentos de las metodologías ágiles, para lograr el efecto deseado de forma efectiva y en tiempos de mercado.

En este contexto, las empresas delegan y confían en sus terceros muchos de los aspectos de seguridad y control, dejando una brecha de monitorización y verificación en el proceso, comoquiera que éstos pueden o no estar certificados y/o cuenten con reportes internacionales que validan sus buenas prácticas al interior de sus procesos y productos. No obstante lo anterior, los adversarios sabiendo que la aplicación de los estándares y buenas prácticas pueden generar cegueras cognitivas y crear una zona de confort para estos

actores, configuran nuevos vectores de ataque que cambian la ecuación de riesgos de la empresa y sus aliados estratégicos aumentando la probabilidad de un incidentes no identificado.

Dichos incidentes, generalmente basados en la confianza y reconocimiento mutuo de los implicados, crea engaños que pueden pasar por actualizaciones de microcódigo en sistemas de control industrial, descarga de aplicaciones actualizadas o ajustes en configuraciones en puntos críticos de conexión entre la infraestructura del tercero y la empresa, de tal forma, que bajo la apariencia de comunicaciones y conexiones confiables (Darkreading, 2019), es posibles crear un evento no deseado que surge por la falta de ejercicios de novedad o inestabilidad, que permita mantener atenta a las partes sobre nuevas tensiones que se crean los posibles adversarios.

Si bien esta tendencia no es nueva, si es consistente con los eventos que se han venido presentando a lo largo del año y que si no se cambian las prácticas vigentes, continuará desarrollándose y avanzando en los procesos cada vez más automatizados y menos monitoreados, particularmente en sectores como el industrial y manufactura, el de la salud y posiblemente el de tecnología dado el incremento de empresas emergentes que buscan desarrollar ecosistemas digitales con aplicaciones y productos de apropiación rápida y expansión viral.

3. Uso adversarial de la inteligencia artificial

La inteligencia artificial como fenómeno tecnológico que ha salido de los laboratorios para convertirse en un producto comercial, da cuenta de una realidad de transformación acelerada de cambios y actividades que antes tomaban tiempo para realizarse. Este ejercicio de automatización e inteligencia basada en el poder de los algoritmos que aprenden tanto de manera supervisada como no supervisada, establece una nueva frontera para crear apuestas particulares en diferentes campos y dominios de la ciencia.

El uso positivo de las capacidades de la inteligencia artificial pasa por diagnósticos médicos, sistemas de detección de intrusos avanzadas, propuestas de pronósticos de eventos en sistemas financieros, entre otras aplicaciones. No se escapan los teléfonos inteligentes, ahora con asistentes basados en este tipo de inteligencia, que atienden las dinámicas de las personas, programan citas y recuerdan aspectos propios de la vida personal y profesional. Los algoritmos de inteligencia artificial están en medio de la dinámica de la sociedad actual, los cuales bien utilizados, se convierten en poderosas herramientas para avanzar y correlacionar eventos de formas novedosas.

Cuando el atacante hace uso de esta misma tecnología y la usa para adelantar sus acciones contrarias, estamos en un campo donde el incierto, el engaño y la premeditación se hacen presentes. Es un ejercicio donde el atacante puede crear contexto de distracción y acciones evasivas que pueden engañar las prácticas actuales de los sistemas más avanzados de detección y análisis. Esto supone aspectos como malware construido para autogenerarse y reconfigurarse, código inteligente que se reescribe a sí mismo en entornos controlados, engaños a otros algoritmos de detección, guerras de información asimétrica, manipulación de tendencias y mercados, entre otras acciones que revelan un campo inestable donde no tenemos reglas concretas para jugar o desafiar (Li, Zhao, Cai, Yu & Leung, 2018).

Avanzar frente a esta nueva amenaza implica desarrollar el concepto de contrainteligencia cognitiva, que adaptando la definición de Jiménez (2019) sobre contrainteligencia, definimos podemos definir como "*el conjunto de actividades que tiene como finalidad localizar, identificar y monitorizar, para neutralizar y, en su caso, contrarrestar y reportar, las actividades no autorizadas de los algoritmos de aprendizaje automático, es decir, aquellas que rompen con las reglas inicial-*

mente establecidas y materializan los riesgos inherentes al desarrollo y puesta en operación de los algoritmos de inteligencia artificial».

4. Compromiso de la integridad de la información

De las características de la información que hoy está más expuesta es la integridad. La confidencialidad y la disponibilidad, si bien igualmente son relevantes, se hace evidente en la actualidad revisar dos atributos más propuestos por Parker (1998) como son la utilidad y la posesión, los cuales son convergentes con la esencia de la integridad. Bajo esta perspectiva, una información es íntegra si en todo su ciclo de vida no ha sido alterada o deteriorada, y si fuese el caso, se tiene registro y trazabilidad de dicha condición.

La *utilidad* definida como el "uso de la información para un propósito" y la *posesión* como "la tenencia o titularidad, el control y la capacidad de utilizar la información" (Parker, 1998, p.240) se vuelven relevantes a la hora de comprender las tendencias actuales donde la manipulación de la información se convierte en un arma estratégica para posicionar un producto o servicios, o un vector de ataque que busca confundir, crear un engaño o facilitar el posicionamiento de intereses de actores con intenciones poco confiables.

Cuando se entiende la degradación o deterioro de la información como estrategia para limitar su utilidad y habilitar usos distintos a los inicialmente establecidos, así como motivar un cambio de titularidad de la misma a un tercero mediante engaños o suplantaciones, con el fin de adelantar acciones no autorizadas a nombre de un intruso, es posible advertir tendencias que afectan la identidad, la veracidad y el control de los imaginarios de las personas en un contexto particular. Cambiar la esencia de la información con fines no conocidos es una realidad que exige más que controles de acceso para poder protegerla y asegurarla.

Parker (1998) de forma visionaria estableció que revelar información sobre un propietario de forma inadvertida, en medios abiertos o sin controles, establece un campo de acción para un adversario donde cualquier uso o utilidad se puede concretar, creando un escenario de negligencia y gestión que se devuelve a su dueño. En consecuencia, perder posesión de la información, no es sólo el acceso a la misma, sino en brindarla a terceros de forma no intencional o inadvertida con la cual se crea conocimiento o se construye nuevas versiones de la misma que están más allá de los propósitos iniciales y legítimos que se tenían.

Enfrentar este desafío, implica pasar del control de acceso al control de uso, donde se hace necesario desarrollos los atributos de posesión y utilidad propuestos hace más de dos décadas, con el fin de fortalecer no solamente la integridad, sino la confidencialidad y la disponibilidad ahora con un propósito y fines superiores y sensibles cuando puede ser utilizada y controlada fuera de un espacio de comprensión y conocimiento autorizado.

5. Redes 5G: hiperconectados y ultravulnerables

El advenimiento de las ciudades inteligentes, la conexión masiva de objetos físicos y la necesidad de pobladores hiperconectados, configura un escenario de alto flujo de información, de infraestructuras basadas en terceros y agilidad en la transmisión de los datos con el fin de concretar la visión de una realidad aumentada, informada y en tiempo real para los moradores de esas ciudades. Por tanto, la aparición de las redes 5G es la respuesta tecnológica que se requiere para cumplir con la promesa de ese entorno hiperconectado, con baja latencia de interacción entre los móviles, la nube y los objetos, y sobremanera, de agilidad y eficiencia en los servicios dispuestos en estas ciudades.

La redes 5G se configuran como la pieza clave del rompecabezas para potenciar servicios y productos en diferentes industrias para

potenciar las capacidades y oportunidades de las personas para acceder a espacios de interacción inexistentes con vehículos autónomos, cirugías asistidas por brazos mecánicos a distancia, sistemas industriales robotizados, sistemas de emergencias conectados y masivos, entre otras actividades. De esta forma, estas nuevas redes potenciarán el desarrollo de una economía digital, donde los bienes intangibles y el internet de las cosas serán parte natural de esta nueva dinámica.

A la fecha cinco son las empresas que están a la vanguardia de esta nueva tecnología: Nokia, Ericsson, Samsung, Huawei y ZTE, la dos últimas representan intereses chinos, con lo cual se crean tensiones geopolíticas, donde "*la posibilidad de que los fabricantes chinos introduzcan en sus productos dispositivos que permitan el envío de información de forma encubierta o que, sencillamente, puedan escapar al control del operador de esos equipos poniendo en peligro la seguridad, integridad o confidencialidad de los sistemas*" (Moret, 2019) de las empresas y las naciones.

Considerando que la infraestructura de las redes 5G configura un ecosistema de ecosistemas, dado que se virtualizan las infraestructuras de redes y se transforman en software de gestión y transmisión, que disminuyen la latencia, reducen un 90% el consumo de energía de la red, ofrecen un tasa de datos de hasta 10Gbs (Gemalto, 2019), entre otras características, se funda un escenario emergente de amenazas dado las limitadas opciones de seguridad y control consideradas en el diseño y desarrollo de esta tecnología.

Un reciente estudio del Instituto Brookings (Wheeler & Simpson, 2019) establece cinco razones por las cuales las redes 5G serán más vulnerables a ciberataques que sus predecesoras. Las razones son:

- La red se ha alejado de la conmutación centralizada basada en hardware y ha pasado a un enrutamiento digital distribuido y definido por software.
- Virtualización en software de funciones de red de alto nivel que anteriormente realizaban los dispositivos físicos.
- Gestión de la red basada en software.
- Expansión del ancho banda de forma dinámica.
- Conexión de miles de millones de dispositivos IoT.

Dado este entorno de software sobre una red distribuida, proclive a los ataques, las organizaciones y naciones deben tomar sus precauciones y acciones concretas para avanzar en una estrategia de protección proactiva en el despliegue de los sistemas socio-técnicos sobre este nuevo ecosistema: infraestructura, aplicaciones y servicios. Surge un deber cibernético de cuidado de todos lo participantes para compartir y asegurar la dinámica de este entorno que aún está por conocerse y descubrirse.

Reflexiones finales

Entender estas cinco tendencias revisadas previamente es reconocer que es necesario superar el enfoque de control y cumplimiento vigente en las empresas, para movilizar a las organizaciones y naciones hacia estrategias accionables que las configuren como corporaciones y naciones resilientes, donde se privilegian las relaciones con el entorno y la generación de valor para sus clientes y ciudadanos (Deloitte, 2018).

La nueva generación de disrupciones tecnológicas creará nuevos entornos desafiantes para los cuales no se puede estar preparados. Por tanto, es clave que las naciones y empresas emprendan con frecuencia un viaje al futuro desde las simulaciones y la experimentación, con el fin de exponer las inestabilidades e inciertos que se pueden presentar con el fin de encontrar patrones y tendencias sobre las cuales poder trabajar de forma previa y aprender de ellas.

Los cinco pronósticos detallados en este breve reporte son una reflexión limitada de

un entorno cada vez más volátil e inestable, que busca comprender posibles vectores de ataques y contextos en los cuales los adversarios pueden tomar ventaja para incrementar la incertidumbre en las variables de gestión de riesgo de los analistas organizacionales.

En consecuencia, la invitación es a construir y actualizar de forma permanente el mapa de amenazas digitales del entorno actual, sobre un territorio que cambia de forma dinámica y muchas veces rizomática creando zonas grises y ocultas, propias de las cegueras cognitivas, para tensionar y desconectar aquello conocido y así, intentar descubrir los patrones y retos de los adversarios.

Referencias

Baños, D. (s.f.). ¿Qué es la criptominería? *Revista Muy Interesante*. Recuperado de: https://www.muyinteresante.es/tecnologia/articulo/que-es-la-criptomineria

Darkreading (2019). Firmware Vulnerabilities Show Supply Chain Risks. Darkreading. Recuperado de: https://www.darkreading.com/vulnerabilities—threats/firmware-vulnerabilities-show-supply-chain-risks/d/d-id/1335313

Deloitte (2018) Auditing the risks of disruptive technologies. Internal Audit in the age of digitalization. *Report*. Recuperado de: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-auditing-the-risks-of-disruptive-technologies.pdf

Gemalto (2019). Red 5G – Características y usos de esta tecnología. Recuperado de: https://www.gemalto.com/latam/telecom/inspiracion/5g

Jiménez, F. (2019). *Manual de inteligencia y contrainteligencia*. Sevilla, España. CISDE

Li, P., Zhao, W., Cai, W., Yu, S. & Leung, V. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. *IEEE Access*. 6, 12103-12117. Doi: 10.1109/ACCESS.2018.2805680

Maxwell, J. (2019). ROX is the new ROI: Prioritizing customer experience. *Strategy + Business*. Recuperado de: https://www.strategy-business.com/blog/ROX-Is-the-New-ROI-Prioritizing-Customer-Experience

Moret, V. (2019). El despliegue de las redes 5G, o la geopolítica digital. *Real Instituto Elcano*. Recuperado de: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari31-2019-moret-despliegue-de-redes-5g-geopolitica-digital

Parker, D. (1998). *Fighting computer crime: a new framework for protecting information*. New York, USA: John Wiley & Sons.

Wheeler, T. & Simpson, D. (2019). Why 5G requires new approaches to cybersecurity. Racing to protect the most important network of the 21st century. *Report*. Brookings Institute. Recuperado de: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

Jeimy J. Cano M., Ph.D, CFE

Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes, Colombia. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Administración de Negocio por Newport University, CA. USA. y Ph.D en Educación (Ed.D) por la Universidad Santo Tomás, Colombia. Cuenta con más de 20 años de experiencia como académico, profesional y ejecutivo en temas de seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y Auditoría de TI. En 2016 recibió el reconocimiento como "Cybersecurity Educator of the Year 2016" para Latinoamérica por el Cybersecurity Excellence Awards. Es examinador certificado de fraude (CFE en inglés). Cuenta con más de 150 publicaciones en revistas y eventos internacionales, así como conferencista invitado a foros y conferencias nacionales e internacionales en temas de seguridad y control en Latinoamérica. Profesor Asociado de la Escuela de Administración de la Universidad del Rosario en Colombia. Profesor Distinguido de la Facultad de Derecho de la Universidad de los Andes en Colombia. Director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas. http://insecurityit.blogspot.com

Mejora del proceso de respuesta frente a incidentes de ciberseguridad aplicando algoritmos de aprendizaje automático

Gastón Rial, Miguel Pérez del Castillo, Rafael Sotelo, Máximo Gurméndez – Universidad de Montevideo

Resumen

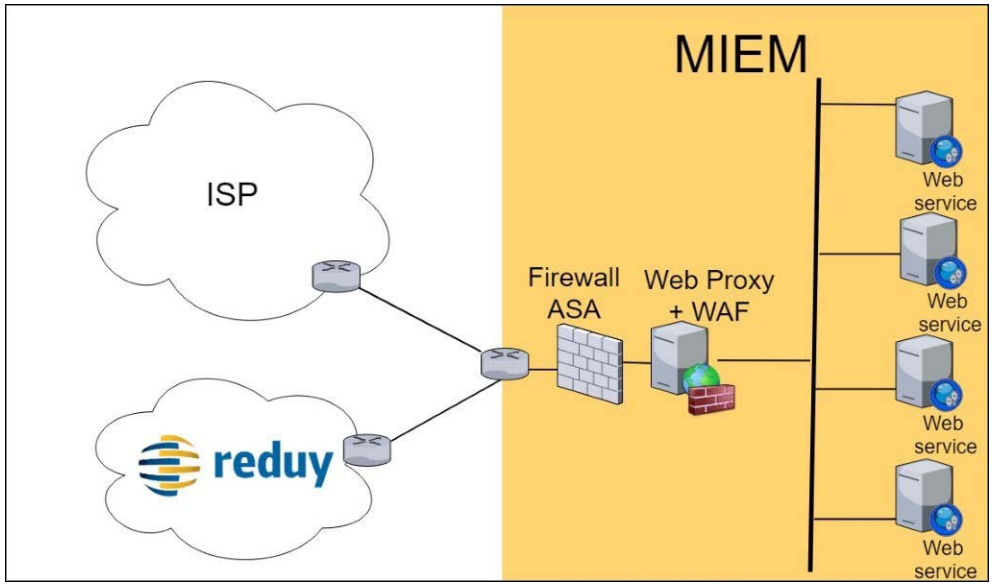
El presente artículo describe un proyecto de colaboración entre AGESIC y la Universidad de Montevideo en el que se abordó mejorar el proceso de respuesta frente a incidentes de ciberseguridad aplicando algoritmos de aprendizaje automático.

En la última década, la informatización de los procesos en el ámbito empresarial, industrial y científico, junto con el acelerado crecimiento en el número de usuarios de Internet, producto de avances tecnológicos en los medios de acceso y la introducción de nueva y más veloz infraestructura de telecomunicaciones, ha dejado expuestos a los gobiernos del mundo, que se encuentran a merced de las amenazas del cibercrimen y el espionaje, tanto por agentes dentro como fuera del Estado.

Una de las principales responsabilidades de AGESIC, como unidad ejecutora dependiente de Presidencia de la República, es encabezar la estrategia e implementación del Gobierno Electrónico de Uruguay y la Sociedad de la Información y del Conocimiento.

Para ello cuenta con el CERTuy y el SOC, centros dependientes de AGESIC. El primero está conformado por un grupo de expertos en medidas preventivas y reactivas ante incidencias de seguridad en los sistemas informáticos, mientras que el segundo se compone de analistas en seguridad para efectuar un monitoreo constante de la actividad registrada en REDuy (red de alta velocidad que reúne la información de los entes estatales). Entre otros objetivos, centralizan y coordinan los procesos de respuesta a incidentes que comprometan la seguridad de la información.

Se decidió investigar la aplicabilidad y el desarrollo de herramientas basadas en aprendizaje automático o Machine Learning (ML, por sus siglas en inglés), el cual consiste en el proceso automatizado de extracción de patrones de los datos, para asistir en las labores de los forenses de las organizaciones mencionadas. Focalizando el trabajo en los logs de acceso a servidores web que son registrados en REDuy, se estudió el comportamiento de los usuarios en el tiempo, y, en especial, el desarrollo de modelos predictivos que cla-

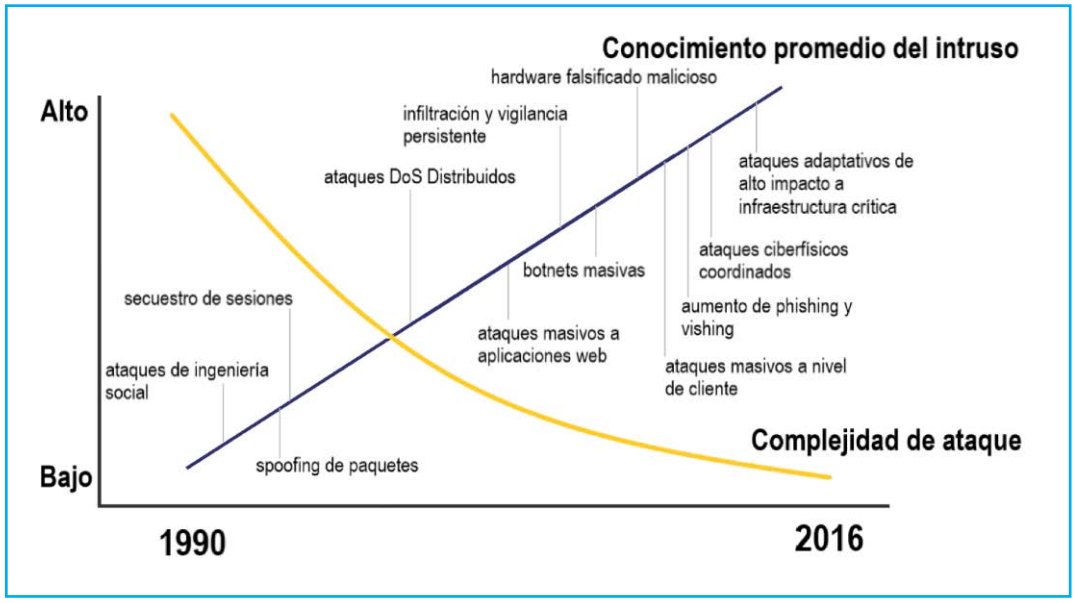


Ejemplo de Topología de RedUy

sifiquen la actividad de estos, de modo de simplificar la búsqueda de los denominados APT (Advanced Persistent Threat).

Parte de la motivación del proyecto surgió de la posibilidad de realizar un aporte a la seguridad de la información de la ciudadanía, la cual se ve amenazada por ataques cada vez más frecuentes y de mayor impacto. La gráfica que se ve a continuación demuestra cómo, con el tiempo, los ataques a sistemas informáticos van aumentando gracias a que las herramientas para perpetuarlos se hacen más comunes y fáciles de utilizar.

Las siguientes páginas resumen el trabajo llevado a cabo y los principales resultados alcanzados durante el desarrollo del proyecto.



Promedio entre conocimiento del intruso y sofisticación del ataque (fuente CMU - CERT)

Introducción

Los trabajos del proyecto tuvieron como principal objetivo el estudio de la mejora en el proceso de análisis de logs históricos de computadoras y redes por parte del equipo de respuesta de AGESIC (CERTuy) y centro de operaciones en seguridad (SOC) frente a incidentes aplicando herramientas de aprendizaje automático. Para lograrlo, se dispuso de un dataset (conjunto de datos) representativo de las trazas investigadas por expertos de este equipo. Siguiendo los lineamientos del marco CRISP-DM (Cross Industry Standard Process for Data Mining, por sus siglas en inglés), este fue sanitizado y preparado para las tareas de entrenamiento y evaluación de los modelos inducidos por medio de diversos algoritmos de aprendizaje automático.

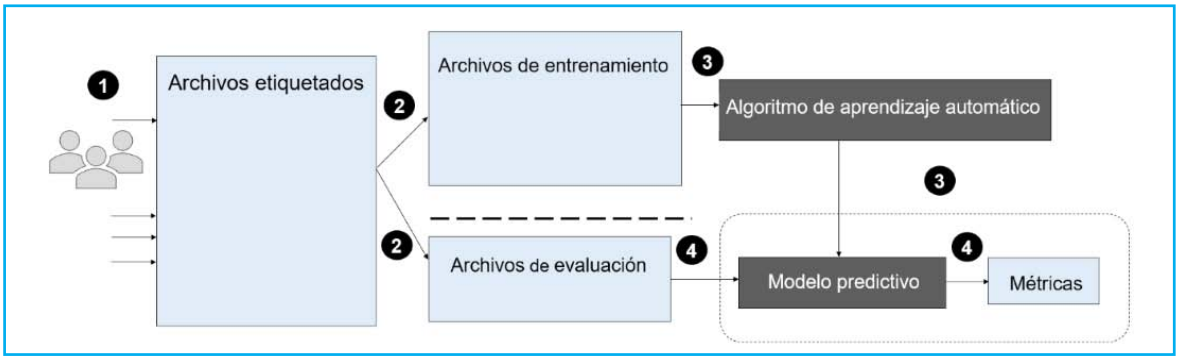
Diagrama de las etapas que comprenden CRISP-DM

Las técnicas o tipos de aprendizaje se pueden clasificar en aprendizaje supervisado, no supervisado, semi-supervisado y reforzado. De ellas, la investigación se centró en el primer grupo, pues han demostrado ser útiles en tareas de clasificación donde el dataset se encuentra etiquetado. Para comprender mejor la información con la que se trabajó, se tomaron muestras de los datos entregados por parte de CERTuy para ser etiquetadas manualmente en trazas de actividad normales y anormales.

El proyecto dio lugar al desarrollo de herramientas basadas en aprendizaje automático para asistir en las labores de los forenses de la mencionada organización. Estas operan sobre trazas de actividad de usuarios web, las cuales deben ser clasificadas como normales o anormales (con cierta probabilidad), mediante el uso de un modelo predictivo. Una traza de actividad se define como el conjunto de líneas de logs de acceso a servidores web de REDuy asociadas a un origen (identificado por su IP) en un intervalo de tiempo dado.

Evaluación de la aplicación de ML

Para determinar el éxito de las herramientas desarrolladas, se propuso medir su desempeño en dos aspectos fundamentales para la labor del forense: volumen de datos asociados al comportamiento sospechoso de usuarios en los servidores web y el tiempo que tarda la herramienta en procesar cierto tamaño de logs. La siguiente tabla (tabla 1.



Proceso de aprendizaje supervisado

Dimensión observada	Umbral
Reducción de tamaño	Mayor al 25% del total actual
Tiempo de procesamiento	Inferior al 10% de lo que tarda un analista

Tabla 1.- Valores Objetivo

Valores Objetivo), resalta cuáles fueron los indicadores que se fijaron para determinar la utilidad de la herramienta.

A partir de encuestas realizadas al equipo de CERTuy, se determinó que, ante la eventualidad de un incidente de seguridad, el tiempo que tarda un forense experto en analizar los logs con herramientas de visualización de datos es aproximadamente 50 fhoras en promedio y el tamaño de los logs observado durante ese período no supera los 7GB. Tomando en cuenta que la mayor parte del tiempo se invierte en el estudio de logs asociados a la actividad normal de los usuarios y no potenciales amenazas, se buscó hacer sus tareas más rápidas y eficientes por medio de las herramientas desarrolladas.

Indicadores de desempeño de los modelos

Para medir el desempeño del modelo predictivo en el ambiente de producción se utilizaron tres métricas: Precisión, Recall y F Measure o F1 Score (Ver fórmulas matemáticas a continuación).

La *Precisión* se corresponde a la proporción de flujos o trazas de actividad etiquetados como sospechosos que efectivamente estaban vinculados a tráfico anormal respecto del total de trazas clasificadas como tráfico sospechoso. Mientras, se denomina Recall a la proporción de flujos o trazas de actividad etiquetada correctamente como anormales respecto al total que realmente están vinculados a tráfico de este tipo.

Por otra parte, el índice F1 Score es una media que combina las anteriores. Es decir, es la media armónica entre Precisión y Recall. A pesar de revestir importancia a la hora de evaluar cuan efectivo fue el modelo en pruebas, es utilizado para comparar entre diferentes algoritmos cuál se adapta mejor al caso de uso.

Aparte de estas medias, con la tasa de verdaderos positivos (TPR) o sensibilidad y la tasa de falsos positivos (FPR) o complemento de la especificidad (1-especificidad), se logra calcular el índice ROC (Receiver Operating Characteristic) o AUC (área debajo de la curva, por sus siglas en inglés) de la curva ROC. A

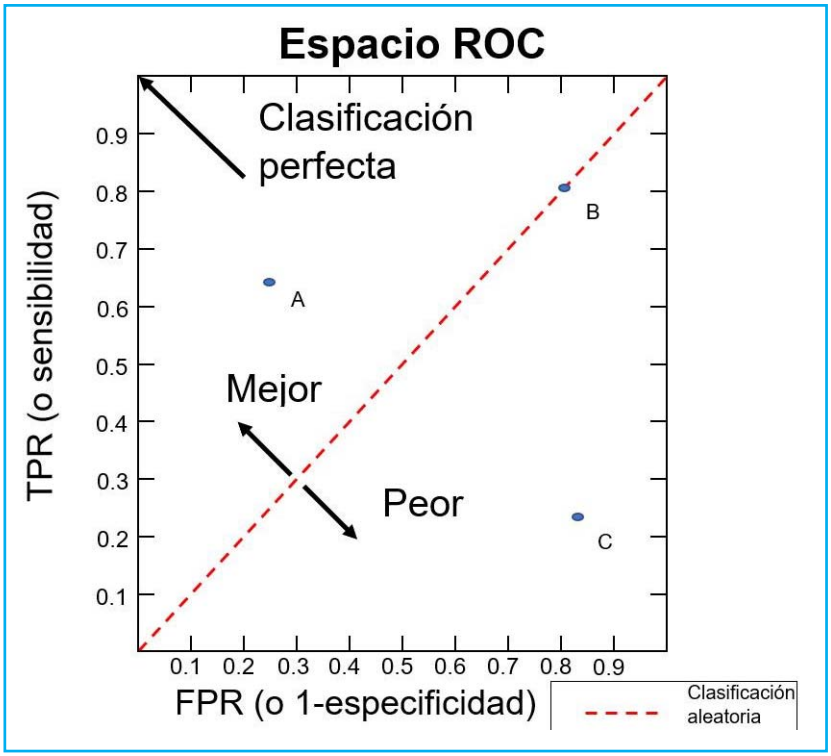
$$\textbf{Recall} = \frac{Verdaderos\ Positivos}{Verdaderos\ Positivos + Falsos\ Negativos}$$

$$\textbf{Precision} = \frac{Verdaderos\ Positivos}{Verdaderos\ Positivos + Falsos\ Positivos}$$

Fórmulas de precisión y recall

$$\mathbf{F_1} = \left(\frac{recall^{-1} + precision^{-1}}{2} \right)^{-1} = 2 \times \frac{recall \times precision}{recall + precison}$$

Fórmulas de F1 Score



Ejemplo de espacio de ROC

continuación, se muestra una figura de ejemplo donde se puede ver que, cuando el índice se mueve más hacia la esquina superior izquierda, el clasificador es más exacto en sus predicciones. El AUC, que toma un valor entre 0 y 1 (incluidos los extremos), es el área de la curva dentro de este espacio. La línea roja y los puntos sobre ella, como lo es "B", muestra un clasificador que no es mejor en su predicción que una elección al azar, pues la tasa de aciertos (o verdaderos positivos) iguala a la de fallos (falsos positivos).

Evaluación de los algoritmos de aprendizaje automático

A continuación, se exhiben los resultados para 1000, 1500 y 2000 muestras o trazas de actividad usadas para el entrenamiento del modelo. En el gráfico de barras, se muestran los resultados del cálculo de área bajo la curva (AUC, por sus siglas en inglés)

ROC (Receiver Operating Characteristic) al aplicar cada uno de los algoritmos de aprendizaje automáticos seleccionados.

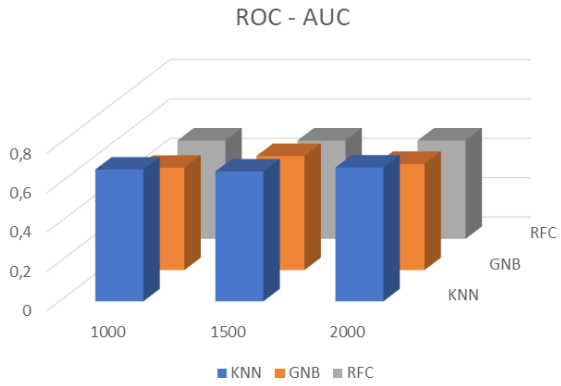


Gráfico de barras del AUC para los algoritmos RFC, GNB y KNN

Del análisis anterior, se puede apreciar que el modelo con peor desempeño fue aquel aprendido con RFC (Random Forest Classifier), ya que el aumento en el número de muestras no implicó una mejora en su funcionamiento.

Por otra parte, el modelo que mejor se adecuó a la tarea fue el inducido mediante K-NN ponderado (K- Nearest Neighbours). Es posible notar una mejora en el desempeño a me-

dida que aumenta en número de ejemplos o puntos de datos usados en el entrenamiento. Este comportamiento era esperable, de acuerdo con la descripción del algoritmo.

Finalmente, Naive Bayes supera a RFC, pero no alcanza los valores de desempeño que logra K-NN. Además, es posible notar que su funcionamiento es óptimo al ser entrenado con 1500 muestras, o algún número entre 1000 y 2000 ejemplos. Puesto que la implementación del servicio de clasificación trabaja por lotes (o batches) de trazas, este valor se elige como cantidad máxima a procesar por iteración.

Arquitectura del sistema de clasificación

Los primeros tres meses del proyecto trataron con los puntos del cronograma correspondientes al marco teórico, la preparación del ambiente de desarrollo (dentro y fuera de las oficinas del CERTuy) y la construcción y presentación de las pruebas de concepto en AGESIC. Una de las tareas necesarias, previa al desarrollo de un sistema es diseñar su arquitectura, es decir, cuáles son los componentes dentro del clasificador, sus responsabilidades, dependencias e interfaces que estos exponen para permitir la interacción entre componentes.

En la etapa de diseño, se priorizó que fuese sencillo modificar el servicio de clasificación de trazas de actividad. Para ello se organizó el sistema en módulos. Cada módulo realiza una tarea específica y es usado y modificado independientemente de los demás. Esa organización de responsabilidades permitió que corregir o mejorar un módulo, no implicara modificar los demás.

Manteniendo la arquitectura modular, producto de las reuniones mantenidas juntos con los tutores y el equipo de CERTuy, se elaboró el diseño cuyo funcionamiento se explica en los siguientes párrafos.

La idea detrás del funcionamiento del clasificador es la siguiente, cuando el sistema, con su modelo ya entrenado, es usado para predecir sobre archivos de log, el módulo correspondiente al controlador/monitor primero invoca al preparador de datos, que los deja en un formato interpretable por el codificador, agrupando las líneas de logs en trazas de actividad de un mismo usuario para un período de tiempo dado, por ejemplo, un día, en archivos de texto separados. Esencialmente, el preparador de datos limpia los datos de entrada y forma la denominada Analytical Base Table (ABT), es decir, una tabla con campos predeterminados, donde cada fila representa una instancia de datos (en nuestro caso, una traza de actividad) y cada columna un atributo de ellos.

Luego el codificador efectúa una transformación de las instancias de datos por medio

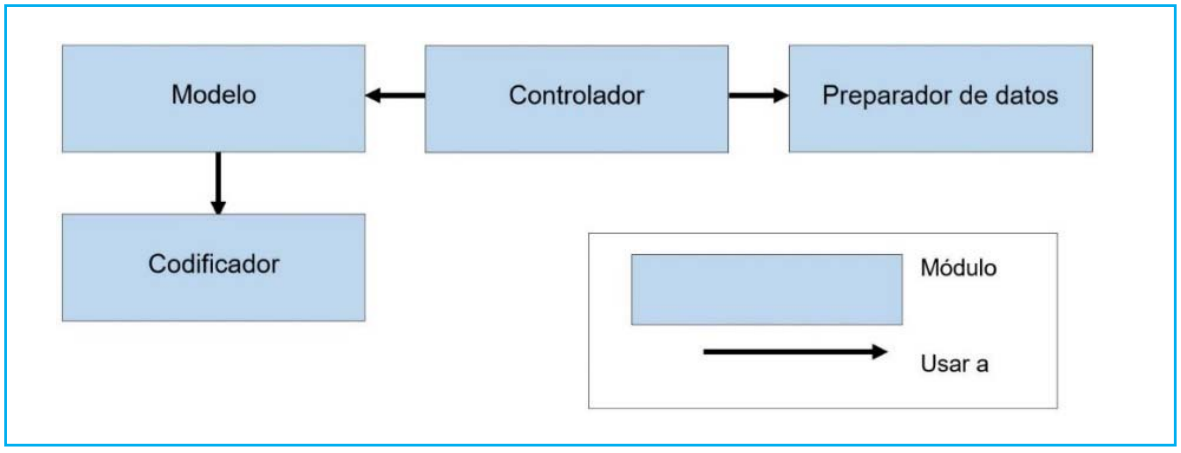


Diagrama de bloques del sistema final

de lo que se conoce como "Word embedding". Esta técnica consiste en realizar un mapeo de las palabras de los logs a vectores de reales mediante el uso de un modelo del lenguaje, el cual, en la implementación del proyecto, fue previamente aprendido con la ayuda de la herramienta de Google "Word2vec". Explotando las relaciones de similitud entre vectores asociados a palabras que suceden en un contexto similar, es posible comprimir la información de los logs dentro de una traza de actividad a un único vector perteneciente a un espacio vectorial en , el cuál sirve de entrada al modelo predictivo.

Finalmente, el controlador inicializa el módulo asociado al modelo predictivo. Para que este prediga sobre la entrada, se carga los parámetros aprendidos del entrenamiento supervisado, con trazas previamente etiquetadas y los hyperparámetros ajustados por medio de varios experimentos o pruebas. La salida o predicción separ a las trazas cuya probabilidad de estar asociadas a actividad anormal supera una probabilidad del 50% del resto.

Integración al SIEM

Una vez alcanzados los objetivos iniciales, como tarea adicional se decidió utilizar el clasificador para contribuir al flujo de trabajo del SOC, aportando valor a la gestión de eventos de seguridad. Sus tareas de monitoreo se basan en el uso de un SIEM (sistema de gestión de información y eventos de seguridad) que centraliza los datos crudos provenientes de diversos sensores en REDuy, por ejemplo, WAFs, UTMs, proxies y varios dispositivos de red, y emplea un motor o "procesador de eventos" que usa reglas estáticas para determinar cuándo puede surgir una ofensa o incidente.

Por lo tanto, se optó por construir un cliente syslog, que actúe como fuente de logs o sensor adicional. De esta forma, se pretende que la aplicación envíe un mensaje por cada traza de actividad, etiquetada por el servicio clasificador, como anormal. Este mensaje, que se encuentra implementado en formato JSON (JavaScript Object Notation), a la vez es identificado por el SIEM como un evento a ser procesado por el CRE (Custom Rules Engine) del "procesador de eventos", indicándole que genere la correspondiente ofensa.

Evaluación del servicio de clasificación

Asumiendo, que se conoce de antemano la cantidad de falsos positivos, falsos negativos, verdaderos positivos y verdaderos negativos (los valores de la matriz de confusión) es posible ser específico en la medición real de este resultado. En base a las pruebas de evaluación, el clasificador se ejecutó con **150 trazas** (Archivos de logs de 500 MB). Según la matriz de confusión, de esas, **120** se clasificaron como verdaderas negativas (trazas clasificadas como normales que efectivamente contenían actividad normal). Por tanto, la **reducción en volumen de logs normales fue de 80%**.

Este valor supera las expectativas del equipo sobre la reducción de volumen, debido a que por lo menos se debía reducir el 25%. Se debe tomar en cuenta que estos valores solamente aplican al contexto (sensor WAF asociado al log de acceso e intervalo temporal) en el que se entrenó y probó al modelo predictivo.

En cuanto a pruebas realizadas, sin conocer la matriz de confusión, sobre el mismo volumen de logs, al medir el tamaño de la salida anormal (datos destinados al análisis forense) respecto al tamaño total de entrada, se encontró una **reducción del 97,5% de trazas vinculadas a actividad normal**.

Por otra parte, para evaluar el factor temporal, se consideró la cantidad de horas que se tarda en procesar un volumen de 1 gigabyte de logs. Recordando que se tardan 50 horas en trabajar sobre un conjunto de logs de 7GB, tomando en cuenta que el volumen de los logs de acceso representa aproximadamente el 30% respecto al total de logs registrados

por la RedUY, se asume que se tardan 15 horas en detectar 2 GB de logs anormales considerando solo los logs de acceso. Por tanto, un analista tardaría 7 horas por gigabyte. El clasificador demora en procesar 450 MB en 15 minutos, por lo que tarda 30 minutos en clasificar 1 gigabyte. Respecto la detección por un analista**, esto implica que el tiempo se reduciría en un 92% del total de horas** que se tarda en abarcar todos los logs relevantes.

Además de las medidas realizadas en los experimentos, se llevaron a cabo pruebas de campo con el personal de CERTuy. Ellos respondieron a una encuesta de satisfacción dando lugar a los siguientes comentarios:

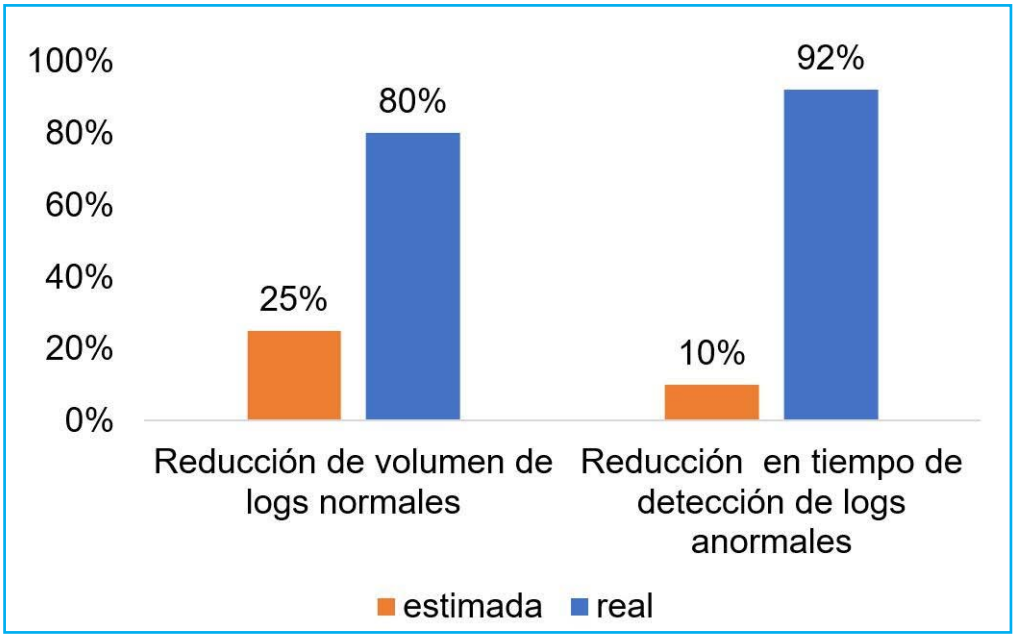
- Genéricos: "detecta correctamente la actividad anómala y casos poco frecuentes", "La herramienta está buena", "está muy bien que se estructuren los logs en archivos y permita ver toda la actividad de una IP", "agregar el atributo de país es muy útil",
- Velocidad:" anda rapidísimo"," comparada con otras herramientas anda muy rápido", "anda super rápido"

Todos los entrevistados tuvieron mucho interés en entender cómo funcionaba internamente el sistema, principalmente lo relacionado al módulo que emplea el modelo predictivo. También, se interesaron por saber cuáles son los criterios que infiere el algoritmo, a partir de los datos de entrenamiento, y si es posible conocer o modificar las variables internas de decisión que utiliza el modelo, además de los hiperparámetros.

Conclusiones

La experiencia realizada fue calificada como exitosa, tanto por el equipo de la Universidad de Montevideo como por el de AGESIC. Se logró cumplir con los objetivos del proyecto y aprender cómo se pueden aplicar algoritmos de aprendizaje automático para la resolución de problemas asociados a la ciberseguridad.

Entre los puntos a destacar, se menciona que inicialmente, la infraestructura de operaciones que se manejaban (previo al comienzo del proyecto) no se encontraba diseñada para la integración de servicios adicionales. Por lo tanto, se tuvo que trabajar en conjunto entre ambas instituciones para configurar el ambiente de trabajo in-situ, en Torre Ejecutiva. Además, de las diversas reuniones mantenidas con los integrantes de los distintos equi-



Histograma de resultados finales respecto criterios especificados

pos, poco a poco se fueron obteniendo privilegios de acceso a más información que permitió mejorar el funcionamiento del clasificador. A modo de ejemplo, originalmente, el sistema trabajaba con las direcciones IP de origen ofuscadas empleando el digesto de una función de hash. Posteriormente, eso cambió, dejando la IP descubierta, y se pudo derivar, mediante el uso de una base de datos local a la herramienta, el país de origen de las peticiones. Este campo adicional mejoró la forma en la que se efectuó el etiquetado de entrenamiento y los resultados provistos por el clasificador.

Todavía restan tareas por hacer para que el servicio entregado se encuentre completamente operativo, como, por ejemplo, establecer un equipo de trabajo encargado de analizar su salida y el entrenamiento periódico del modelo predictivo requerido para mantener niveles aceptables de precisión a lo largo del tiempo. Por ello, se deja abierta la posibilidad de continuar con el proyecto en un futuro.

Referencias

KELLEHER, John. Fundamentals of machine learning for predictive data analytics: algorithms, worked examples, and case studies. 1a edición. Cambridge, Massachusetts: MIT Press, 2015. 624p. ISBN: 978-0262029445.

BUCZAK, Anna. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials. Vol. 18 Ent. 2. 2016. 1162-1165p. Disponible en: https://ieeexplore.ieee.org/document/7307098 ISSN: 1553-877X

BERTERO, Christophe. Experience Report: Log Mining using Natural Language Processing and Application to Anomaly Detection. 28th International Symposium on Software Reliability Engineering (ISSRE). 2017. 351-360p.

SPRING, Jonathan M., et al. Machine Learning in Cybersecurity: A Guide. CMU/SEI-2019-TR-005.

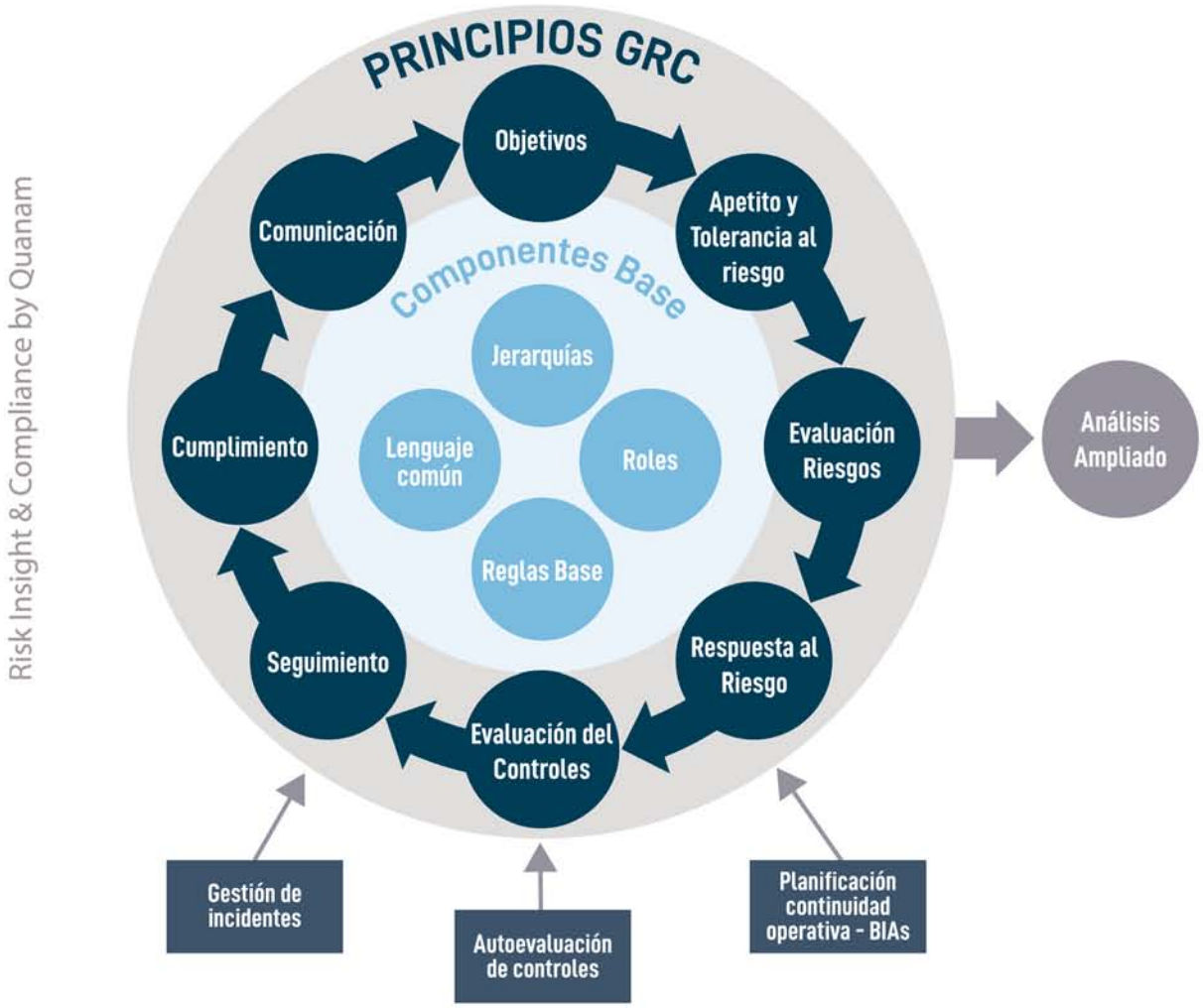
TANKARD, Colin. Advanced persistent threats and how to monitor and deter them. Network security, 2011. 16-19p. Disponible vía Timbó en : https://www.sciencedirect.com DOI: 10.1016/S1353-4858(11)70086-1

SKOUDIS, Edward. Counter hack reloaded: a step-by-step guide to computer attacks and effective defenses. Second edition. Stoughton, Massachusetts, EEUU: Prentice Hall Press, 2005. ISBN 0-13-148104-5.

Rafael Sotelo

Es Doctor en Ingeniería Telemática por la Universidad de Vigo, MBA por el IEEM e Ingeniero Electricista opción Telecomunicaciones por la UDELAR. En la Universidad de Montevideo dirige las carreras Ingeniería Telemática e Ingeniería en Informática, así como el Departamento de Tecnologías de la Información y las Comunicaciones. Integra el Sistema Nacional de Investigadores de ANII. Es miembro titular de la Academia Nacional de Ingeniería. Es asesor en el Ministerio de Industria, Energía y Minería, referente técnico en el Centro de Desarrollo de Contenidos y Laboratorio de TV Digital. Es Profesor Adjunto en la Facultad de Ingeniería de UDELAR. Fue Gerente de Ingeniería de Canal 10 de Montevideo, donde trabajó entre 1991 y 2010. Ha sido consultor de diversas empresas y organizaciones, entre ellas TCC, GEOCOM y LATU. Es senior member de la IEEE, habiendo participado en diversos comités y posiciones a nivel nacional. Tiene numerosas publicaciones en revistas y congresos científicos. Integra el comité editorial de varias revistas internacionales y el comité de programa de diferentes congresos internacionales.

EL DESAFÍO DE UNA GESTIÓN DE RIESGO EFICIENTE...



Risk Insight & Compliance es una plataforma que permite implementar una práctica robusta de gestión de riesgos, alineada a los estándares internacionales más relevantes en el tema, pudiendo aplicarse a procesos de gestión de Riesgos Operativos (Enterprise Risk Management – ERM), de gestión de Riesgos de IT y de gestión de Riesgos de Proyectos y Portafolios.

RI&C cuenta adicionalmente con funcionalidades adicionales que permiten soportar un molde de **Gobernanza, Riesgo y Cumplimiento** (GRC) bajo un eficiente enfoque convergente, que integra estas prácticas en forma óptima, permitiendo:

- *Verificar el nivel de Cumplimiento de la organización respecto de las Normas, Políticas, Leyes, Procedimientos, etc., ingresados en RI&C; contando con Bases de Conocimiento que ya incluyen los principales marcos de referencia a nivel de Seguridad y Control IT*
- *Realizar un Análisis Ampliado de los datos gestionados, aplicando herramientas de Analytics.*

CiGRAS X

ISACA Montevideo Chapter

X Congreso Internacional sobre Gobierno, Riesgos, Auditoría y Seguridad de la Información

PATROCINADOR PLATINO

GlobalSUITE

PATROCINADORES ORO

QUANAM®

agesic

ARNALDO C. CASTRO S.A.
TECNOLOGÍA / INNOVACIÓN / PROYECTOS / SERVICIO

Microsoft

APOYAN

UDE
UNIVERSIDAD DE LA EMPRESA

Instituto Uruguayo de Auditoría Interna

AsIAP

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

FACULTAD DE INGENIERIA

UM
UNIVERSIDAD DE MONTEVIDEO

ORT
UNIVERSIDAD ORT Uruguay

FCEA
FACULTAD DE CIENCIAS ECONÓMICAS Y DE ADMINISTRACIÓN

IEEE
Advancing Technology for Humanity

PMI
MONTEVIDEO, URUGUAY CHAPTER

Universidad Católica del Uruguay

UruguayNatural
Ministerio de Turismo

Congreso Internacional sobre Gobierno, Riesgos, Auditoría y Seguridad de la Información

CiGRAS X

10° EDICIÓN - 2 Y 3 DE OCTUBRE DE 2019 - HOTEL NH COLUMBIA - MONTEVIDEO, URUGUAY

MIÉRCOLES 2 DE OCTUBRE DE 2019

HORARIO	TEMA	DISERTANTE	ENTIDAD / PAIS
8:00 a 9:00 hs.	Acreditaciones.		
9:00 a 9:15 hs.	Palabras de bienvenida.	Ing. José Luis Mauro Vera, MBA, CISA	Presidente ISACA Montevideo Chapter
9:15 a 10:00 hs.	La necesaria regulación de los sistemas autónomos. ¿Dónde estamos y hacia donde vamos?	Dr. Matías Rodríguez	Uruguay
10:00 a 10:45 hs.	El rol de TI en modelos GRC exitosos.	A/P Graciela Ricci, CISA, CGEIT, CRISC	Quanam, Uruguay
10:30 a 11:00 hs.	Corte para café		
11:00 a 11:45 hs.	Las aristas ocultas de la resiliencia organizacional.	Javier Rosado, CISA, ITIL-F	Global Suite, España
11:45 a 12:45 hs.	Auditoría de TI resiliente en el proceso de transformación digital del nuevo milenio.	Lic. Randall Artavia, CISA, CIA	ISACA Costa Rica Chapter
12:45 a 14:30 hs.	Tiempo libre para almuerzo.		
14:30 a 16:00 hs.	SheLeadsTech. Desafiando estadísticas.	Panel: Fernanda Molina, Mariana Grunfeld, Ma. Emilia Irrazabal, Sabrina Lanzotti; Victoria Pérez, Daniela Gómez, Silvia Nane, Magela Giorgi, Florencia Ripa	Moderan: Ing. Evelyn Antón, A/P Ethel Kornecki, Ing. Ma. Inés García
16:00 a 16:30 hs.	Corte para café		
16:30 a 17:30 hs.	Bendito sea nuestro bugs bounty de cada día. Los ciber buscadores de vulnerabilidades.	Panel: Ezequiel Pereira Santiago Presedo Fabrizio Fagiani	Modera: Maximiliano Alonzo, CISM

JUEVES 3 DE OCTUBRE DE 2019

HORARIO	TEMA	DISERTANTE	ENTIDAD / PAÍS
9:00 a 9:30 hs.	Riesgos y oportunidades en la seguridad IoT.	Ing. Ana Lucero, PMP, CSM, ITIL-F Lic. Joaquín Pérez	Tilo Security, Uruguay
9:30 a 10:00 hs.	Desafíos y oportunidades en la industria de TI. Acciones de CUTI.	Anibal Gonda	GeneXus, Cámara Uruguaya de Tecnologías de la Información (CUTI)
10:00 a 10:30 hs.	¡Limones tengo!	Ing. Florencia Polcaro	Big Cheese, Girls in Tech. Uruguay
10:30 a 11:00 hs.	Corte para café		
11:00 a 11:30 hs.	El desafío de IoT, la seguridad y Blockchain.	Ing. Gustavo Giannattasio, PMP	PMI Montevideo, IEEE Montevideo, Uruguay
11:30 a 12:00 hs.	Blockchain para negocios.	Ing. Ignacio Varese, PMP	Blockbear, Uruguay
12:00 a 12:45 hs.	Agregando Sec a DevOps.	Genry Leyva	Arnaldo C. Castro, Uruguay
12:45 a 14:30 hs.	Almuerzo cortesía de ISACA.		
14:30 a 15:15 hs.	Practicas de desarrollo seguro con Microsoft SDL y herramientas para SecDevOps	Fabian Alves	Microsoft Uruguay
15:15 a 16:00 hs.	Una visión de la Gestión de Riesgos de IT, para entornos cambiantes.	Hector Calderazzi	ISACA Buenos Aires Chapter
16:00 a 16:30 hs.	Corte para café.		
16:30 a 17:30 hs.	Centro de excelencia en ciberseguridad: mirando el futuro.	Silvia Da Rosa y Juan Pablo Garcia	AGESIC, Uruguay

ISACA®
Montevideo Chapter