OBSERVATORIO CT+i

OPORTUNIDADES Y TENDENCIAS TECNOLÓGICAS
PARA LOS NEGOCIOS DEL FUTURO

LICENCIA

REFERENCIA BIBLIOGRÁFICA

Sugerimos se referencie el documento de la siguiente forma:

Corporación Ruta N (2018). Observatorio CT+i: Informe No. 1. Ciberseguridad
Recuperado desde www.rutanmedellin.org

ÁREA DE OPORTUNIDAD: CIBERSEGURIDAD

OBSERVATORIO CT+i

ruta n
MEDELLÍN
CENTRO DE INNOVACIÓN Y NEGOCIOS

OBSERVATORIO CT+i

INNRUTA

RED DE INTELIGENCIA COMPETITIVA

tecnnova
Conectamos Universidad Empresa Estado

UNIVERSIDAD DE ANTIOQUIA

UNIVERSIDAD NACIONAL DE COLOMBIA

UNIVERSIDAD EAFIT

Universidad Pontificia Bolivariana

UNIVERSIDAD EIA
Ser, Saber y Servir
Con Acreditación Institucional

UNIVERSIDAD DE MEDELLIN

ITM
Institución Universitaria
Acreditada en Alta Calidad

OBSERVATORIO CT+i

DESARROLLA EL ESTUDIO

ASESOR
Ramiro Paniagua
Director Tanque de Pensamiento

PARTICIANTES

El estudio de vigilancia tecnológica e inteligencia competitiva denominado CIBERSEGURIDAD fue desarrollado por el Instituto Tecnológico Metropolitano - ITM en el cual los participantes asumieron los siguientes roles:

Metodólogo: Asesora con la metodología de vigilancia tecnológica e inteligencia competitiva diseñada para el proyecto Observatorio CT+i y definida por INNRUTA - Red de Inteligencia competitiva. Adicionalmente coordina dentro de cada institución los ejercicios realizados.

Vigía: Encargado de recopilar de fuentes primarias y secundarias los datos e información relacionada con el área de oportunidad estudiada. Realiza con expertos temáticos y asesores el análisis de la información recopilada y la consolidación de los informes del estudio de inteligencia competitiva.

El estudio contó con la participación de Ramiro Paniagua quien desempeñó el papel de asesor temático con las siguientes actividades.

Asesor temático: Participa en las etapas de análisis y validación de la información recopilada por el vigía. Orienta y da lineamientos del estudio de inteligencia competitiva realizado.

Se contó con la participación de un grupo de actores con conocimientos en relación a la temática, quienes contribuyeron en la validación y priorización de oportunidades.

PARTICIANTES

DIRECTOR DEL PROYECTO:
Elkin Echeverri

COORDINADORES DEL PROYECTO:
María Isabel Palomino Ángel
Carlos Andrés Franco Pachón

EXPERTA TIC
Ana María Salazar

DIRECTOR DEL PROYECTO:
Camilo Andrés García Giraldo

COORDINADORA DEL PROYECTO:
Diana María Aguilar Valencia

METODÓLOGAS:
Diana María Aguilar Valencia
Paola Vargas González

METODÓLOGOS:
David Alejandro Coy
Eliana Villa

VIGÍA:
Juan Fernando Pérez Pérez
Jhonjali García Mosquera

INTRODUCCIÓN

El presente estudio es un panorama sobre Ciberseguridad desde el análisis de compañías emergentes como *startups*, así como capacidades y oportunidades locales.

La información aquí contenida representa el resultado de un estudio de inteligencia competitiva en el cual se realizó una revisión de modelos de negocio de *startups* a nivel global, identificando sus dinámicas, características y lo que las hace diferentes y atractivas para inversión. *Las startups* fueron revisadas y priorizadas por Ruta N, como actores claves dentro de escenarios de negocios que podrían aprovecharse en la ciudad y Latinoamérica.

Adicionalmente se realizó un mapeo de las capacidades locales tanto desde las empresas como desde la investigación, para finalmente, a partir de la comparación entre las soluciones globales y las locales, identificar las potenciales oportunidades de innovación para la ciudad, las cuales fueron validadas y priorizadas con el aporte de actores del ecosistema de innovación.

El estudio ofrece a los lectores una focalización en modelos de negocios emergentes, con el fin de promover trabajo colaborativo, donde se complementen capacidades y se aprovechen oportunidades de negocios que aún no están siendo explotadas a nivel local. Busca incentivar la curiosidad por profundizar más en el tema y generar dinámicas para la creación de nuevos negocios en la ciudad.

METODOLOGÍA

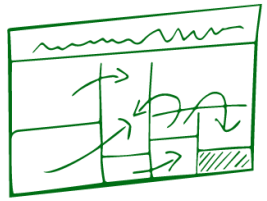
Estos estudios fueron realizados con la siguiente metodología:

Definición de áreas de oportunidad

- Se tuvieron en cuenta: El historial de proyectos de I+D; la oferta y demanda tecnológica de la ciudad en la plataforma SUNN; áreas de oportunidad identificadas en estudios previos del observatorio.
- Reportes de tendencias globales

Definición de empresas a analizar

A partir de las temáticas definidas se identifican mediante reportes de *startups*, aquellas que tienen propuestas novedosas y que son definidas como empresas para "mantener bajo observación" ya que son potenciales para crear una disrupción de mercado.



Análisis de modelos de negocio Empresas identificadas

Búsqueda y análisis de información asociada al modelo de negocio de las empresas priorizadas. Esta información se esquematiza según un lienzo de modelo de negocio definido para este estudio. Se presenta de manera consolidada en este documento y detallada en el informe Anexo.

Identificación de oferta de soluciones locales

Se realiza referenciación de empresas y grupos de investigación locales, así como de su oferta de soluciones y productos.

Definición de oportunidades para la ciudad

Esta definición se realiza considerando las soluciones globales para las cuales no se identifica actualmente oferta en Medellín, estas soluciones son potenciales oportunidades de innovación para la ciudad y serán estudiadas y priorizadas en un taller con grupos de interés para cada área de oportunidad.

ALCANCE DEL ESTUDIO

CIBERSEGURIDAD

1. GENERALIDADES

- Contexto sobre Ciberseguridad.
- Inversiones en *startups* de Ciberseguridad.

2. MODELOS DE NEGOCIO

- *Insights* modelos de negocio para cada enfoque.
- Desarrollos tecnológicos asociados para las *startups* analizadas.

3. CAPACIDADES LOCALES

- Contexto de ¿Cómo está Medellín? Desde el ámbito tecnológico, investigativo y político.

4. OPORTUNIDADES

- Oportunidades de desarrollo de innovación y negocios con el análisis de las capacidades requeridas y brechas detectadas.

OBSERVATORIO CT+i

CONTENIDO

No DE DIAPOSITIVA

CONTENIDO

No DE DIAPOSITIVA

GENERALIDADES DEL ÁREA DE OPORTUNIDAD

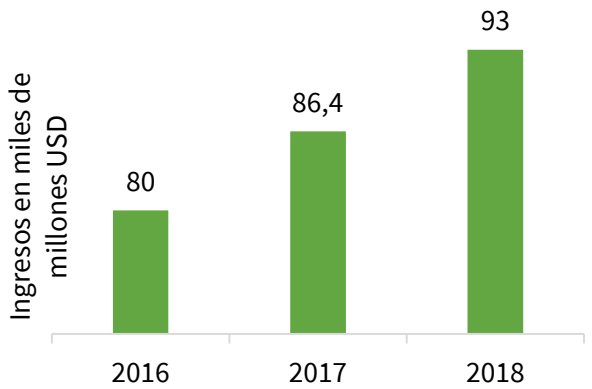
A continuación se presenta una descripción del área de oportunidad con los aspectos más importantes.

CONTEXTO DE CIBERSEGURIDAD

La seguridad es un pilar fundamental de la transformación digital y, en una economía basada en datos, la ciberseguridad se ha convertido en una prioridad para las organizaciones que deben anticiparse a los riesgos digitales para evitar posibles ataques y pérdidas de información [1]

Los atacantes cibernéticos y los responsables de la seguridad de las empresas están desarrollando tecnologías y tácticas cada vez más sólidas. Por otro lado, los atacantes están creando infraestructuras back-end cada vez más fuertes para atacar a los objetivos. Los ciberdelincuentes están perfeccionando sus técnicas para obtener dinero de sus víctimas y para evitar ser detectados mientras continúan robando datos y propiedad intelectual. Por lo que es necesario que las organizaciones tomen consciencia de la importancia de mejorar sus infraestructuras de seguridad [2].

Mercado de Ciberseguridad [3]



De acuerdo al reporte de Gartner [3], la inversión en productos y servicios de seguridad alcanzará USD $86,4 mil millones USD en 2017, un 7% más que el año anterior.

Una organización se enfrenta todos los años a una media de 94 ataques dirigidos, de los que una tercera parte alcanza su objetivo; eso equivale a 2-3 ataques con éxito por mes. Esta discrepancia pone de manifiesto un serio problema de ciberseguridad [4].

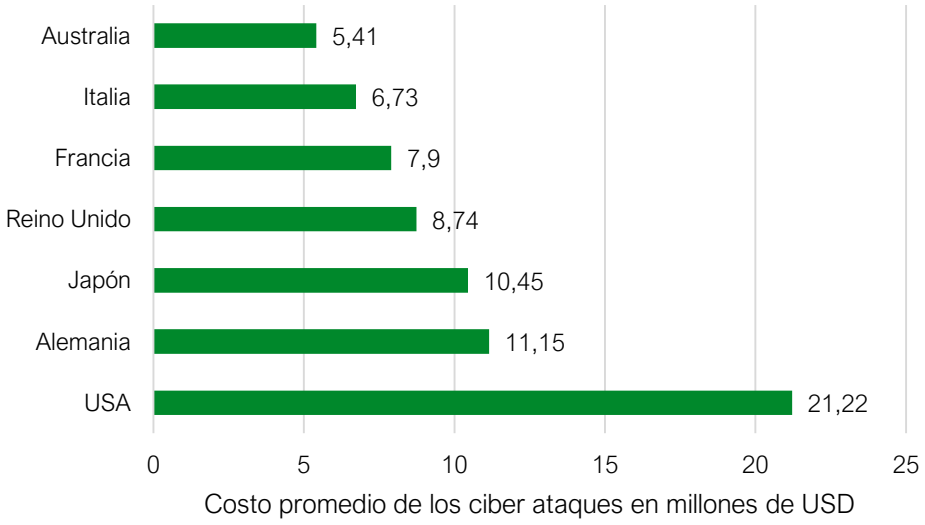
Según algunos cálculos, el cibercrimen le cuesta al mundo hasta $575 mil millones USD al año, lo que representa 0,5% del PIB global [5].

OBSERVATORIO CT+i

CONTEXTO DE CIBERSEGURIDAD

Según la firma analista de tecnologías de la información IDC, las áreas de las que se proyecta mayor crecimiento en servicios de seguridad de la información son análisis de seguridad/SIEM (Sistemas de Información y Gestión de Eventos) con un 10%; inteligencia de amenazas 10%; seguridad móvil 18% y seguridad en la nube con un 50% [6].

Costo promedio de ciberataques en empresas de países seleccionados a partir de agosto de 2017 (millones USD)



Fuente: elaboración propia a partir de [7]

Problemas de ciberseguridad más importantes según profesionales en seguridad TI

Fuente: elaboración propia a partir de [8]

"Desde una perspectiva de riesgos tecnológicos, las empresas no han incluido, en su reingeniería de procesos de negocio, la ciberseguridad como un elemento básico para tener en cuenta" [9].

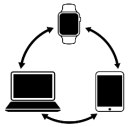
Gianluca D'Antonio, director académico del Máster en Ciberseguridad del IE Business School y presidente de ISMS Forum (Asociación Española para el Fomento de la Seguridad de la Información).

OBSERVATORIO CT+i

CONTEXTO DE CIBERSEGURIDAD

En este estudio Ciberseguridad se analizará abordando seis enfoques:

SEGURIDAD MÓVIL



SEGURIDAD EN INTERNET DE LAS COSAS

ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

SEGURIDAD DE APLICACIONES MÓVILES

ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

INTELIGENCIA PREDICTIVA

MODELOS DE NEGOCIO

En este capitulo se presentan los *insights* de los modelos de negocio para las *startups* analizadas, presentando un lienzo por cada enfoque estudiado. Este lienzo presenta los hallazgos mas relevantes en relación a las *startups*.

LIENZO DEL MODELO DE NEGOCIO CONSIDERADO

POR QUÉ EXISTEN LAS *STARTUPS*

PROBLEMAS

Requerimientos o dolores del mercado, los cuales promueven la generación de las soluciones.

QUÉ HACEN DIFERENTE LAS *STARTUPS*

PROPUESTA Y ATRIBUTOS DE VALOR

Descripción de los beneficios que los clientes pueden esperar de los productos y servicios. Aquello que es difícil de copiar por parte de los competidores.

CÓMO FUNCIONAN LAS *STARTUPS*

SOLUCIONES

Productos y Servicios ofertados por las *startups*.

ADOPTANTES TEMPRANOS

Clientes, de acuerdo a los segmentos a los cuales se les ofrece.

CANALES

Es la forma en la que llega el producto al cliente. Existen tres tipos de canales: de comunicación, de pago y de compra.

RECURSOS CLAVE

Tecnológicos: recursos que hacen posible la solución. Orientados a tecnologías.

Humanos: formación y conocimientos de las personas que conforman las *startups*.

ALIADOS CLAVE

Son agentes con los que las *startups* necesitan trabajar para hacer posible el funcionamiento del modelo de negocio.

POTENCIAL DE LAS *STARTUPS*

FUENTES DE INGRESO

Describe la manera en que las *Startups* ganan dinero. ¿Por qué y cómo van a pagar los clientes?

INVERSIONISTAS

Empresas, entidades o personas que han invertido en las *startups.*

MÉTRICAS CLAVE

Indicadores para la toma de decisiones. ¿Cómo están midiendo el éxito?, ¿Qué indicadores están usando?

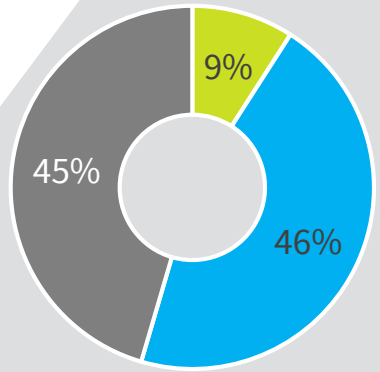
OBSERVATORIO CT+i

SEGURIDAD MÓVIL

Implementación de protocolos de seguridad para evitar que hackers y cibercriminales obtengan acceso a las redes corporativas a través del engaño de los usuarios mediante las plataformas móviles.

RESUMEN EMPRESAS ANÁLIZADAS PARA SEGURIDAD MÓVIL

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
Zimperium	USA	2010	● ●	4	60.000.000
Appthority	USA	2011	● ● ●	5	25.250.000
Skycure	USA	2012	● ●	4	27.500.000
Mi3 Security	USA	2013	● ●	0	550.000
Sentegrity	USA	2014	● ●	1	124.297



- Plataforma de análisis avanzado
- Aplicaciones de análisis de riesgo
- Software de autenticación inteligente

SOLUCIONES

OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD MÓVIL

PROBLEMAS

- Riesgos asociados a vulneraciones de seguridad y de la información confidencial, por la instalación de aplicaciones.
- Vulnerabilidad en la administración de credenciales y datos personales de clientes.
- Violaciones de seguridad por medio de dispositivos móviles.

SOLUCIONES

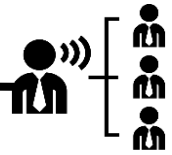
- **Plataforma de análisis avanzado:** para evaluar continuamente el riesgo en apps móviles, permitiendo mantenerse al tanto del estado de las mismas y generar estrategias de protección en tiempo real.
- **Aplicaciones de análisis de riesgo:** detección de amenazas móviles basada en puntuación de riesgos de las aplicaciones, detecta amenazas de malware y riesgo de pérdida de datos.
- **Software de autenticación inteligente:** aplicación de inteligencia contra amenazas y reconocimiento basado en el comportamiento del usuario para prevenir vulneraciones y fraudes en las aplicaciones.

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD MÓVIL

ADOPTANTES TEMPRANOS

- **Sector salud**: *Aetna*.
- **Sector financiero**: *New York Life*.
- **Manufacturero**: *Republic National Distributing Company*.
- **Operadores móviles y servicios web**: *Samsung KNOX, SDG, Corporation, Matrix42, Citrix, Microsoft, SAP, MobileIron*.
- Gobierno.
- Aseguradoras.

CANALES



Comunicación: *Twitter, Facebook, YouTube, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

- **E-mail, teléfono**: Contacto directo con los clientes.
- **WebSite**: publicación general de la compañía
- **Blog**: publicación de noticias de actualidad, artículos sobre temas alrededor de la seguridad móvil.
- **Webinars**: seminarios web sobre mejores prácticas, instrucción sobre lo que se debe saber en temas de seguridad móvil

Pago: pago online por medio de tarjeta débito y crédito.

Compra: a través del sitio web.

RECURSOS CLAVE

Tecnológicos: se emplea el método de análisis de reputación que proporciona información de la seguridad de las Apps, emplea técnicas avanzadas en aprendizaje automático y procesamiento paralelo.

- **Plataformas:** emplean aprendizaje automático para detectar y prevenir amenazas y vulnerabilidades en las aplicaciones móviles.
- **Software:** Se basa en el análisis sensorial y *machine learning* para la autentificación inteligente.

Paquete tecnológico

- **Ventas y BD:** *Clearbit Connect*, Software de *CRM, Lead Flows*.
- **Devops y IT:** *Explorer by 42matters, Amazon ELB, Amazon CloudFront, DigiCert.*
- **Desarrollador:** *PHP, Applivery, Cloudwords*.
- **Analítica y ciencias de datos**: *Google Analytics, CrazyEgg*.
- **Producto y diseño:** *Google Fonts, fancyBox3, Squarespace*.
- **Productividad y operaciones:** *Siftery Discover, Grasshopper, dmarcian.*
- **Atención y éxito al cliente:** *Zendesk, Olark, Intercom*.
- **Marketing:** *LinkedIn, MailChimp, Cloudwords*.

Humanos: Ciencias computacionales, programadores web y de software, administración, ciencia de datos.

- **Conocimientos** en Bases de datos *SQL, No-SQL, Oracle, MySQL, MongoDB, Postgres*; en lenguajes *scripting Bash, Python; Tecnologías de Amazon* (*EC2, RDS, SQS, ElastiCache, CloudFormation*).
- **Certificaciones** CIO / CISO.

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD MÓVIL

PROPUESTA Y ATRIBUTOS DE VALOR

- Las tecnologías, productos y servicios ofrecidos, le permiten a los clientes comprender los niveles de riesgo a los que está expuesta la organización, brindándole herramientas a través de tecnología avanzada para la detección, eliminación y prevención de ataques cibernéticos.
- Protección móvil con inteligencia avanzada frente amenazas móviles al tiempo que cumple con las políticas del proveedor del sistema operativo.

FUENTES DE INGRESO

1. Suscripción

Paquetes únicos

- **Por dispositivo móvil:** integración automatizada de Gestión de Dispositivos Móviles (MDM por sus siglas en inglés) para la detección de las aplicaciones de los empleados, así como la recopilación y la aplicación de políticas de riesgo.
- **Por aplicación móvil:** incluye informes de envío y control de políticas.

2. Soporte

- Programas de soporte técnico empresarial.

INVERSIONISTAS

- *SoftBank*
- *Blue Coat*
- *Trident Capital Cybersecurity*
- *U.S. Ventures Partners (USVP)*
- *Foundation Capital*

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD MÓVIL

ALIADOS CLAVE

Aliados tecnológicos

- ***MobileIron*:** soluciones de gestión de dispositivos móviles (MDM) y gestión de movilidad empresarial (EMM)
- ***BlackBerry*:** dispositivos y soluciones inalámbricas .
- ***Microsoft*:** soporte de software y apps.
- ***Samsung*:** electrónica, hardware, dispositivo y semiconductor.
- ***Citrix*:** software empresarial, SaaS y virtualización.
- ***VmWare*:** servicios de virtualización y nube.
- ***AirWatch*:** dispositivos móviles y seguridad.

MÉTRICAS CLAVE

- Número de análisis realizados diariamente.
- Mitigación automática de amenazas.
- Número de amenazas detectadas.
- Número de ataques prevenidos.
- Porcentaje de ahorro por la disminución de ataques cibernéticos.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - SEGURIDAD MÓVIL

	Número de Patentes	Descripción de las Patentes	Geografías de protección
appthority	5	Invenciones que permiten la clasificación automática de aplicaciones móviles, arrojando una clasificación de acuerdo al perfil de riesgo que éstas posean, permitiendo realizar filtrado de componentes maliciosos, como malware publicitario.	• USA
Sentegrity	1	Se describe un sistema para autenticar usuarios de dispositivos móviles de manera transparente.	• USA

DESARROLLOS TECNOLÓGICOS ASOCIADOS - SEGURIDAD MÓVIL

	Número de Patentes	Descripción de las Patentes	Geografías de protección
Skycure	4	La tecnología patentada de Skycure se basa en mecanismos de defensa avanzada móvil que incluye enfoque Honeypot activo para la seguridad de la red, confirmación de hack del servidor que utiliza inteligencia artificial para identificar la fuente y el destino del hacker, motores de análisis e inteligencia de amenazas que permiten una identificación rápida de aplicaciones reempaquetadas basadas en una amplia variedad de datos forenses, protección selectiva de recursos (SRP) y protección de conexión segura (SCP).	• USA • PCT[1]
ZIMPERIUM	4	Las tecnologías patentadas hacen referencia a sistemas, técnicas, procedimientos y motores de defensa basados con IA (machine learning), empleados para proporcionar seguridad móvil con actividades de prevención, análisis y detección de ataque cibernético en redes de acuerdo a la ubicación geográfica, malware y amenazas avanzadas.	• USA • Republica de Corea

1. PCT, es un tratado internacional ratificado por más de 150 Estados contratantes. Con el PCT puede solicitar la protección de una invención por patente mediante la presentación de una única solicitud "internacional" de patente en un gran número de países, sin necesidad de cursar por separado varias solicitudes de patente nacionales o regionales.

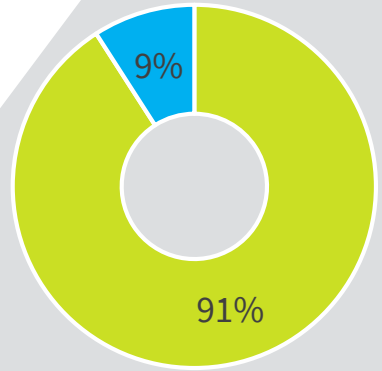
ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

Comprende la implementación de un conjunto de tecnologías, herramientas, controles, protocolos, reglas y políticas de seguridad para la detección, prevención y respuestas contra actividades fraudulentas provocadas y ejecutadas por ciberdelincuentes.

La gestión de identidad es "la combinación de sistemas técnicos y comerciales, políticas y procesos que se utilizan para habilitar, gobernar y sincronizar la recopilación, utilización y protección de la información de identidad de los usuarios.

RESUMEN EMPRESAS ANÁLIZADAS PARA ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
Feedzai	USA	2010	●	2	76.120.203
siftscience.com	USA	2011	● ●	0	53.600.000
Agari	USA	2012	●	1	44.700.000
Shift Technology	Francia	2013	●	1	39.800.000
Socure	USA	2014	●	2	31.900.000
Datavisor	USA	2010	●	3	14.500.000
Trooly	USA	2011	●	1	10.000.000
Greathorn	USA	2012	●	1	8.825.000
Skymind	USA	2013	●	0	7.200.000
Simility	USA	2014	●	0	6.320.000



Detección inteligente de amenazas

Verificación de identidad

SOLUCIONES

OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

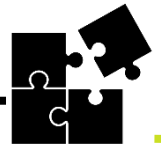
Contenido

INSIGHTS MODELO DE NEGOCIO - ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

PROBLEMAS

- Fugas de información y fraudes por ataques cibernéticos a las cuentas bancarias.
- Transacciones fraudulentas.
- Creaciones de cuentas falsas.
- Poca capacidad para detectar ataques de suplantación de identidad -*phishing*.
- Poca seguridad en la comunicación de los clientes a través del e-mail.
- Poca capacidad para la protección de datos de los clientes.
- Poca agilidad en la reacción ante ataques de fraude.

SOLUCIONES

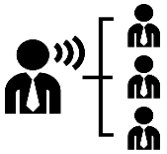


- **Detección inteligente de amenazas:** empleando inteligencia artificial y aprendizaje automático avanzado, permite la detección de comportamientos fraudulentos, así como de malos actores que publiquen contenido malicioso o de baja calidad que pueda dañar la reputación de las empresas; evita transacciones fraudulentas.
- **Verificación de identidad:** plataforma de inteligencia artificial y biometría social para la verificación de identidad digital para prevenir vulneraciones y fraudes.

ADOPTANTES TEMPRANOS

- **E-Commerce**: *Jet, Wayfair*, Grupo *Alibaba, Letgo.*
- **Sector financiero**: *Farm Bureau Bank, Digital Bank.*
- **Sector seguros**: *Direct Line Insurance.*
- **Sector salud**: *Aetna.*
- **Sector tecnológico**: *Facebook, Microsoft, Google, Neustar*.
- **Aplicaciones móviles y servicios web**: *Yelp, Pinterest, Momo.*
- **Gobierno**: *U.S. Senate, United States Postal Service*.
- **Viajes**: *Traveloka, Airbnb, Fareportal, Despegar.com.*
- **Saas**: *Twilio, DigitalOCean, Shippo, Hostinger.*
- Marketing y comunidades: *Twitter, Yelp, indeed, Match.com.*

CANALES



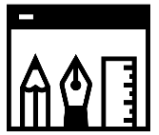
Comunicación: *Twitter, Facebook, YouTube, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

- **E-mail, teléfono**: Contacto directo con los clientes.
- **WebSite**: publicaciones de la compañía.
- **Blog**: publicación de noticias de actualidad, artículos sobre temas alrededor del fraude en línea. Blog de ingeniería, blog especializado en la publicación de contenido técnico en tecnologías como el aprendizaje automático.
- **Webinars**: seminarios web sobre el aprendizaje automático.

Pago: pago online por medio de tarjeta débito y crédito.

Compra: online a través de la pagina web.

RECURSOS CLAVE



Tecnológicos:

- **Algoritmos de aprendizaje automático:** emplea algoritmos de aprendizaje automático para el análisis de grandes cantidades de datos públicos y privados en tiempo real que permiten verificar identidades y la procedencia de e-mails maliciosos.
- **Plataformas, APIs y motores inteligentes:** que utilizan aprendizaje automático profundo, para realizar detección y prevención avanzada del fraude.

Paquete tecnológico

- **HR:** *AngelList Jobs, Greenhouse, SumoMe*.
- **Ventas y BD:** *Clearbit Connect, SumoMe, LeadIQ, Salesforce Sales Cloud*.
- **Analítica y ciencias de datos:** *Google Analytics, Inspectlet, KISSmetrics*.
- **Devops y IT:** *GoDaddy SSL, New Relic, MediaElement.js, WordPress*.
- **Desarrollador:** *Bootstrap, Lightbox, Pitón, jQuery*.
- **Marketing:** *AdRoll, Buffer, DoubleClick, Bombora, Google Doubleclick*.
- **Productividad y diseño:** *Google Fonts,, Asana, Trello*.
- **Productividad y operaciones:** *Box, Airflow, DocuSign*.
- **Finanza y contabilidad:** *Expensify.*

Humanos: Ingenieros de sistemas, desarrolladores web y software, especialistas en análisis y procesamiento de datos, profesionales en finanzas, ciencias computacionales, científicos de datos, expertos en seguridad informática.

- **Conocimientos** en lenguajes de programación *Bash, Ruby, Python, Java, Scala o C++*; en conceptos de modelado estadístico, aprendizaje automático, minería de datos, NLP.
- **Experiencia** en desarrollo de sistemas distribuidos, de trabajo con las bases de datos *SQL, PostGreSQL, NoSQL, Spark, Akka, RabbitMQ o Cassandra*.

PROPUESTA Y ATRIBUTOS DE VALOR

- Detección y prevención de fraude cibernético integrando técnicas avanzadas de aprendizaje automático no supervisado e inteligencia artificial.
- Posibilita que las experiencias en línea sean más rápidas y seguras.
- La tecnología desarrollada, proporciona seguridad para todas las conexiones inalámbricas y puntos finales.

FUENTES DE INGRESO

1. **Suscripción**

Suscripción Freemium: versión gratuita.

Suscripción Premium: paquetes que varían de acuerdo a los servicios que incluye cada plan y por número de usuario utilizando la aplicación. Esto incluye:

- *Small*: 15000 eventos facturados USD1000/mes.
- *Medium*: 45000 eventos facturados USD1000/mes.
- *Large*: 100.000 eventos facturados USD1000/mes.
- *X-Large*: 225.000 eventos facturados USD1000/mes.

2. **Soporte Técnico:** equipo experto en ciberseguridad que ofrecen servicio técnico de acuerdo a la necesidad.
3. **Formación**: capacitación en línea con personal experto en aprendizaje automático y ciberseguridad.

INSIGHTS MODELO DE NEGOCIO - ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

INVERSIONISTAS

- *Dell Technologies Capital.*
- *Battery Ventures.*
- *Accel Partners.*
- *Microsoft Accelerator Paris.*
- *Santander InnoVentures.*
- *FF Venture Capital.*

ALIADOS CLAVE

Aliados tecnológicos

- **SAP:** proporciona software de planificación de recursos empresariales.
- **Cloudera:** Software basado en *Apache Hadoop*.
- **Deloitte:** Consultoría en gestión de riesgos financieros.
- **Optiv:** Servicios avanzados de seguridad cibernética.
- **Cisco:** apoyo en hardware de red, equipos de telecomunicaciones .
- **Microsoft:** Licencias de software.
- **Slack:** plataforma de software empresarial.

MÉTRICAS CLAVE

- Número de URL maliciosas detectadas.
- Número de siniestros detectados.
- Porcentaje de reducción de fraude.
- Porcentaje de aumento en la precisión de detección.
- Porcentaje de reducción en el tiempo de revisión manual.
- Porcentaje de reducción de falsos positivos.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

feedzai	Número de Patentes	Descripción de las Patentes	Geografías de protección
	2	La invención hace referencia a una unidad de procesamiento de gráficos (GPU) para acelerar el procesamiento de flujo de datos.	• USA

AGARI	Número de Patentes	Descripción de las Patentes	Geografías de protección
	1	La patente hace referencia a una técnica de autenticación de los remitentes de un mensaje para evaluar el nivel de riesgo del mensaje.	• USA

SOCURE	Número de Patentes	Descripción de las Patentes	Geografías de protección
	2	Se proporcionan herramientas, estrategias y técnicas para evaluar las identidades de diferentes entidades para la protección de los datos de los usuarios y empresas, mediante la actividad biométrica con datos o la llamada biométrica social.	• USA

DESARROLLOS TECNOLÓGICOS ASOCIADOS - ANTIFRAUDE Y GESTIÓN DE IDENTIDAD

DATAVISOR

Número de Patentes	Descripción de las Patentes	Geografías de protección
3	Las invenciones desarrolladas por Datavisor hacen referencia a herramientas, métodos, sistemas y motores que combinan tecnologías avanzadas de inteligencia artificial y Big Data para detectar ataques como fraudes, falsificación y robo de identidad, cuentas, sin utilizar datos de entrenamiento.	• USA • PCT[1]

trooly

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	Métodos, sistemas y aparatos, incluidos programas informáticos codificados en un medio de almacenamiento, para identificar documentos relacionados con una persona, derivar comportamientos y rasgos de personalidad desde el análisis de documentos, obtener información relevante que evalúe el comportamiento y determinar puntuación de confiabilidad o puntaje de compatibilidad de la persona evaluada.	• USA

GreatHorn

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	La presente invención hace referencia a métodos y sistemas implementado por ordenadores para seleccionar cadenas de caracteres de texto de un corpus de cadenas relevantes similares a las del ser humano.	• USA

1. PCT, es un tratado internacional ratificado por más de 150 Estados contratantes. Con el PCT puede solicitar la protección de una invención por patente mediante la presentación de una única solicitud "internacional" de patente en un gran número de países, sin necesidad de cursar por separado varias solicitudes de patente nacionales o regionales.

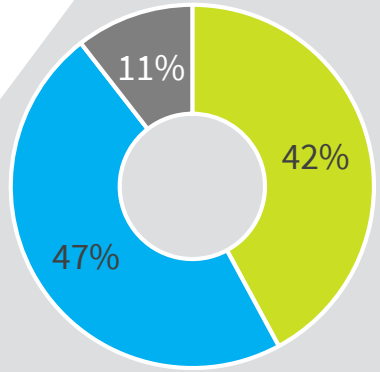
ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

Análisis de datos multimodales, que incluyen audio, video, archivos de registro de actividades, para crear patrones de comportamiento del usuario a través de las actividades digitales [13].

La detección de anomalías, consiste en el desarrollo e implementación de técnicas y procedimientos avanzados, que permitan identificar comportamientos inusuales con el fin de minimizar riesgos y amenazas de seguridad.

RESUMEN EMPRESAS ANÁLIZADAS PARA ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANOMALÍAS

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
Exabeam	USA	2013	● ●	2	65.000.000
Perimeterx	USA	2014	● ●	1	34.500.000
Sqrrl	USA	2012	● ●	4	26.500.000
Fortscale	USA	2014	● ●	1	23.000.000
E8 Security	USA	2013	● ●	1	21.800.000
Redlock	USA	2015	● ●	0	12.000.000
Cyberx	USA	2012	● ●	1	11.020.000
Interset	Canadá	2015	● ●	3	10.000.000
Intensity Analytics	USA	2009	● ● ●	1	8.500.000
BehavioSec	Suecia	2007	●	1	6.400.000



● Plataforma de detección de amenazas

● Análisis de comportamiento de usuarios y entidades

● Software de autentificación de identidad inteligente

SOLUCIONES

OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

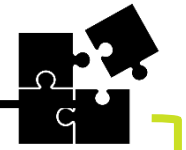
Contenido

INSIGHTS MODELO DE NEGOCIO - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

PROBLEMAS

- Falencia de herramientas que integren información de diferentes fuentes que incluyen audio, video y archivos de registro de actividades para identificar amenazas.
- Desconocimiento del comportamiento normal de las personas, que puede ayudar a identificar fallas potenciales a la seguridad.
- Falta de monitoreo al uso de credenciales de los usuarios

SOLUCIONES



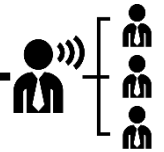
- **Plataforma de detección de amenazas:** detección de amenazas tanto internas como externas, para evitar pérdida de datos empleando aprendizaje automático profundo y modelo de riesgos estadísticos especializados.
- **Análisis de comportamiento de usuarios y entidades**: por medio de aprendizaje automático correlacionan la actividad del usuario y de otras entidades (como *endpoints*, dispositivos móviles redes locales, y amenazas externas), para identificar de forma temprana y efectiva amenazas.
- **Autentificación de identidad inteligente:** software que combina la tecnología de biometría conductual pasiva y el aprendizaje automático continuo, permitiendo al cliente implementar novedosos mecanismos de autentificación para detener el fraude, evitar ataques y verificar a los usuarios.

INSIGHTS MODELO DE NEGOCIO - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

ADOPTANTES TEMPRANOS

- **Retail**: *Safeway, The Real Real, Axfood, PUMA.*
- **Sector financiero**: *BBCN Bank, American Express, MoneyGram.*
- **Sector seguros**: *Zipongo*.
- **Educación**: *Universidad de Ohio*.
- **E-Commerce**: *Coupons Inc, Grubhub.*
- **Publicidad y Marketing**: *Zillow.*
- **Sector de desarrollo web**: *Cross Match, WIX.*
- **Servicios tecnológicos**: *Mitsubishi, Siemens, Toshiba, ABB, Yokogawa.*

CANALES



Comunicación: *Twitter, Facebook, YouTube, WebSite, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

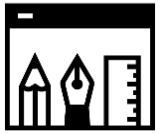
- **E-mail, teléfono**: Contacto directo con los clientes.
- ***Website***: publicación general de la compañía.
- ***Blog***: publicación de noticias de actualidad, artículos sobre temas relacionados con el fraude y la seguridad en el comercio electrónico, recomendaciones para hacer seguro un sitio web, ataques de bot, entre otros temas de interés.
- ***Webinars***: seminarios web bajo demanda sobre temas de seguridad en la web, ataques de bots, análisis de comportamientos para la protección de los sitios *webs.*

Pago: pago online por medio de tarjeta débito y crédito

Compra: online a través de la página web.

INSIGHTS MODELO DE NEGOCIO - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

RECURSOS CLAVE



Tecnológicos:

Complementos *JavaScript*: que se agrega al navegador web, el cual actúa como un sensor que recopila y envía datos para analizar el comportamiento de los usuarios y del dispositivo así como de la actividad de la red, mediante aprendizaje automático.

Plataformas y motores de análisis con Inteligencia Artificial: integradas con tecnologías de evaluación de riesgos y vulnerabilidades para la detección de amenazas basadas en el comportamiento y con una probabilidad mínima de falsos positivos.

Paquetes tecnológico

- **Ciencias y analítica de datos:** *Matomo, Hotjar, Google Analytics*.
- **Devops y IT:** *Apache HTTP Server, GoDaddy SSL, Incapsula, Wistia*.
- **Productividad y operaciones**: *Criteo, Microsoft Outlook, My Ally (formerly Skedool.it*).
- **Marketing:** *AdRoll, AddToAny, Eyeota*.
- **Desarrollador:** *Adobe Flash, Bootstrap, PHP, jQuery*.
- **Productividad y diseño:** *GreenSock Animation Platform, Google Fonts*.
- **Servicios y éxitos al cliente:** *Drift*
- **Ventas y BD:** *Clearbit Connect, Sumo*.
- **HR:** *Lever, Kin, TheLions.*

Humanos: Ingenieros de sistemas, desarrolladores web y software, especialistas en análisis y procesamiento de datos, ciencias computacionales, matemáticas, científicos de datos, expertos en seguridad.

- **Conocimientos** en tecnologías *Big Data* como *Hadoop/Hive/Spark/Flink/Storm / Kafka*; de las tecnologías de seguridad, incluidos *Firewalls*, *Antivirus/Malware*, Prevención de intrusiones (IDS/IPS) y *End Point Security.*
- **Experiencia** en lenguajes *scripting* como *Java, Scala, Python, GO, Ruby, NodeJS, C++, C#, PHP, JavaScript*, con bases de datos *NoSQL (MongoDB, ElasticSearch, Cassandra, Redis*) y sistemas de mensajería como *Kafka, en Amazon o Google Cloud.*

INSIGHTS MODELO DE NEGOCIO - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

PROPUESTA Y ATRIBUTOS DE VALOR

- Posibilidad de detección de ciber amenazas avanzadas, protegiendo la información.
- Detección de actos maliciosos en menor tiempo, mediante *Big Data* y aprendizaje automático,
- Rápida identificación de variables y cambios en el entorno para ofrecer información más precisa y basada en riesgos en tiempo real.
- Seguridad de la infraestructura crítica en la nube y uso de aprendizaje automático profundo para detectar y descubrir anomalías y ciberataques.

FUENTES DE INGRESO

Suscripción *Freemium*: versión gratuita.

Suscripción *Premium*: paquetes de pago mensual que varían de acuerdo a la capacidad de almacenamiento.

Socios revendedores: Otra de las formas de obtener ingresos, es haciendo socios:

- Compañeros de Canal: Socios para impulsar las ventas de la compañía.
- Socios tecnológicos: Alianzas estratégicas con proveedores de tecnología.

Soporte: planes de soporte técnicos de acuerdo a la necesidad de cada cliente

INSIGHTS MODELO DE NEGOCIO - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

INVERSIONISTAS

- *Lightspeed Venture Partners*
- *Cisco Investments*
- *Intel Capital*
- *Dell Technologies Capital*
- *Technologies Fund*
- *Valor Capital Group*
- *Blumberg Capital*

ALIADOS CLAVE

Aliados tecnológicos

- ***Optiv:*** servicios avanzados de seguridad cibernética.
- ***McAfee*:** proporciona software empresarial, seguridad de red, seguridad.
- ***Netscope*:** seguridad y administración de internet.
- ***Carbon Black*:** software de Seguridad cibernética y seguridad física.
- ***Amazon Web Services*:** servicios de infraestructura de tecnología de la información.
- ***Anomali*:** Tecnología de detección e identificación más temprana de adversarios en la red.
- ***Cloudera*:** proporciona ofrece software basado en *Apache Hadoop.*
- ***Dell*:** proporciona soluciones de electrónica.
- ***Hewlett Packard Enterprise* (HPE):** proporciona hardware y electrónica de consumo.
- ***IBM*:** tecnología y consultoría de tecnologías de la información.

MÉTRICAS CLAVE

- Número de incidentes detectados.
- Porcentaje de reducción del fraude.
- Porcentaje de reducción de tiempo de acción ante amenazas.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

	Número de Patentes	Descripción de las Patentes	Geografías de protección
exabeam	2	La invención hace referencia a un sistema, método y programa para detectar y evaluar riesgos de seguridad en la red informática de una empresa a través del diseño de un modelo de comportamiento para el usuario en la red.	• USA
perimeterx	1	Procedimiento para realizar la validación de seguridad de acuerdo a la navegación de un usuario de red por medio de patrones de comportamiento.	• USA
BehavioSec	8	Esta invención se refiere a método, programa y sistema que utilizan algoritmos biométricos para la autenticación e identificación de usuarios.	• USA • Suecia

DESARROLLOS TECNOLÓGICOS ASOCIADOS - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

	Número de Patentes	Descripción de las Patentes	Geografías de protección
sqrrl	4	Corresponde a un método de análisis de datos y luego generar a partir de los registros, un modelo de identidad-relación que facilita el control de acceso basado en políticas de asociación.	• USA
FORTSCALE	1	Sistema computarizado para la detección de anomalías en el comportamiento monitoreado de entidades, el sistema posee una unidad de almacenamiento de eventos supervisados, desviaciones y parámetros, para con ello asociar una puntuación del evento detectado (malicioso).	• USA
E8 SECURITY	1	Sistema para detectar amenazas de seguridad en una red local, el sistema analiza la seguridad y recopila datos, establece relaciones entre los datos recopilados y los grafica, estableciendo nodos que son conocidos como entidades.	• USA

DESARROLLOS TECNOLÓGICOS ASOCIADOS - ANÁLISIS DE COMPORTAMIENTO Y DETECCIÓN DE ANORMALIDADES

CyberX
Trusted. Industrial. Cybersecurity.

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	La invención hace referencia a métodos y sistemas utilizadas para detectar y mitigar ataques cibernéticos en sistemas de control industrial.	• USA • EP[1]

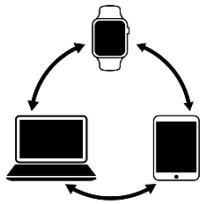
INTERSET

Número de Patentes	Descripción de las Patentes	Geografías de protección
3	Las presentes invenciones, hacen referencia a métodos, sistemas y procedimientos que utilizan IA con modelos de regresión matemática para agregar y clasificar datos que permitan identificar alertas de seguridad, analizar el riego y prevenir amenazas por ataques a la infraestructura crítica.	• USA • Canadá • España

intensity analytics

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	Esta tecnología hace referencia a un método de autenticación de identidad que proporciona integridad de autenticación superior e inteligencia de amenazas con una experiencia de usuario sin fricciones.	• USA

1. EP. El sistema de patente europea permite obtener protección mediante una solicitud de patente europea directa con designación en aquellos Estados europeos en que se quiere obtener protección y sean parte del Convenio Europeo de Patentes. Así, se puede obtener protección en hasta 38 países del ámbito europeo.

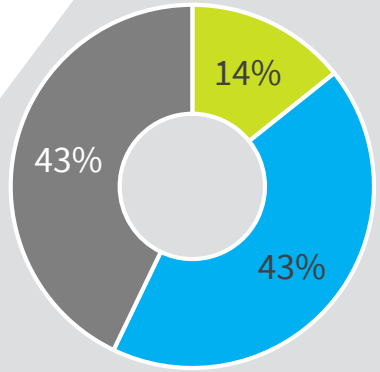


SEGURIDAD EN INTERNET DE LAS COSAS

IoT (Internet de las cosas en inglés), consiste en diseñar marcos de seguridad integrados a través de diferentes técnicas y procedimientos, para mitigar amenazas durante la conexión y transferencia de datos entre dispositivos u objetos tecnológicos articulados mediante una red.

RESUMEN EMPRESAS ANÁLIZADAS PARA SEGURIDAD EN INTERNET DE LAS COSAS

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
Bastille SECURITY FOR THE INTERNET OF RADIOS http://www.bastille.net/	USA	2014	● ●	0	39.000.000
sparkcognition™ sparkcognition.com	USA	2013	● ● ●	5	38.870.000
CUJOAI http://www.cujo.com/platform	USA	2015	● ●	3	51.923



- Predicciones de fallas de equipos
- Detección avanzadas contra vulnerabilidades inalámbricas
- SaaS Defense IA

SOLUCIONES

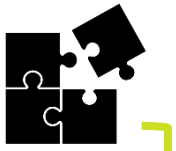
OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

PROBLEMAS

- Amenazas y vulneraciones de la información transmitida a través de redes inalámbricas y de infraestructuras para *IoT*.
- Perdidas de información sensible por ataques cibernéticos.
- Vulnerabilidad de los dispositivos conectados.
- Vulnerabilidad de los dispositivos móviles y portátiles por amenazas en línea como piratería, phishing o malware.
- Incertidumbre ante las fallas que puede presentar un equipo.

SOLUCIONES



Predicciones de fallas de equipos: predicción de posibles fallos mediante el análisis y aprendizaje de los datos de sensores instalados en los equipos, permitiendo generar ahorros asociados a dichos fallos.

Detección avanzadas contra vulnerabilidades inalámbricas: detección y seguridad avanzada contra las principales vulnerabilidades y amenazas conocidas y desconocidas generadas por conexiones inalámbricas en dispositivos y equipos IoT.

Software como servicios para defensa con IA: software como servicios de defensa con inteligencia artificial, para brindar seguridad en la red, inteligencia de dispositivos y controles parentales semánticos.

ADOPTANTES TEMPRANOS

- **Sector de soluciones energéticas**: *Dover Energy Automation, Invenergy, LLC.*
- **Productos de consumo**: *Honeywell, Flowserve.*
- **Gobierno**: *Defense Innovation Unix Experimental (DIUx).*
- **Aeronáutico**: *Boeing.*
- **Telecomunicaciones y medios digitales**: *TechCrunch, Yahoo Finance, Silicon Republic, TheHuffingtonPost.co.uk.*

CANALES

Comunicación: *Twitter, Facebook, YouTube, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

- **E-mail, teléfono**: contacto directo con los clientes.
- **WebSite**: publicación general de la compañía.
- **Blog**: publicación de noticias de actualidad como de desarrollo tecnológico, artículos sobre temas alrededor del internet de las cosas, noticias relacionadas con los productos y servicios que ofrece la compañía.
- **Webinars**: seminarios web sobre temas relacionados con tecnologías aplicadas a los sectores de petróleo y gas, energía eólica y seguridad cibernética, sobre tecnologías revolucionarias como el aprendizaje automático.

Pago: pago online por medio de tarjeta débito y crédito.

Compra: online a través del sitio web.

RECURSOS CLAVE

Tecnológicos:

Algoritmos de predicción y clasificación y filtración: Recopila datos de los sensores de los equipos; los transforma y aplica algoritmos de predicción y clasificación, generando ideas de acciones que se deban tomar, dando información para el análisis de las fallas.

Plataformas, SaaS IA: Plataformas y SaaS apoyadas de IA para ofrece visibilidad completa y prevención avanzada de riegos, amenazas y ciberataques en la infraestructura de la red en dispositivos y equipos *IoT*.

Algoritmo de aprendizaje automático profundo: Se emplean para extraer, analizar y puntuar las características de los archivos para la detección de archivos maliciosos.

Paquete tecnológicos

- **Analítica y ciencias de datos:** *Google Analytics, Hotjar, Parse Core*.
- **Devops y IT:** *GoDaddy DNS, software Apache Traffic Server, New Relic, WordFence*.
- **Marketing:** *AddThis, Salesforce Pardot, HubSpot* .
- **Desarrollador:** *API de Flickr, Lightbox, Select2*.
- **Producto y diseño:** *Google Fonts, GreenSock Animation Platform, Squarespace*.
- **Productividad y operaciones:** *Slack, Siftery Discover, Google Apps for Work*.
- **HR:** *JazzHR, Lever*.
- **Venta y BD:** *Clearbit, OptinMonster, Salesforce Sales Cloud.*

- **Humanos**: Ingenieros de sistemas, desarrolladores web y software, especialistas en análisis y procesamiento de datos, científicos de datos, ciencias computacionales.
- **Conocimientos** en integración de *R / C*, en lenguajes *scripting como Python, JavaScript, PHP o Perl, Shell, Bash, C++, C.*
- **Experiencia** en aprendizaje automático, como *PyTorch, TensorFlow, Thean*; en desarrollo de bases de datos HTTP, JSON, REST; con el desarrollo de algoritmos en un entorno distribuido, como *Hadoop, Spark* o un entorno *MPP*, usando *SQL, PL / SQL, TSQL* y otras técnicas de *scripting.*

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD EN INTERNET DE LAS COSAS

PROPUESTA Y ATRIBUTOS DE VALOR

- Optimización de activos ciber físicos (sistema físico controlado por algoritmos integrados con internet), apoyados de aprendizaje automático como herramienta de Inteligencia Artificial.
- Soluciones integrales para el hogar y proveedores de servicios de Internet.
- Conexión confiable y con minimización de amenazas cibernéticas o ataques a la estructura de la red en los dispositivos y equipos *IoT*.
- Alertas sobre fallas tempranas antes de que ocurran, mejorando los tiempo de reacción y costos de paradas no programadas.

FUENTES DE INGRESO

- **Suscripción *Freemium*:** versión gratuita.
- **Suscripción *Premium***: paquetes de pago mensual que varían de acuerdo a la capacidad de almacenamiento.
- **Soporte técnico**: servicio de soporte técnico personalizado.
- **Programa afiliados**: clientes comisionistas que promuevan los productos y servicios.

INVERSIONISTAS

- *Sequoia Capital*
- *Salesforce Ventures*
- *Battery Venturea*
- *Silicon Valley Bank*
- *Bain Capital Ventures*
- *Insight Ventures Partners*
- *Index Ventures*

ALIADOS CLAVE

Aliados tecnológicos

- **IBM**: Servicios en la nube y tecnologías de la información.
- **Google:** Red publicitaria, Software empresarial, tecnologías de la información.
- **National Instruments**: Productos de medición y automatización
- **General Electric**: infraestructura y servicios financieros
- **Verizon**: tecnologías de la información, servicios móviles.

Aliados comerciales y publicitarios

- ***Fast Company*:** medios de negocios y publicidad.

MÉTRICAS CLAVE

- Número de amenazas detectadas.
- Número de amenazas bloqueadas.
- Porcentaje de detección de fallas tempranas.
- Porcentaje de reducción de tiempos de acción ante amenazas.
- Porcentaje de ahorro en costos por detección de acciones fraudulentas.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - SEGURIDAD EN INTERNET DE LAS COSAS

	Número de Patentes	Descripción de las Patentes	Geografías de protección
sparkcognition™	5	Se proporciona un sistema y método para generar una heurística que es capaz de identificar patrones de datos, incluye extraer los datos de múltiples fuentes, asignar atributos, identificar tendencias. Ello genera una huella digital cognitiva. Otra de las invenciones proporciona un sistema para predecir el tiempo útil de componentes mecánicos tales como rodamientos.	• USA • PCT[1] • EP[2]
CUJOAI	3	Las invenciones hacen referencia a métodos y sistemas desarrollados para detectar el comportamiento malicioso de los dispositivos inteligentes dentro de una red.	• USA • PCT[1]

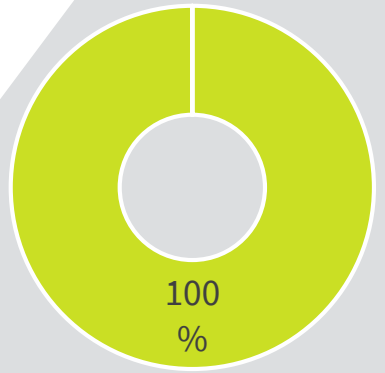
1. PCT, es un tratado internacional ratificado por más de 150 Estados contratantes. Con el PCT puede solicitar la protección de una invención por patente mediante la presentación de una única solicitud "internacional" de patente en un gran número de países, sin necesidad de cursar por separado varias solicitudes de patente nacionales o regionales.
2. EP. El sistema de patente europea permite obtener protección mediante una solicitud de patente europea directa con designación en aquellos Estados europeos en que se quiere obtener protección y sean parte del Convenio Europeo de Patentes. Así, se puede obtener protección en hasta 38 países del ámbito europeo.

SEGURIDAD DE APLICACIONES MÓVILES

Enfoques de seguridad que se llevan a cabo para prevenir ataques y reducir la probabilidad de instalar aplicaciones maliciosas, proporcionando las herramientas necesarias para la toma de decisiones seguras e informadas durante el proceso de selección y manejo de una aplicación.

RESUMEN EMPRESAS ANÁLIZADAS PARA SEGURIDAD EN APLICACIONES MÓVILES

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
Cryptosense (cryptosense.com\)	Francia	2013	Detección profunda de ciberataques	0	700.000
CYBER 20/20 (http://www.cyber2020.com/)	USA	2016	Detección profunda de ciberataques	0	162.786
AUTHBASE (http://www.authbase.net/)	India	2016	Detección profunda de ciberataques	0	101.142



Detección profunda de ciberataques

SOLUCIONES

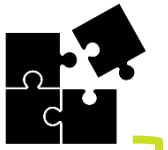
OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

PROBLEMAS

- Pérdida de datos por los ataques del ciberentorno.
- Es difícil detectar y solucionar fallas de seguridad relacionadas con el uso de la criptografía en las aplicaciones.
- Amenazas de la red por malware.
- Aumento de tasas de falsos positivos en el análisis de actividades maliciosas.

SOLUCIONES



Detección profunda de ciber ataques: aplica IA con avanzados algoritmos de aprendizaje automático, para detectar, corregir y solucionar fallas asociadas a la seguridad de cifrado y vulnerabilidades de las Apps.

Permite realizar pruebas de penetración, probando la red y su infraestructura en busca de vulnerabilidades.

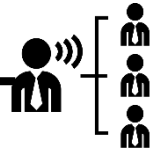
Apoyo a los clientes en el diseño de arquitecturas de red seguras, realizando verificación de códigos y solucionando posibles vulnerabilidades.

Combinación del aprendizaje automático profundo, la caracterización de malware de última generación y la computación de alto rendimiento para proporcionar un motor de detección de malware de alta precisión.

ADOPTANTES TEMPRANOS

- *E-Commerce*.
- Sector de desarrollo de App móviles.
- Sector financiero.
- Sector seguros.
- Sector salud.

CANALES



Comunicación: *Twitter, Facebook, YouTube, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

- ***E-mail*, teléfono**: contacto directo con los clientes
- ***WebSite***: publicaciones en general de la compañía.

Pago: pago online por medio de tarjeta débito y crédito.

Compra: online a través del sitio web.

RECURSOS CLAVE

Tecnológicos: plataforma que combina el Big Data y algoritmos avanzados de aprendizaje automático profundo para corregir todo tipo de vulnerabilidades y problemas de configuración de las Apps, así como de detección de malware con mayor precisión.

Paquete tecnológico

- **Analítica y ciencias de datos:** *LeadLander, Google Analytics*.
- **Desarrollador:** *HTML5, PHP, Modernizr, jQuery.*
- **Producto y diseño:** *Google Fonts*.
- **Devops IT:** *Apache, GeoTrust SSL, Caché total W3.*
- **Marketing:** *Facebook Login, LinkedIn, MailChimp, Google Sign-In. OneAll.*
- **Atención y éxito al cliente:** *Aircall.*

Humanos: Ingenieros de sistemas, desarrolladores web y software, especialistas en analítica de datos, ciencias computacionales, matemáticas, científicos de datos, expertos en seguridad e IA.

- **Conocimientos** lenguajes scripting como *Java*.
- **Experiencia** en Seguridad de aplicaciones, *IASP*, seguridad de *Java*, seguridad *OpenSSL, ocaml* y *Secure Devops.*

PROPUESTA Y ATRIBUTOS DE VALOR

- Protección de aplicaciones por medio de soluciones de última tecnología.
- Detectar, reparar y monitorear la web, dispositivos y aplicaciones móviles y redes contra vulnerabilidades, a través de algoritmos de aprendizaje automático.
- Las tecnologías aprovechan los avanzados algoritmos de aprendizaje automático acelerados con computación de alto rendimiento para analizar grandes cantidades de malware y obtener una detección alta y una baja tasa de falsos positivos.

FUENTES DE INGRESO

- **Suscripción *Freemium*:** versión gratuita.
- **Suscripción *Premium***: paquetes de pago mensual que varían de acuerdo a la capacidad de almacenamiento.
- **Socios**: estrategia para escalar sus productos y servicios y obtener ingresos.
- **Cursos de formación**: cursos de capacitación sobre identificación y evaluación de fallas criptográficas en aplicaciones e infraestructura.

INSIGHTS MODELO DE NEGOCIO - SEGURIDAD DE APLICACIONES MÓVILES

INVERSIONISTAS

- *Elaia Partners*

ALIADOS CLAVE

Aliados tecnológicos

- ***Tensorflow***: biblioteca de software de código abierto.
- ***Amazon Web Service AWS*:** servicios de información, tecnología de la información, desarrollo web.
- ***sCikit learn*:** proporciona una biblioteca de aprendizaje de máquina de código abierto para el lenguaje de programación *Python*.
- ***NASSCOM*:** servicios de información y Tecnologías de la Información.

Aliados comerciales

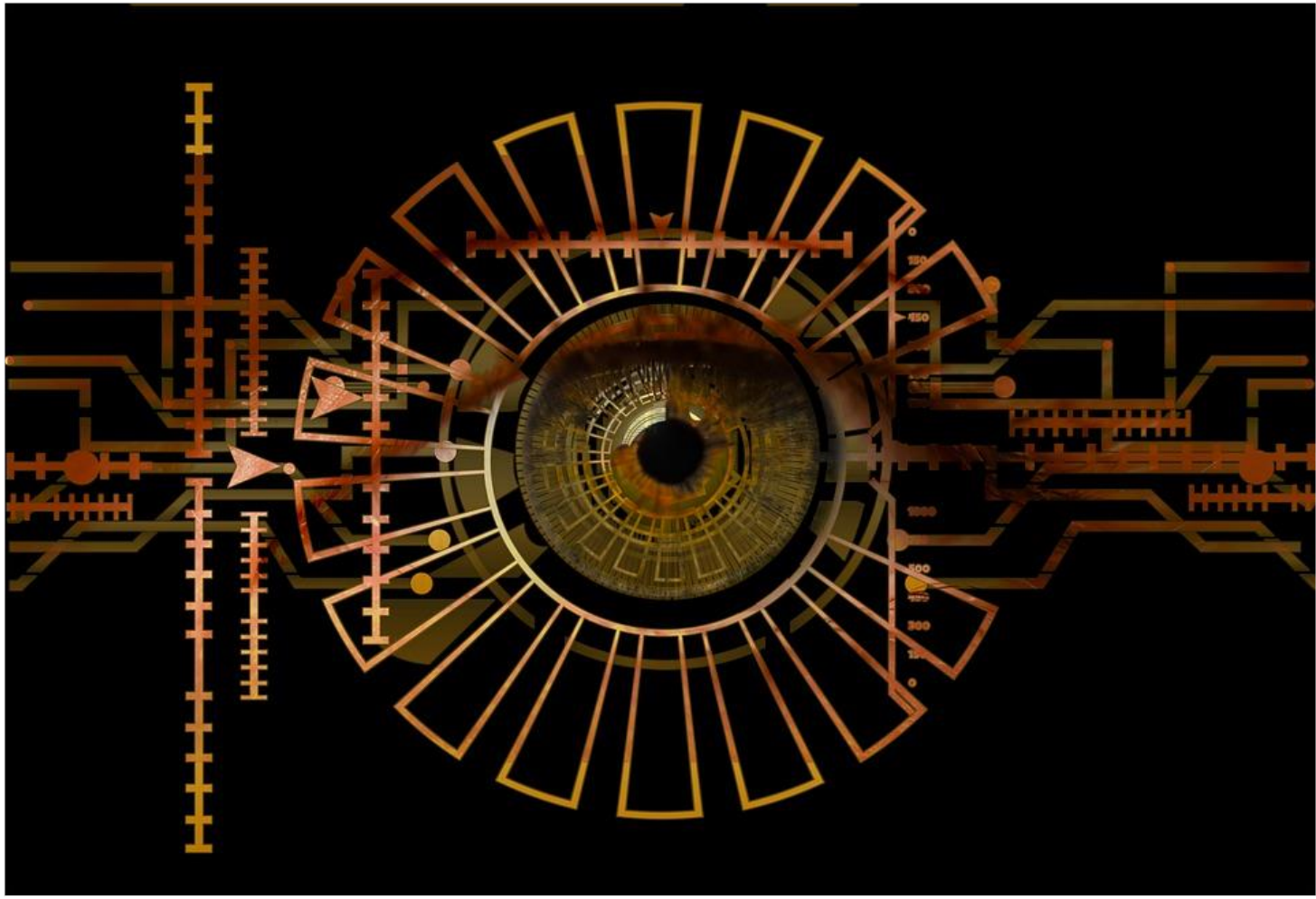
- ***Spark*:** Publicidad, marketing en redes sociales.

MÉTRICAS CLAVE

- Reducción del porcentaje de falsos positivos.
- Incremento en el porcentaje de detección de anomalías.
- Número de malware detectados.
- Porcentaje de reparación de vulnerabilidades.

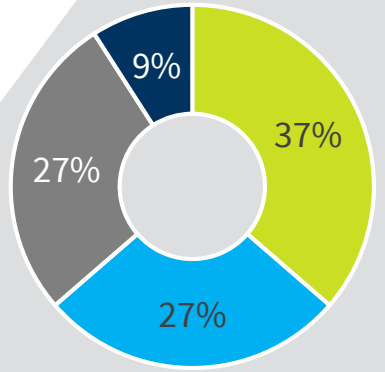
INTELIGENCIA PREDICTIVA

Consiste en modelos de razonamientos y mecanismos de aprendizaje automático e inteligencia artificial, empleados para aplicar inferencia frente a eventos en tiempo real, detectar eficientemente patrones de comportamiento con base a datos actuales e históricos e identificar riesgos y oportunidades [17].



RESUMEN EMPRESAS ANÁLIZADAS PARA INTELIGENCIA PREDICTIVA

Empresa	Lugar de Origén	Año de Fundación	Producto o Servicio	Familias de Patentes	inversión en Dólares
LogRhythm logrhythm.com	Reino Unido	2003	● ● ●	2	126.250.948
ANOMALI http://www.anomali.com/	USA	2013	● ● ●	1	56.300.000
deepinstinct http://www.deepinstinct.com/	Israel	2014	● ● ●	1	32.000.000
JASK http://www.jask.ai/	USA	2015	● ● ●	0	14.000.000
indeni http://www.indeni.com/	USA	2009	● ● ●	1	10.000.000
PROTENUS http://www.protenus.com/	USA	2014	● ● ●	0	8.400.000
patternex patternex.com\	USA	2013	●	2	7.800.000
SECBI http://www.secbi.com/	Israel	2014	●	2	5.000.000
splunk> https://www.splunk.com/	USA	2013	●	1	1.300.000
SECLYTICS http://www.seclytics.com/	USA	2014	●	0	109.727



- Aprendizaje automático profundo
- Investigación forense
- Protección avanzada de usuario
- Plataforma de análisis de datos e inteligencia predictiva

SOLUCIONES

OBSERVATORIO CT+i

La información del modelo de negocio para cada *startup* se encuentra en el informe Anexo

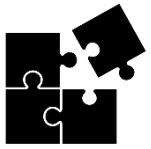
Contenido

INSIGHTS MODELO DE NEGOCIO - INTELIGENCIA PREDICTIVA

PROBLEMAS

- Riesgos y amenazas de filtración de datos en los dispositivos por el uso de aplicaciones vulnerables.
- Aumento de amenazas en la red o *Endpoints* por *softwares* maliciosos.
- Falta de gestión, control y prevención de las amenazas cibernéticas.
- Amenazas por el robo de contraseñas a través de la red.
- Riesgos por ataques de *phishing*.

SOLUCIONES



Aprendizaje cibernético profundo: aplican el aprendizaje profundo a la seguridad cibernética que permite obtener una protección de ataques de día cero en dispositivos móviles y *endpoints*.

Investigación forense: soluciones que implican velocidad en el descubrimiento, análisis y priorización de amenazas, proporcionando el conocimiento necesario a los analistas de seguridad para la prevención y eliminación de riesgos y amenazas.

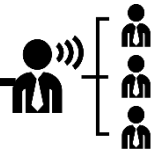
Protección avanzada de usuario: se basan en IA para el seguimiento, control y protección de los datos del usuario, generando alertas contra actividades sospechosas en el registro electrónico.

Plataforma de análisis de datos e inteligencia predictiva: tecnología que desarrolla inteligencia operativa para supervisar, informar y analizar datos en tiempo real que permitan identificar los cambios en la infraestructura de Internet, identificar las actividades sospechosas de los ciberdelincuentes y predecir futuros ataques antes de su lanzamiento.

ADOPTANTES TEMPRANOS

- **Sector financiero**: *Equifax, ING Bank, Financial Service Company.*
- **Telecomunicaciones**: *Orange, CenturyLink, Telenor.*
- **Sector salud**: *BOSHC, CardianalHealth, Cerner.*
- **Educación**: *Bayolar University, University Duke.*
- **Tecnología**: *Adobe, analyticsMD, Autodesk, Atlassian.*
- **Retail**: *Cocacola, Dominos, Eleven 7.*
- **Medios y entretenimiento**: *Amaya, Discovery Comunications, Nexon*.
- **Viajes y transporte**: *Aurizon, Etravel, Instacab.*

CANALES



Comunicación: *Twitter, Facebook, YouTube, LikedIn*: publicación de campañas publicitarias, noticias, información acerca de la compañía, así como contacto directo con los clientes.

- ***E-mail*, teléfono**: contacto directo con los clientes.
- ***WebSite***: publicaciones en general de la compañía.

Pago: pago online por medio de tarjeta débito y crédito.

Compra: *online* a través de la pagina web.

RECURSOS CLAVE

Tecnológicos:

Plataformas y software: que proporcionan inteligencia profunda a los analistas de seguridad para prevenir, detectar anomalías y tráficos en la red, resolver actividades sospechosas y mitigar los riesgos de violación de la privacidad de los datos de los usuarios.

Paquete tecnológico:

- ***Devops y IT*: *Amazon S3, Disqus, Salesforce App Cloud, TRUSTe*.
- **Desarrollador**: *Adobe Flash, Algolia, Bold Commerce*.
- **Productividad y operaciones**: *Egnyte, LifeSize, Teem*.
- **Analítica y ciencias de datos**: *Google Analytics*.
- **Marketing**: *SendGrid, RadiumOne Po.st, TechValidate*.
- **Atención y éxito al cliente**: *ConnectAndSell, Lithium, LivePerson*.
- **HR**: *Greenhouse.*
- **Ventas y BD**: *Akkroo, Aviso , CommercialTribe.*

Humanos: Ciencias computacionales, expertos en ciberseguridad, ingeniería de software, desarrolladores web y de software, científicos de datos.

- **Conocimientos** en lenguajes de programación como: *Python, Java, C, C++, Ruby, Go, Scala, JavaScript*; Modelado predictivo y análisis de algoritmos y estructuras de datos.
- **Experiencia** en tecnologías de bases de datos *NoSQL, ElasticSearch, Cassandra, MongoDB*; plataformas y tecnologías de *big data, (Hadoop, Spark)*.
- **Certificación** *SFDC*

INSIGHTS MODELO DE NEGOCIO - INTELIGENCIA PREDICTIVA

PROPUESTA Y ATRIBUTOS DE VALOR

- Uso de Inteligencia Artificial avanzada para análisis forense profundo.
- Detección, prevención y protección en tiempo real de las amenazas de día cero y ataques APT (Amenazas Persistentes Avanzadas) en toda la infraestructura de red y dispositivos móviles de la organización.
- Integraciones con soluciones de TI que permiten a las organizaciones entregar inteligencia de amenazas optimizada directamente en *SIEM, firewalls*, soluciones de punto final y otros sistemas.

FUENTES DE INGRESO

1. Suscripción

La suscripción se realiza para que los clientes y público en general, puedan obtener en la versión paga, los planes y servicios relacionados con los productos de las compañías. Estos planes incluye:

- Plataformas de defensa
- *SaaS* de defensa
- Motores de análisis de vulnerabilidades
- Soporte técnico y profesional

2. Socios: socio channel partner para la reventa de la plataforma.

3. Foros online: foros con expertos en ciberseguridad donde reciben pago de inscripción de los participantes.

INVERSIONISTAS

- *General Catalyst Partners GV*
- *Battery Ventures*
- *Dell Technologies Capital*
- *Blumberg Capital*
- *Sequoia Capital*
- *Orange Digital Ventures*

INSIGHTS MODELO DE NEGOCIO - INTELIGENCIA PREDICTIVA

ALIADOS CLAVE

Aliados tecnológicos

- ***Bayer Impact***: equipos de ciencia de datos.
- ***Glide***: electrónica de consumo, IoT, seguridad de cámaras.

Aliados comerciales y publicitarios

- ***StudentRND***: servicios de publicitarios y de reclutamiento.
- ***Infoxchange***: repositorio en línea de información.
- ***NetHope***: consultorías y asesorías en el desarrollo de TI.

MÉTRICAS CLAVE

- Número de amenazas detectadas.
- Número de amenazas bloqueadas.
- Número de amenazas resueltas.
- Número de alertas notificadas al día.
- Porcentaje de prevención de amenazas.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - INTELIGENCIA PREDICTIVA

	Número de Patentes	Descripción de las Patentes	Geografías de protección
LogRhythm	2	Comprende un motor de inteligencia avanzada para identificar eventos o desarrollos complejos en una plataforma de datos, incluye datos estructurados o normalizados.	• USA
ANOMALI	1	La invención se refiere a un método inteligente empleado para la detección de amenazas de eventos en una red desde el día cero.	• USA
deepinstinct	1	Método utilizado para entrenar un sistema para el análisis del tráfico de datos, comprendiendo el sistema un algoritmo de aprendizaje profundo, en el que comprende un modelo de predicción que está entrenado para tener en cuenta el historial de datos.	• USA • PCT[1]

1. PCT, es un tratado internacional ratificado por más de 150 Estados contratantes. Con el PCT puede solicitar la protección de una invención por patente mediante la presentación de una única solicitud “internacional” de patente en un gran número de países, sin necesidad de cursar por separado varias solicitudes de patente nacionales o regionales.

DESARROLLOS TECNOLÓGICOS ASOCIADOS - INTELIGENCIA PREDICTIVA

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	La invención se refiere en general al campo de los componentes de seguridad de red, que emplea un aparato para la identificación y monitorización del estado de los componentes en una red basado en sistemas de seguridad.	• USA

Número de Patentes	Descripción de las Patentes	Geografías de protección
2	Estas invenciones se refieren a procesos, métodos y sistemas para entrenar una máquina de Big Data y recuperar líneas de registros, además, aplicar modelos de reglas adaptativas para identificar y detectar amenazas en empresas de comercio electrónico.	• USA

DESARROLLOS TECNOLÓGICOS ASOCIADOS - INTELIGENCIA PREDICTIVA

Número de Patentes	Descripción de las Patentes	Geografías de protección
2	Las invenciones se relacionan con métodos y aparatos para detectar y responder a la presencia de *malware* y a la autenticación de usuario a través del análisis de datos.	• USA

Número de Patentes	Descripción de las Patentes	Geografías de protección
1	La invención se refiere a un método utilizado para clasificar información a través de una red usando una computadora que incluye uno o más procesadores de *hardware*, donde cada acción del método es realizada por el uno o más procesadores.	• USA

PARA TENER EN CUENTA

- Las soluciones en ciberseguridad continúan evolucionando, incluyendo herramientas de análisis como inteligencia artificial y de algunos de sus componentes como el aprendizaje automático (*Machine Learning*) y el Procesamiento de Lenguaje Natural (NLP), para mejorar la protección. **Es necesario generar soluciones mas robustas que eviten los múltiples ataques cibernéticos a los cuales se enfrentan diariamente la empresa**s. Ello se evidencia con las grandes pérdidas económicas generadas anualmente por ciberataques.
- Se evidencian modelos de negocios exitosos en el mundo, que han permitido a las organizaciones que se preocupan por los riesgos y vulnerabilidades inherentes a sus procesos, **minimizar las amenazas y proteger su información**.
- **Los fraudes y usos inadecuados de los productos y servicios, como falsificaciones o robo de identidad**, no solamente generan perdidas económicas sino que adicionalmente crean una imagen negativa de la marca.
- Los sectores **financiero, de seguros, gubernamental y el sector salud**, son los más vulnerables a ciber ataques.
- A medida que avanza la tecnología para la protección de los riesgos y amenazas cibernéticas, **los ciberdelincuentes también desarrollan mecanismos avanzados para aprovecharse de vulnerabilidades de las estructuras de red,** haciendo necesarios mecanismos de protección mas robustos.
- Las *Startup* analizadas, emplean la **suscripción *Freemium* como forma de atraer y fidelizar a los clientes**, para posteriormente ofrecer suscripción *Premium*. Cuentan con una **red de socios comerciales que sirven como canal** para llevar los productos y servicios a nuevos clientes y adicionalmente ofrecen **servicios profesionales y de capacitación a los clientes**, relacionados con la tecnología que implementan.

CAPACIDADES LOCALES

En este capitulo se realiza la identificación de la situación actual de Medellín desde el ámbito social, tecnológico y político, con el fin de identificar las dinámicas y capacidades locales en relación al área de oportunidad.

DESDE LO TECNOLÓGICO

Oferta de productos y servicios en el Valle de Aburrá

- Seguridad y administración de endpoints.
- Monitorear actividades en internet para detectar patrones peligrosos.
- Hacking ético, análisis de puntos débiles.
- Seguridad biométrica.
- Protección y recuperación de datos ante desastres.
- Investigación digital forense

Algunas Compañías con oferta de soluciones o servicios en Ciberseguridad.

Algunos grupos de investigación con oferta de soluciones o servicios en Ciberseguridad.

ENTIDADES	DESCRIPCIÓN
Universidad Pontificia Bolivariana	**Grupo de Investigación** Desarrollo y Aplicación en Telecomunicaciones e Informática **GIDATI** **GIDATI:** desarrolla, diseña, evalúa y recomienda sobre metodologías y tecnologías para facilitar la comunicación entre personas y dispositivos en infraestructura de telecomunicaciones, enfocado en tecnologías de comunicaciones ópticas e inalámbricas. También, desarrolla e implementa aplicaciones, contenidos digitales y sistemas de seguridad de la información y analiza datos para extraer y procesar información, mediante metodologías genéricas de desarrollo de software y técnicas especializadas de minería de datos. **Líneas de investigación** • Acceso inalámbrico. • Ciudades inteligentes. • Contenidos digitales. • Redes y comunicaciones ópticas.

Contenido

Algunas instituciones con oferta de formación relacionada con Ciberseguridad

DESDE LA FORMACIÓN

ENTIDADES	DESCRIPCIÓN
ITM Institución Universitaria Acreditada en Alta Calidad	**Modalidad Posgrado** Ofrece la **Maestría en Seguridad Informática** y tiene como misión la generación de propuestas, modelos, estrategias y soluciones tecnológicas en ciber-defensa y ciber-seguridad. El objeto de la formación se basa en crear perfiles profesionales para la solución de problemas en Seguridad Informática con énfasis en gestión de incidentes de seguridad de la información. Esta dirigida a Ingenieros Informáticos, Sistemas, Telecomunicaciones, Auditores de Sistemas y a fines.
Corporación Universitaria Americana Institución Universitaria®	En respuesta a la creciente demanda de control y supervisión que plantean los nuevos y cada vez más complejos sistemas informáticos, en sus usos públicos, privados, empresariales y personales, la Corporación Universitaria Americana ofrece la **Especialización en Seguridad Informática**, teniendo en cuenta el gran impacto de esta formación sobre las Amenazas Persistentes Avanzadas (APT), los hacktivistas (utilización no violenta de herramientas digitales) y sobre otras formas sofisticadas de amenazas electrónicas recientes. El especialista en Seguridad Informática estará en capacidad de: • Definir políticas de seguridad en las organizaciones. • Definir los procedimientos para aplicar la política de seguridad informática. • Diseñar sistemas informáticos teniendo en cuenta las características de seguridad necesarias. • Realizar análisis de vulnerabilidades y test de penetración a los sistemas informáticos de las organizaciones. • Llevar a cabo análisis forense sobre la evidencia digital, luego de la ocurrencia de un incidente. • Definir la misión de seguridad informática de la organización en conjunto con las autoridades de la misma. • Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la organización.

DESDE LA FORMACIÓN

Algunas instituciones con oferta de formación relacionada con Ciberseguridad

ENTIDADES	DESCRIPCIÓN
UNIVERSIDAD DE SAN BUENAVENTURA MEDELLÍN	**Modalidad Posgrado** Ofrece la **especialización en Seguridad Informática** con el objetivo de dar solución a la necesidad existente sobre la gestión de la seguridad de la información, teniendo como precedente las amenazas y vulnerabilidades que se presentan en los sistemas informáticos de las organizaciones. Dirigida a Ingenieros de sistemas, ingenieros electrónicos, ingenieros informáticos, ingenieros telemáticos y profesionales de otras disciplinas que acrediten experiencia en el área de informática.
Universidad Pontificia Bolivariana	**Grupo de Investigación** Desarrollo y Aplicación en Telecomunicaciones e Informática **GIDATI** **GIDATI:** desarrolla, diseña, evalúa y recomienda sobre metodologías y tecnologías para facilitar la comunicación entre personas y dispositivos en infraestructura de telecomunicaciones, enfocado en tecnologías de comunicaciones ópticas e inalámbricas. También, desarrolla e implementa aplicaciones, contenidos digitales y sistemas de seguridad de la información y analiza datos para extraer y procesar información, mediante metodologías genéricas de desarrollo de software y técnicas especializadas de minería de datos. **Líneas de investigación** • Acceso inalámbrico. • Ciudades inteligentes. • Contenidos digitales. • Redes y comunicaciones ópticas.

Algunas iniciativas políticas asociadas con Ciberseguridad

DESDE LO POLÍTICO

ENTIDADES	DESCRIPCIÓN
	El **CAI VIRTUAL** de la Policía Nacional de Colombia, es la primera iniciativa iberoamericana en atención policial en línea, donde se pueden reportar delitos informáticos, realizar análisis de Malware, encontrar recomendaciones de ciberseguridad, visualización en tiempo real de los incidentes informáticos que afectan la ciberseguridad nacional, entre otros servicios y usos.
	Es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

OPORTUNIDADES

En este capítulo se identifican oportunidades y brechas para el área de interés, considerando aspectos como capacidad requerida, segmento de clientes y barreras.

METODOLOGÍA DE IDENTIFICACIÓN Y PRIORIZACIÓN DE OPORTUNIDADES

Definición de potenciales oportunidades para Medellín a partir de la oferta de soluciones globales y locales. La identificación de las potenciales oportunidades se realiza considerando las soluciones globales para las cuales no se identifica actualmente oferta en Medellín, o aquellas que a partir del estudio se identifican como necesidades para la ciudad. Estas soluciones son potenciales oportunidades de innovación para la ciudad.

Taller de priorización de oportunidades. Las potenciales oportunidades identificadas son priorizadas y analizadas en un taller con grupos de interés, en los cuales se realiza una calificación de cada potencial oportunidad, considerando variables de mercado y capacidades locales para su implementación. Las variables consideradas son:

Mercado

- Necesidad del mercado
- Beneficios de la solución
- Disposición de compra
- Productos complementarios
- Adopción del mercado

Capacidades

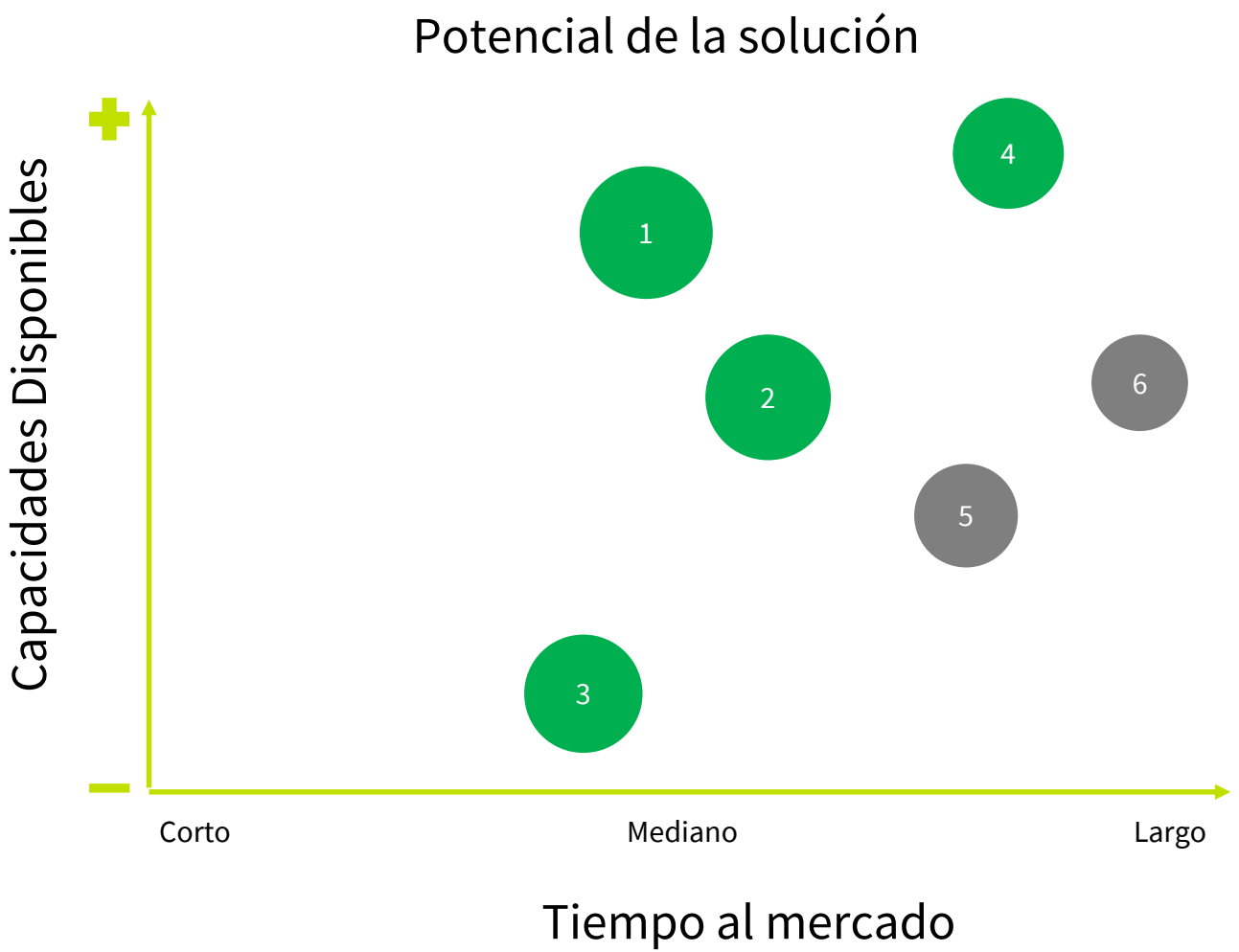
- Recursos humanos
- Infraestructura
- Capacidad de financiación
- Cadena de valor

Identificación de oportunidades para la ciudad. A partir de la evaluación en los grupos de interés, se identifican las cinco oportunidades que tengan mayor potencial, puesto que se pueden implementar en un corto plazo y se cuenta con la capacidades a nivel local, necesarias para su implementación. Para estas oportunidades se definen en este capitulo los potenciales clientes, capacidades requeridas para su implementación y brechas.

ASISTENTES AL TALLER DE OPORTUNIDADES

Tanque de pensamiento en TIC Colombia	Ramiro Paniagua (Asesor)
Colombia inteligente	Juan David Molina
csiete	Carlos Fernández
FLUID SECURITY WITHOUT MYSTERY	Rafael Álvarez

POTENCIALES OPORTUNIDADES PARA MEDELLÍN



El tamaño de la burbuja representa el potencial de la oportunidad y se calcula con la sumatoria entre la puntuación de las capacidades y del mercado.

Oportunidades priorizadas

1. Plataforma de identidad digital
2. Sistema de seguridad para el perfilamiento del comportamiento de usuarios y/o entidades
3. Sistema de detección de amenazas
4. Sistema para la detección de vulnerabilidades en la lógica de programación o desde el diseño del dispositivo
5. Sistema de detección avanzadas contra vulnerabilidades inalámbricas o sistemas embebidos
6. Sistema de respuesta especializados a riesgos

* Se sugiere priorizar una oportunidad adicional relacionada con centros de entrenamiento en temas de ciberseguridad.

OBSERVATORIO CT+i

1. Plataforma de identidad digital

Segmentos de clientes

Entidades financieras

Oferta hacia los clientes

Evitar el fraude y el robo de identidades en transacciones multicanal para entidades financieras, a través de plataforma de identidad digital con reconocimiento inteligente de los usuarios, empleando Inteligencia Artificial, herramientas de procesamiento de lenguaje natural y análisis de información no estructurada para prevenir vulneraciones y fraudes.

¿Por qué es una oportunidad?

- Permite mayor seguridad de los usuarios a la hora de realizar transacciones en línea.
- Altas pérdidas de dinero ocasionadas por ataques y fraudes cibernéticos.
- La seguridad aumenta la credibilidad de los servicios que ofrecen la compañías.
- Se requieren herramientas que generen confianza en los usuarios al realizar transacciones electrónicas, incentivando así su uso.

Capacidades requeridas

- Personal con conocimientos y experiencia en ciberseguridad, analítica de datos, procesamiento de imágenes, vídeos y texto.
- Desarrollo o adquisición de tecnología (hardware y software biométrico) para la captura, almacenamiento y procesamiento de datos.
- Realización de ensayos y pilotos validados de las soluciones desarrolladas.

Brechas/ Barreras

- Carencia de normatividad y/o regulación necesaria para implementar la solución.
- Falta de estandarización a nivel internacional sobre temas relacionados con ciberseguridad.
- Desconocimiento de los directivos de las compañías acerca de las ventajas de implementar la tecnología.
- Desconfianza en desarrollos locales.

2. Sistema para perfilamiento del comportamiento de usuarios y/o entidades

Segmentos de clientes

Entidades financieras

entidades gubernamentales

sector salud

servicios públicos, comercio electrónico

Oferta hacia los clientes

Detección y prevención efectiva de amenazas por medio de un sistema que correlaciona la actividad de usuarios y de entidades (endpoints, dispositivos móviles, redes locales, entre otros) por medio del aprendizaje automático, identificando comportamientos atípicos que pueden representar vulneraciones a la seguridad y posibles fraudes.

¿Por qué es una oportunidad?

- El perfilamiento del comportamiento de usuarios y/o entidades es un sistema que correlaciona actividad de estos para detectar de manera efectiva y temprana todo tipo de amenazas cibernéticas.
- El gran volumen de transacciones electrónicas entre personas y dispositivos (incluyendo el internet de las cosas), dificulta la identificación de amenazas, este tipo de soluciones facilitan su detección.
- Perdidas económicas generadas por fraudes cibernéticos.

Capacidades requeridas

- Personal capacitado en temas de seguridad avanzada, ciencias de la computación, expertos en seguridad en la nube, desarrolladores de software y aplicaciones web.
- Hardware para el almacenamiento y procesamiento de grandes volúmenes de datos.
- Software de reconocimiento biométrico y facial.

Brechas/ Barreras

- Carencia de normatividad y/o regulación necesaria para implementar la solución.
- Falta de estandarización a nivel internacional sobre temas relacionados con ciberseguridad.

3. Sistema de detección de amenazas a la seguridad

Segmentos de clientes

Oferta hacia los clientes

Sistema para la identificación de amenazas, tanto físicas como informáticas, a partir del análisis de información disponible como los sistemas de vigilancia públicos, información en redes sociales entre otros, para detectar el comportamiento de las personas y alteraciones en los patrones normales que pueden representar amenazas en la seguridad.

¿Por qué es una oportunidad?

- Mayor control de las condiciones de seguridad de los ciudadanos, especialmente en eventos de difícil contención que implican concentración de gran número de personas como conciertos, deportes, eventos culturales.
- Permite reducir los impactos ocasionados por las vulneraciones a la seguridad tanto informática como ciudadana y a nivel personal.
- Habilitan la investigación efectiva en eventos que generen alteraciones de la seguridad.
- Puede ser una opción para minimizar la violencia, ya que permite un mayor control de las condiciones de seguridad.

Capacidades requeridas

- Desarrollo o adquisición de tecnología (hardware y software) para la captura, almacenamiento y procesamiento de datos.
- Personal con conocimientos y experiencia en ciberseguridad, analítica de datos, procesamiento de imágenes y vídeos.

Brechas/ Barreras

- Altas inversiones requeridas para implementar la solución.
- Falta de regulación legal en el tratamiento de los datos y la sostenibilidad de los mismos frente a un delito.

4. Detección de vulnerabilidades en la programación o desde el diseño del dispositivo

Segmentos de clientes

desarrolladores móviles y web

Oferta hacia los clientes

Protección para ataques de día cero (exposición desde el código de los algoritmos de programación), por medio de un sistema de pruebas y control en dispositivos, aplicaciones móviles, entre otros, para identificar posibles vulnerabilidades en la programación o en el diseño.

¿Por qué es una oportunidad?

- Las vulnerabilidades de la lógica de programación son una puerta para las violaciones de seguridad, que pueden llevar a fraudes y perdidas de información.
- Prevenir posibles ataques por la vulneración proveniente de los dispositivos desde su programación y diseño.
- Permite mayor seguridad y confianza en los desarrollos, garantizando la privacidad desde la lógica de programación y diseño del dispositivo.

Capacidades requeridas

- Personal capacitado en seguridad cibernética, tecnología en la nube, desarrollo de aplicaciones móviles.
- Expertos en lenguajes de programación como Java, Python.
- Desarrolladores y arquitectos de software.

Brechas/ Barreras

- Desconocimiento de los beneficios de la solución.
- Poca confianza de los desarrollos locales, por parte de los clientes potenciales.
- Falta conocimiento de estándares internacionales en temas de ciberseguridad.

5. Centro de entrenamiento en ciberseguridad

Segmentos de clientes

Instituciones de seguridad

desarrolladores móviles y web

Entidades financieras

Oferta hacia los clientes

Acceso a capacitación de calidad, por medio de entrenamientos virtuales y presenciales para la formación de equipos especializados en áreas de ciberseguridad (Reversing, análisis de malware, criptografía, ataques web, o detección de amenazas avanzadas persistentes), por medio de plataformas virtuales de capacitación.

OBSERVATORIO CT+i

¿Por qué es una oportunidad?

- Un centro de entrenamiento en la ciudad, se convierte en una estrategia clave de apoyo de los programas de formación, para fortalecer capacidades en diversas especialidades cibernéticas.
- La formación virtual da mayor flexibilidad y permite mayor cobertura favoreciendo el acceso.
- Un centro de entrenamiento favorece la generación de relaciones y alianzas, así como la identificación de talento para el desarrollo de soluciones de ciberseguridad.
- Un campo de operaciones virtual permite reproducir ciberataques reales en un entorno seguro y con total realismo, ofreciendo preparación a ataques reales en la práctica diaria.

Capacidades requeridas

- Alianzas con empresas nacionales e internacionales que ofrecen tecnologías y plataformas virtuales en ciberseguridad.
- Alianzas entre universidades, centros de formación y gobierno generando sinergias dente los diferentes actores que promuevan el desarrollo del centro de formación.
- Infraestructura para el montaje del centro de entrenamiento.
- Se necesitan expertos y profesionales en ciencias computacionales, científicos de datos y en ciberseguridad.
- Plataformas SaaS y APIs con sistemas de IA y aprendizaje automático.
- Conocimientos en aplicaciones de tecnología Blockchain.

Brechas/ Barreras

- Falta articulación entre los diferentes actores.
- Alta inversión de capital requerida.

PARA TENER EN CUENTA

- La ciberseguridad se ha convertido en una **necesidad para protegerse de los riesgos y ataques que afectan la infraestructura crítica e información confidencial**, tanto para entidades como para usuarios, con el fin de salvaguardar la privacidad, reducir pérdidas económicas y mala reputación de las compañías.
- Falta cultura en las empresas y las personas en el manejo de la información, **la seguridad no siempre es un pilar fundamental a tener en cuenta al interior de las organizaciones**.
- N**o existe confianza en la adopción de tecnología desarrollada localmente** y en muchos casos se prefiere optar por soluciones desarrolladas en otros países.
- Existe una **necesidad a nivel local en formación** en seguridad cibernética, ciencia de datos, ciencias computacionales, tecnología en la nube, inteligencia artificial, analítica, procesamiento de información no estructurada, entre otros, para promover el desarrollo de soluciones en ciberseguridad.
- **Falta articulación entre los diferentes actores** como empresas universidades y gobierno, para promover la activación de oportunidades asociadas con ciberseguridad. Las capacidades actuales están sectorizadas y **no hay dinámicas de colaboración**.
- Una de las principales barreras para las oportunidades priorizadas, es las **altas inversiones requeridas** para su desarrollo.
- Hay una **carencia de normatividad y/o regulación** en ciberseguridad, es necesario promover su generación para habilitar el desarrollo de las soluciones.

REFERENCIAS

[1] Aguilar, L. J. (2016). Presente y futuro de la ciberseguridad : el impacto y la necesidad de la colaboración público-privada Luis Joyanes Aguilar, 2016, 351–356.

[2] Cisco, 2016. Informe annual de seguridad. https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

[3] Forbes, 2017. Gartner Predicts Information Security Spending To Reach $93 Billion In 2018. Recuperado en la dirección electrónica https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#170eca4c3e7f

[4] Accenture Security, 2016. Informe alto rendimiento en seguridad 2016 de Accenture. https://www.accenture.com/t20170406T051638Z__w__/es-es/_acnmedia/PDF-42/Accenture-Security-Report-2016_Key-Insights_SPAIN-esp.pdf

[5] BID & OEA, 2016. Cybersecurity, Are We ready in Latin America and the Caribbean?. https://publications.iadb.org/handle/11319/7449?locale-attribute=es&

[6] Forbes, 2016. Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020. Recuperado de https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#7786da4e6832

[7] Statista, (2017). Recuperado de https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/

[8] Statista, (2017). Recuperado de https://www.statista.com/statistics/709789/most-pressing-global-cyber-security-issues/

[9] Revista Portafolio, (2017). Recuperado de http://www.portafolio.co/negocios/empresas/la-ciberseguridad-es-responsabilidad-de-todos-508818

[10] Shaulov, M. (2016). Bridging mobile security gaps. Network Security, 2016(1), 5–8. https://doi.org/10.1016/S1353-4858(16)30006-X

[11] Mejía Quijano, R. C. (2012). Autoevaluación del Sistema de Control Interno. AD-Minister; No 6 (2005), (6), 82–95. Retrieved from http://publicaciones.eafit.edu.co/index.php/administer/article/view/664

[12] Froomkin, A. M. (2016). Building Privacy into the Infrastructure : Towards a New Identity Management Architecture, (May).

[13] Khan S.M. (2017) Multimodal Behavioral Analytics in Intelligent Learning and Assessment Systems. In: von Davier A., Zhu M., Kyllonen P. (eds) Innovative Assessment of Collaboration. Methodology of Educational Measurement and Assessment. Springer, Cham

[14] Al-Musawi, B., Branch, P., & Armitage, G. (2017). BGP Anomaly Detection Techniques: A Survey. IEEE Communications Surveys & Tutorials, 19(1), 377–396. https://doi.org/10.1109/COMST.2016.2622240

REFERENCIAS

[15] Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016). Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework. Proceedings of the International Conference on Internet of Things and Cloud Computing - ICC '16, 1–5. https://doi.org/10.1145/2896387.2906198

[16] Isis Chong, Huangyi Ge, Ningui Li, & Robert W (2017). Influence of Privacy Priming and Security Framing on Android App Selection Proceedings of the Human Factors and Ergonomics Society Annual Meetin.g Vol 61, Issue 1, pp.796 – 96. Recuperado en https://doi.org/10.1177/1541931213601691

[17] Anagnostopoulos, C., & Kolomvatsos, K. (2017). Predictive intelligence to the edge through approximate collaborative context reasoning. Applied Intelligence. https://doi.org/10.1007/s10489-017-1032

ANEXO

SOLICITANTE	NÚMERO DE PRIORIDAD	TÍTULO
Appthority	US201715470717 20170327	AUTOMATED CLASSIFICATION OF APPLICATIONS FOR MOBILE DEVICES
	US201614988393 20160105	QUANTIFYING THE RISKS OF APPLICATIONS FOR MOBILE DEVICES
	US201514867661 20150928	IN-LINE FILTERING OF INSECURE OR UNWANTED MOBILE DEVICE SOFTWARE COMPONENTS OR COMMUNICATIONS
	US201514675327 20150331	APPLICATION MALWARE FILTERING FOR ADVERTISING NETWORKS
	US201414541007 20141113	OFF-DEVICE ANTI-MALWARE PROTECTION FOR MOBILE DEVICES
Sentegrity	US201615332850 2016102	SYSTEM FOR TRANSPARENT AUTHENTICATION ACROSS INSTALLED APPLICATIONS
Skycure	US201514876804 20151006	DETECTION OF MUTATED APPS AND USAGE THEREOF
	US201414509064 20141008	POTENTIAL ATTACK DETECTION BASED ON DUMMY NETWORK TRAFFIC
	US201261660773P 20120617	ACCESS CONTROL SYSTEM FOR A MOBILE DEVICE
	US201261660777P 20120617	SELECTIVE ENCRYPTION IN MOBILE DEVICES
Zimperium	US201414153976 20140113	CLASSIFIER-BASED SECURITY FOR COMPUTING DEVICES
	US201313865212 20130418	PREVENTIVE INTRUSION DEVICE AND METHOD FOR MOBILE DEVICES
	US201313925904 20130625	SYSTEM AND METHOD FOR DETECTION AND PREVENTION OF HOST INTRUSIONS AND MALICIOUS PAYLOADS
	US201313892337 20130513	DETECTION OF THREATS TO NETWORKS, BASED ON GEOGRAPHIC LOCATION
Feedzai	US201662293535P 20160210	AUTOMATIC DETECTION OF POINTS OF COMPROMISE
	PT20100105174 20100626	APPARATUS AND METHOD FOR DATA STREAM PROCESSING USING MASSIVELY PARALLEL PROCESSORS
Agari	US201615040288 20160210	MESSAGE AUTHENTICITY AND RISK ASSESSMENT
Socure	AU20170228607 20170913	RISK ASSESSMENT USING SOCIAL NETWORKING DATA
	US201515317735 20150611	ANALYZING FACIAL RECOGNITION DATA AND SOCIAL NETWORK DATA FOR USER AUTHENTICATION
Datavisor	US201514620028 20150211	USING HYPERGRAPHS TO DETERMINE SUSPICIOUS USER ACTIVITIES
	US201662312365P 20160323	USER INTERFACE FOR DISPLAYING AND COMPARING ATTACK TELEMETRY RESOURCES
	US201662308674P 20160315	USER INTERFACE FOR DISPLAYING NETWORK ANALYTICS
Trooly	US201514980343 20151228	DETERMINING TRUSTWORTHINESS AND COMPATIBILITY OF A PERSON

ANEXO

SOLICITANTE	NÚMERO DE PRIORIDAD	TÍTULO
GreatHorn	US201615161746 20160523	COMPUTER-IMPLEMENTED METHODS AND SYSTEMS FOR LDENTIFYING VISUALLY SIMILAR TEXT CHARACTER STRINGS
Exabeam	US201414507585 20141006	SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR DETECTING AND ASSESSING SECURITY RISKS IN A NETWORK
	US201514845943 20150904	SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR TRACKING USER ACTIVITY DURING A LOGON SESSION
PerimeterX	US201462050449P 20140915	ANALYZING CLIENT APPLICATION BEHAVIOR TO DETECT ANOMALIES AND PREVENT ACCESS
Sqrrl	US201614988489 20160105	DOCUMENT-PARTITIONED SECONDARY INDEXES IN A SORTED, DISTRIBUTED KEY/VALUE DATA STORE
	US201514801950 20150717	ENTITY-RELATIONSHIP MODELING WITH PROVENANCE LINKING FOR ENHANCING VISUAL NAVIGATION OF DATASETS
	US201414570067 20141215	POLICY-BASED DATA-CENTRIC ACCESS CONTROL IN A SORTED, DISTRIBUTED KEY-VALUE DATA STORE
	US201414298890 20140607	SECURE ACCESS TO HIERARCHICAL DOCUMENTS IN A SORTED, DISTRIBUTED KEY/VALUE DATA STORE
Fortscale	US201615068590 20160313	IDENTIFYING INSIDER-THREAT SECURITY INCIDENTS VIA RECURSIVE ANOMALY DETECTION OF USER BEHAVIOR
E8 Security	US201615331654 20161021	DETECTING SECURITY THREATS IN A LOCAL NETWORK
CyberX	US201514830776 20150820	METHOD FOR REDUCING CYBER ATTACK IN INDUSTRIAL CONTROL SYSTEM
Interset	US201562165560P 20150522	METHOD AND SYSTEM FOR AGGREGATING AND RANKING OF SECURITY EVENT-BASED DATA
	US201562155820P 20150501	SYSTEMS AND METHODS FOR MATHEMATICAL REGRESSION WITH INEXACT FEEDBACK
	US201414579421 20141222	METHOD AND SYSTEM FOR ANALYZING RISK
intensity analytics	US201615248174 20160826	USER AUTHENTICATION VIA KNOWN TEXT INPUT CADENCE
BehavioSec	US201615048021 20160219	METHOD, COMPUTER PROGRAM AND SYSTEM THAT USES BEHAVIORAL BIOMETRIC ALGORITHMS
	US201514928974 20151030	ADVANCED LOCALIZATION OF RADIO TRANSMITTERS IN ELECTROMAGNETIC ENVIRONMENTS
	US201514728825 20150602	ELECTROMAGNETIC THREAT DETECTION AND MITIGATION IN THE INTERNET OF THINGS
	US201462006605P 20140602	ELECTROMAGNETIC PERSONA GENERATION BASED ON RADIO FREQUENCY FINGERPRINTS
	US20160124071	DIVERSE RADIO FREQUENCY SIGNATURE, VIDEO, AND IMAGE SENSING FOR DETECTION AND LOCALIZATION
	US20160127403	SENSOR MESH AND SIGNAL TRANSMISSION ARCHITECTURES FOR ELECTROMAGNETIC SIGNATURE ANALYSIS
	US20160127907	BLIND SIGNAL CLASSIFICATION AND DEMODULATION IN A MULTIMODAL RADIO FREQUENCY ENVIRONMENT
	US20160127392	ELECTROMAGNETIC SIGNATURE ANALYSIS FOR THREAT DETECTION IN A WIRELESS ENVIRONMENT OF EMBEDDED COMPUTING DEVICES

ANEXO

SOLICITANTE	NÚMERO DE PRIORIDAD	TÍTULO
SparkCognition	US201715489564 20170417	COOPERATIVE EXECUTION OF A GENETIC ALGORITHM WITH AN EFFICIENT TRAINING ALGORITHM FOR DATA-DRIVEN MODEL CREATION
	US201615354122 20161117	SYSTEM AND METHOD FOR GENERATION OF A HEURISTIC
	US201514683735 20150410	SYSTEMS AND METHODS FOR USING COGNITIVE FINGERPRINTS
	US201514644346 20150311	SYSTEM AND METHOD FOR CALCULATING REMAINING USEFUL TIME OF OBJECTS
	US201414152610 20140110	SYSTEM AND METHOD FOR CREATING A CORE COGNITIVE FINGERPRINT
Cujo	US201562150684P 20150421	NETWORK SECURITY ANALYSIS FOR SMART APPLIANCES
	US201529542946F 20151019	INTERNET OF THINGS HUB
	US201615377856 20161213	INTERCEPTING INTRA-NETWORK COMMUNICATION FOR SMART APPLIANCE BEHAVIOR ANALYSIS
logRhythm	US201615369550 20161205	ADVANCED INTELLIGENCE ENGINE
	US20050735482P 20051112	LOG COLLECTION, STRUCTURING AND PROCESSING
Anomali	US201562109862P 20150130	SPACE AND TIME EFFICIENT THREAT DETECTION
Deep Instinct	US201514969080 20151215	METHODS AND SYSTEMS FOR DATA TRAFFIC ANALYSIS
Indeni	US201113016090 20110128	APPARATUS FOR REAL-TIME MANAGEMENT OF THE PERFORMANCE OF SECURITY COMPONENTS OF A NETWORK SYSTEM
PatternEx	US201715662323 20170728	COMPUTER-IMPLEMENTED PROCESS AND SYSTEM EMPLOYING OUTLIER SCORE DETECTION FOR IDENTIFYING AND DETECTING SCENARIO-SPECIFIC DATA ELEMENTS FROM A DYNAMIC DATA SOURCE
	US201615382413 20161216	METHOD AND SYSTEM FOR TRAINING A BIG DATA MACHINE TO DEFEND
SecBI	US201113077076 20110331	METHOD AND APPARATUS FOR AUTHENTICATING A USER USING DYNAMIC CLIENT-SIDE STORAGE VALUES
	US20100981072 20101229	MALWARE DETECTION USING RISK ANALYSIS BASED ON FILE SYSTEM AND NETWORK ACTIVITY
Splunk	US201461947651P 20140304	CLASSIFYING DATA WITH DEEP LEARNING NEURAL RECORDS INCREMENTALLY REFINED THROUGH EXPERT INPUT


OBSERVATORIO CT+i
OPORTUNIDADES Y TENDENCIAS TECNOLÓGICAS
PARA LOS NEGOCIOS DEL FUTURO