2022 PEDET

BIG DATA

CIBERSEGURIDAD

INTELIGENCIA ARTIFICIAL

ORIGO Lab

Proyecto apoyado por CORFO

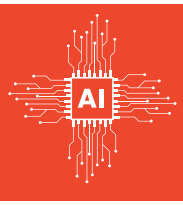
Gobierno de Chile
gob.cl

COLECCIÓN E-BOOKS

BIG DATA
CIBERSEGURIDAD
INTELIGENCIA ARTIFICIAL

Estamos viviendo en un mundo cada vez más digitalizado, incluso la pandemia aceleró considerablemente este proceso. Por una parte, la era digital trae beneficios, pero también nos obliga a estar atentos tanto de las amenazas como poder aprovechar las oportunidades que podemos encontrar. Una de las principales tendencias en ciberinteligencia es la incorporación de analítica avanzada de seguridad para hacer frente a las amenazas del ciberespacio o lograr comprender más rápido las necesidades de los clientes, poder recopilar, analizar y gestionar los datos que generan los usuarios de Internet.

En este curso revisaremos 3 conceptos: Inteligencia artificial IA, Big Data y Ciberseguridad.



Inteligencia Artificial: A través de la inteligencia artificial se pueden optimizar las tareas y procesos de una empresa, su objetivo es mejorar considerablemente las capacidades y contribuciones humanas. Esto convierte a la IA en un activo muy valioso para cualquier empresa.

Big Data: Nos presenta un conjunto de tecnologías creadas para poder recopilar, analizar y gestionar los datos que se están generando en Internet.

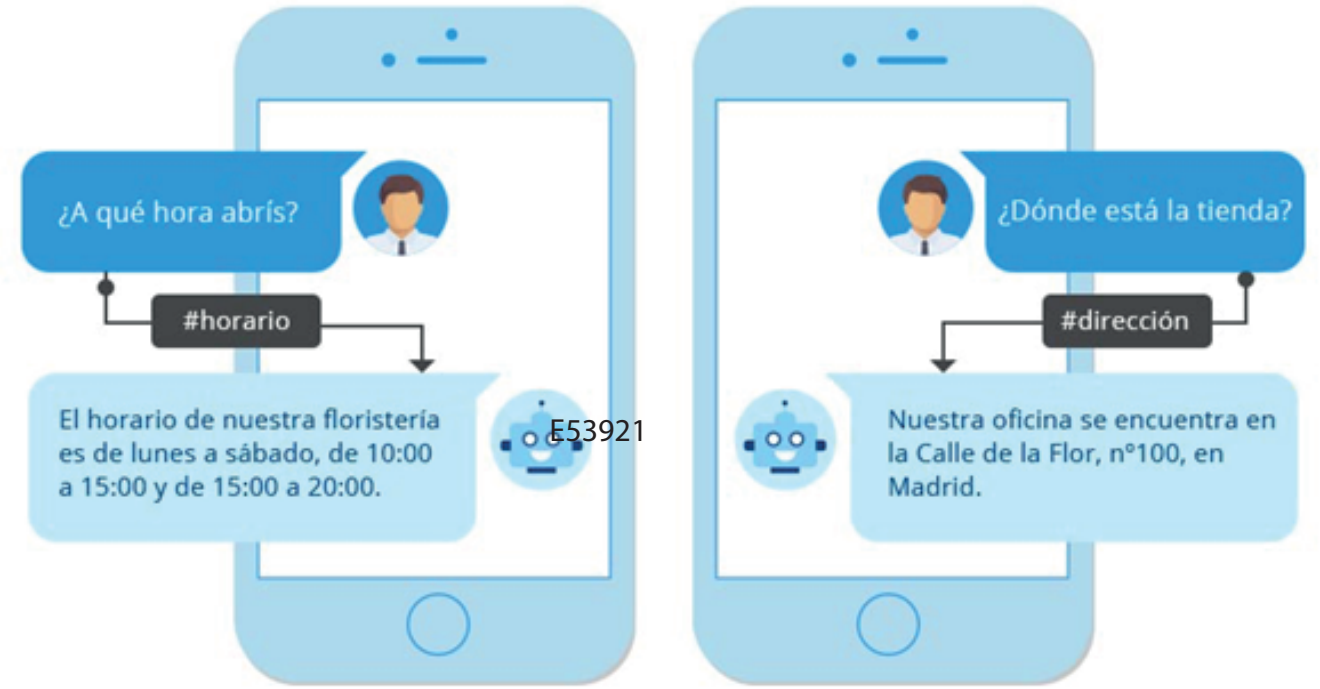
Ciberseguridad: Por medio de la ciberseguridad se busca proteger los sistemas importantes y la información confidencial de los ataques digitales. Las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización.

Esta era digital gira en torno a nuevas tecnologías e Internet y es un gran desafío para las empresas y para cada emprendimiento porque nos habla de cambios profundos y transformaciones que se manifiestan a través de una verdadera revolución tecnológica que está transformando incluso los hábitos de los consumidores, el lenguaje, y el cómo gestionar nuestras empresas.

INTELIGENCIA ARTIFICIAL (IA)

En términos simples, inteligencia artificial (IA) se refiere a sistemas o máquinas que imitan la inteligencia humana para realizar tareas y pueden mejorar iterativamente a partir de la información que recopilan. La IA se manifiesta de varias formas. Algunos ejemplos son:

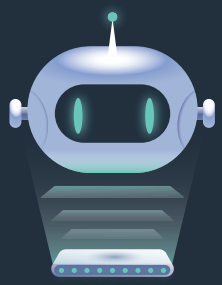
• Los chatbots utilizan la IA para comprender más rápido los problemas de los clientes y proporcionar respuestas más eficientes.



E53921

• Los asistentes inteligentes utilizan la IA para analizar información crítica proveniente de grandes conjuntos de datos de texto libre para mejorar la programación.

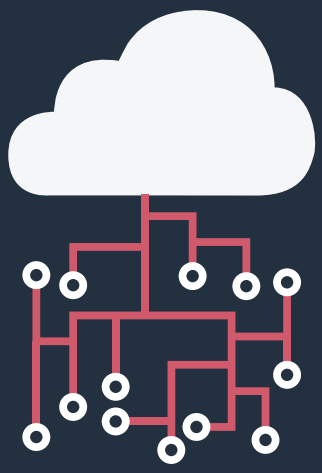
• Los motores de recomendación pueden proporcionar recomendaciones automatizadas para programas de TV según los hábitos de visualización de los usuarios.



La IA consiste más sobre el proceso y la capacitación del pensamiento avanzada y el análisis de datos que sobre cualquier otra función en particular. Se visualizan imágenes de robots con IA y aspecto humano de alto funcionamiento que se apoderan del mundo, pero la IA no busca reemplazar a los humanos. Su objetivo es mejorar considerablemente las capacidades y contribuciones humanas. Esto convierte a la IA en un activo empresarial muy valioso.

TERMINOLOGÍA

En su terminología la inteligencia artificial se ha convertido en un término general para las aplicaciones que realizan tareas complejas que antes necesitaban aportes humanos, tales como la comunicación online con los clientes o jugar ajedrez. El término se usa indiscriminadamente con sus subcampos que incluyen aprendizaje de maquina (machine learning) y aprendizaje profundo (Deep learning).



Existen diferencias, machine learning se centra en la creación de sistemas que aprenden o mejoran su rendimiento en función de los datos que consumen. Es importante tener en cuenta que, aunque todo machine learning es IA, no toda la IA es machine learning.

PRINCIPIO FUNDAMENTAL

El principio fundamental de la IA es replicar, y luego superar, la forma en que los humanos perciben y reaccionan ante el mundo. Se está convirtiendo rápidamente en la piedra angular de la innovación. La IA, impulsada por diferentes modelos de aprendizaje de maquina (machine learning) reconoce patrones en los datos que permite mejorar la toma de decisiones mediante predicciones que agregan valor al negocio al:

- Proporcionar una comprensión más completa de la abundancia de datos disponibles.
- Confiar en las predicciones para automatizar tareas excesivamente complejas o mundanas.

La tecnología de IA mejora el rendimiento y la productividad de la empresa mediante la automatización de procesos y tareas que antes requerían de esfuerzo humano. Con IA se puede dar sentido a datos a una escala que ningún humano jamás podría. Un ejemplo de ello es Netflix que utiliza machine learning para proporciona un nivel de personalización de contenido, esto ayudo a la empresa a aumentar su base de clientes en más de 25% en un año.

Actualmente las empresas consideran la analítica y la inteligencia artificial como tecnologías de diferenciación más importante para sus organizaciones. El valor que IA posee aplica en casi todas las funciones, negocios e industrias tales como:

- Uso de datos transaccionales y demográficos para predecir cuánto gastarán ciertos clientes en el curso de su relación con una empresa (o el valor de la vida útil del cliente).
- Optimización de precios basada en el comportamiento y preferencias del cliente.
- Uso del reconocimiento de imágenes para analizar imágenes de rayos X en busca de síntomas de cáncer.

Principalmente las empresas utilizan IA para:

- Detectar y disuadir intrusiones de seguridad (44%)
- Resolver problemas tecnológicos de los usuarios (41 %)
- Reducir el trabajo de la gestión de producción (34 %)
- Medir el cumplimiento interno en el uso de proveedores aprobados (34 %)

3 FACTORES QUE ESTÁN IMPULSANDO EL DESARROLLO DE LA IA EN LAS INDUSTRIAS

CÓMPUTO ASEQUIBLE Y DE ALTO RENDIMIENTO

La capacidad de cómputo asequible y de alto rendimiento ya se encuentra disponible. La abundancia del poder de la computación de productos básicos en la nube permite un fácil acceso a un poder de computación asequible y de alto rendimiento. Antes de este desarrollo, los únicos entornos informáticos disponibles para la IA no estaban basados en la nube y tenían un coste prohibitivo.

VOLÚMENES DE DATOS

Se encuentran disponibles grandes volúmenes de datos para la formación. La IA debe formarse en muchos datos para hacer las predicciones correctas. La aparición de diferentes herramientas para etiquetar datos, además de la facilidad y asequibilidad con que las organizaciones pueden almacenar y procesar datos estructurados y no estructurados, permite a más organizaciones diseñar y formar algoritmos de IA.

VENTAJA COMPETITIVA

La IA aplicada proporciona una ventaja competitiva. Cada vez más, las empresas reconocen la ventaja competitiva de aplicar los conocimientos de IA a los objetivos empresariales y lo convierten en una prioridad para toda la empresa. Por ejemplo, las recomendaciones específicas proporcionadas por la IA pueden ayudar a las empresas a tomar mejores decisiones más rápido. Muchas de las características y capacidades de la IA pueden reducir los costes y los riesgos, acelerar el tiempo de comercialización y mucho más.

5 MITOS HABITUALES SOBRE IA EMPRESARIAL

Si bien muchas empresas han adoptado con éxito la tecnología de inteligencia artificial, también circula mucha información errónea sobre la inteligencia artificial y lo que puede y no puede hacer. Aquí, exploramos cinco mitos habituales sobre la IA:

Mito n° 1: La IA empresarial requiere un enfoque de construcción propia.

Realidad: la mayoría de las empresas adoptan la IA combinando las soluciones internas con otras listas para usar. El desarrollo interno de la IA permite que las empresas se adapten a las necesidades empresariales exclusivas. Las soluciones de inteligencia artificial predefinidas le permiten optimizar su implementación con una solución lista para usar que aborda los problemas comerciales más comunes.

Mito n° 2: La IA ofrece inmediatamente resultados mágicos.

Realidad: se necesita tiempo para alcanzar el éxito en el camino hacia la IA, además de una idea clara de lo que se desea lograr. Se necesita un marco estratégico y un enfoque iterativo para evitar el suministro de un conjunto aleatorio de soluciones de IA desconectadas.

Mito n° 3: No es necesario que las personas ejecuten la IA empresarial.

Realidad: en la IA empresarial los robots no se hacen cargo de todo. El valor de la inteligencia artificial reside en que aumenta las capacidades humanas y descarga a los empleados para que realicen las tareas más estratégicas. Además, la IA depende de que las personas proporcionen los datos correctos y trabajen con ellos de la manera adecuada.

Mito n°4: Cuantos más datos, mejor.

Realidad: la IA empresarial necesita datos inteligentes. Para obtener la información empresarial más efectiva a partir de la IA, sus datos deben ser de alta calidad, actualizados, relevantes y enriquecidos.

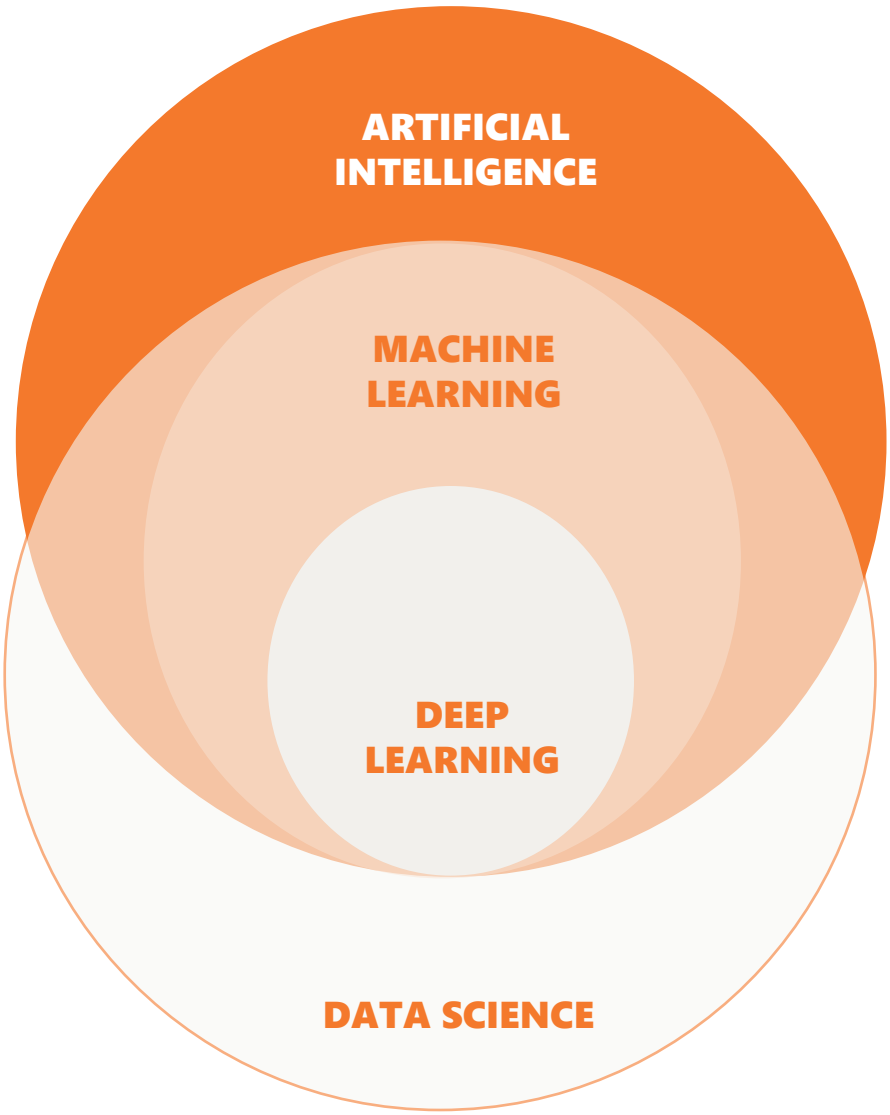
Mito n° 5: La IA empresarial solo necesita datos y modelos para alcanzar el éxito.

Realidad: los datos, los algoritmos y los modelos son un el punto de partida, pero una solución de inteligencia artificial debe ser escalable para satisfacer las cambiantes necesidades comerciales. Hasta la fecha, la mayoría de las soluciones de IA para empresas las han creado los científicos de datos manualmente. Estas soluciones requieren amplias tareas de configuración y mantenimiento manuales y no se escalan. Para implementar con éxito proyectos de inteligencia artificial, necesita soluciones de inteligencia artificial que se escalen de cara a cumplir con los nuevos requisitos a medida que se avanza en el desarrollo de la inteligencia artificial.

PRIMER PASO CON IA

Comunicación con los clientes a través de chatbots. Los chatbots utilizan el procesamiento del lenguaje natural para comprender a los clientes y permitirles hacer preguntas y obtener información. Estos chatbots aprenden con el paso del tiempo para que puedan agregar mayor valor a las interacciones con los clientes.

Ejecute análisis empresariales sin necesidad de contar con un experto. Las herramientas analíticas con una interfaz de usuario visual permiten a las personas sin conocimientos técnicos consultar fácilmente un sistema y obtener una respuesta comprensible.



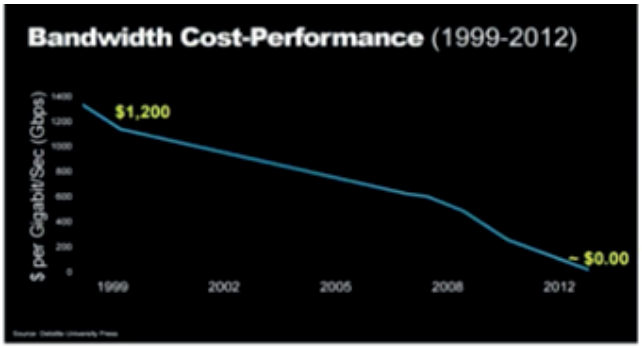
BIG DATA

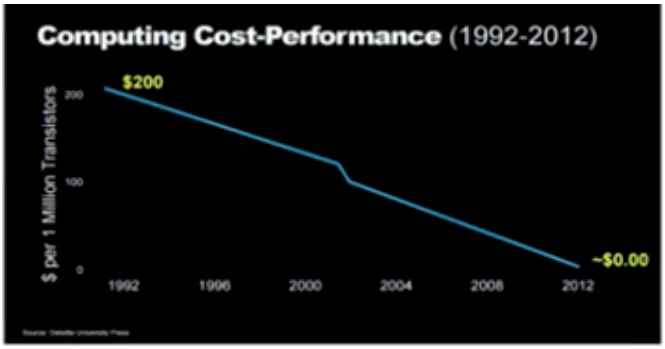
Todos somos seres digitales, seres que interactuamos permanentemente en redes sociales de internet, donde cada una de estas interacciones genera un rastro digital. Cosas que antes hacíamos de forma física hoy se hacen de manera digital, un pasaje de avión antes era impreso, hoy lo tenemos en digital, al llegar a un sitio donde tenemos que esperar, antes buscábamos una revista, hoy buscamos wifi para conectarnos, antes sacábamos fotografías oportunas, hoy sacamos más fotografías de lo que podemos procesar. Cada una de estás interacciones genera un rastro digital que hasta ahora técnicamente no era posible de analizar. El crecimiento de internet por lo tanto tiene que ver con el crecimiento del mundo móvil y con el crecimiento de las interacciones, pero el crecimiento futuro no solo tiene que ver con la interacción con redes sociales, también tiene que ver con la interacción de las cosas entre sí.

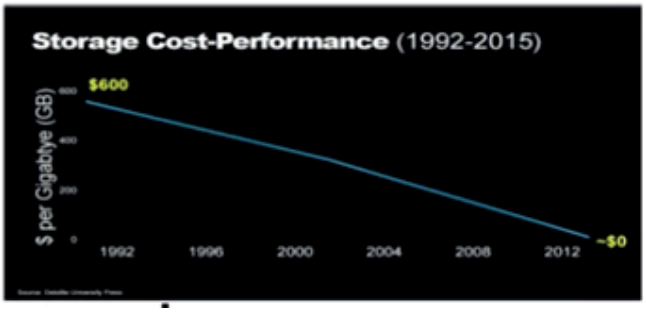
Por lo tanto, existen dos internets; el internet de las personas y el internet de las cosas. Un hecho es que la explotación a nivel de volúmenes de datos que se gestionarán a futuro va a tener que ver más con las cosas conectadas entre sí, interacciones máquina a máquina. En el internet de las cosas se proyecta que habrá más de 26.000 millones de objetos conectados en internet en el año 2026 y esto junto con la interacción de las personas con el mundo digital van a generar un volumen de información inmenso. De eso habla big data, de la capacidad de gestionar estos volúmenes de información de todo tipo. Y esto es posible hacerlo hoy en día porque ya existe la tecnología capaz para poder capturar esta información para poder procesarla, entenderla y poder accionar.

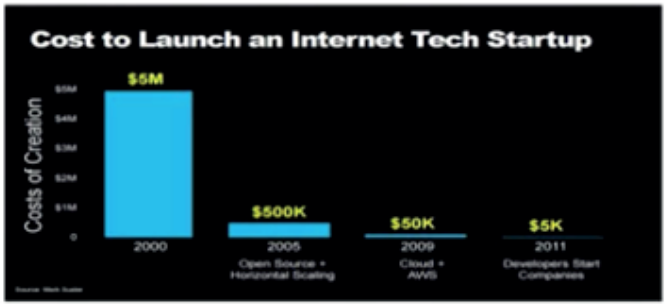
La principal causa de que haya nacido big data como mercado es la evolución tecnológica. Las caídas dramáticas en los costes de procesamiento de datos, en los costes de almacenamiento de datos lo que ha facilitado un crecimiento exponencial junto a de la cloud de poder procesar mucha información a muy bajo costo.

EVOLUCIÓN DEL BIG DATA
CAPACIDAD DE PROCESAMIENTO A BAJO COSTE









Big data habla de la democratización masiva del procesamiento de datos a muy bajo coste gracias a la caída de costes de almacenamiento, de procesamiento y de la cloud. Big data tiene que ver con el gran salto cuantitativo que es la cantidad de datos que podemos procesar, nos lleva a un salto cualitativo que es la cantidad de cosas nuevas que se pueden descubrir.

Big data responde a lo llamado las tres V: la V de volumen de la información, la V de variedad de tipos de información y la V de velocidad. Podemos analizar datos prácticamente a tiempo real y poder tomar decisiones a tiempo real.

Pero existe una cuarta V muchísimo más importante que es la V de valor. Big data solo tiene sentido si el resultado de descubrir esos patrones ocultos de la información nos lleva a descubrir cosas nuevas que nos permiten tomar decisiones de impacto en el negocio.

Una de las V que se debe aclarar es la V de variedad, que refiere que tenemos varios tipos de datos, básicamente existen tres tipos de datos, datos estructurados, datos no estructurados y datos semi estructurados.

FUENTE DE DATOS

ESTRUCTURADOS	SEMI - ESTRUCTURADOS	NO ESTRUCTURADOS
Relation & Legacy Databases Spreadsheels Flat Files with Proper Record Formats	XML EDI Documents	Web E-mails Multimedia (Video, audio) RSS Feeds Messages

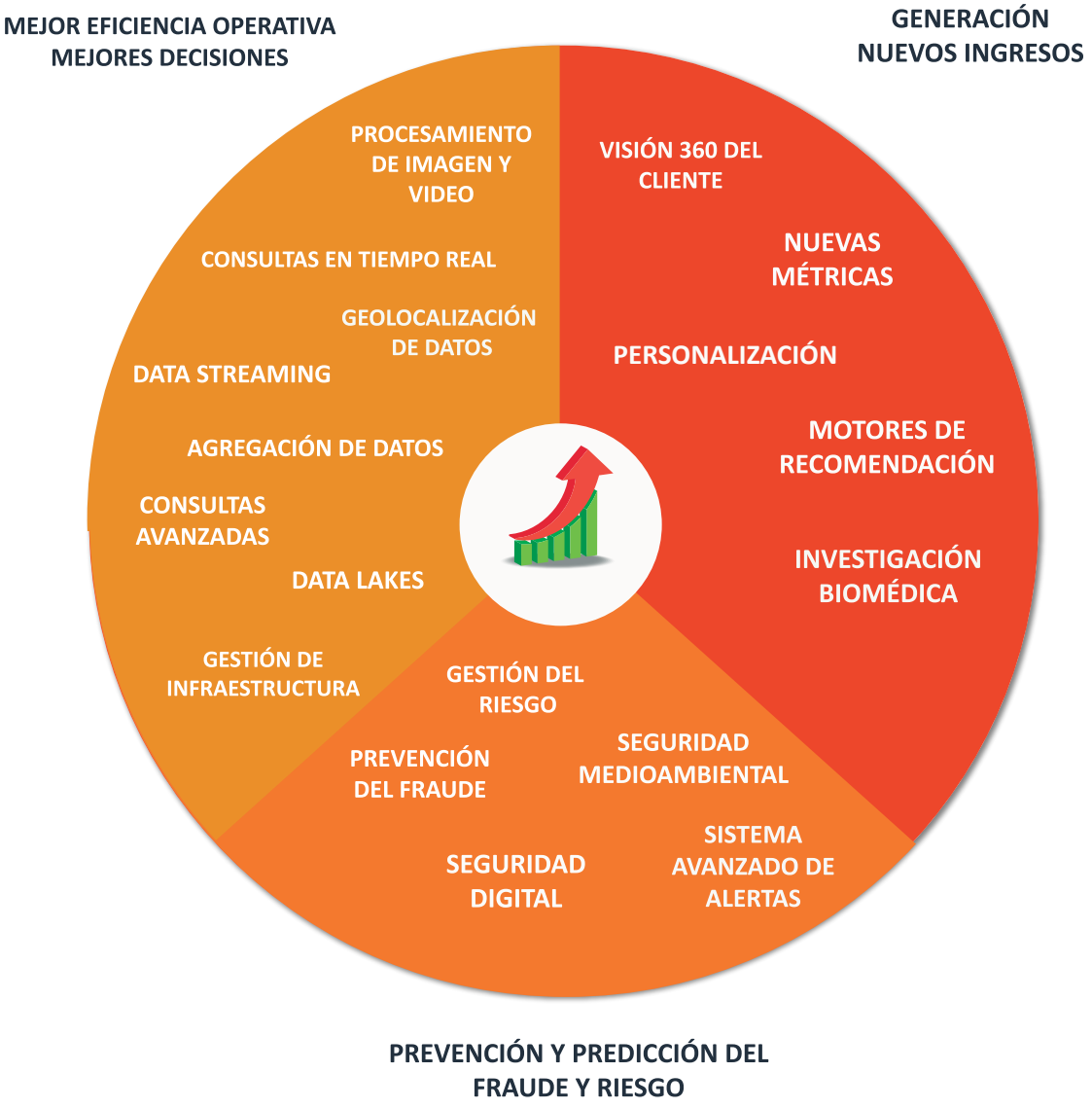
Los datos estructurados son los datos que conocemos, toda la informática tradicional solo ha podido gestionar datos estructurados, es decir filas y columnas en una base de datos relacional en una hoja de Excel, 1 y 0, bases de datos. El resto de información no estructurada, es decir imágenes, textos, videos, grabaciones de voz de nuestros clientes en un call center, toda esta información no tiene más manera de poderla procesar y analizar. Tampoco la información semi estructurada, por ejemplo los logs de navegación de internet.

Toda esta información es la que nos permite procesar big data. Big data nos permite tratar la información no estructurada y semi estructurada de la misma manera que hasta ahora hemos podido tratar la información estructurada.

Así se logra conseguir una visión mucho más granular, un conocimiento más profundo de nuestros clientes y de nuestros productos y servicios. Esto es lo que pretende big data, descubrir los patrones ocultos de la información y gracias a ello, ser capaz de caracterizar mejor los comportamientos, por ejemplo de nuestros clientes para poder desarrollar estrategias que nos permitan desarrollar nuestros productos y servicios más personalizados, y sobre todo a partir de las tecnologías de big data desarrollar modelos de analítica avanzada que nos permiten pasar de ser compañías reactivas a compañías predictivas.

BENEFICIOS DE LA APLICACIÓN DEL BIGDATA

CASOS DE USO



CIBERSEGURIDAD

La ciberseguridad es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

- La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista.

- La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

- La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.

- La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría.

- La recuperación ante desastres y la continuidad del negocio definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos.

- La capacitación del usuario final aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización.

4 MITOS PELIGROSOS DE LA CIBERSEGURIDAD

Los incidentes de ciberseguridad están aumentando en todo el mundo, pero todavía persisten algunos conceptos erróneos, incluida la noción de que:

Mito n.º 1: Los ciberdelincuentes son personas externas.

En realidad, las brechas de seguridad cibernética son a menudo el resultado de personas internas malintencionadas que trabajan por su cuenta o junto con piratas informáticos externos. Estas personas internas pueden ser parte de grupos bien organizados, apoyados por estados.

Mito n.º 2: Los riesgos son bien conocidos.

De hecho, la superficie de riesgo aún se está expandiendo, con miles de nuevas vulnerabilidades informadas en aplicaciones y dispositivos tanto antiguos como nuevos. Y las posibilidades de errores humanos, específicamente por parte de empleados o contratistas negligentes que causan involuntariamente una brecha de seguridad de datos, siguen aumentando.

Mito n.º 3: Los vectores de ataque están bajo control.

Los ciberdelincuentes están encontrando nuevos vectores de ataque todo el tiempo, incluyendo los sistemas Linux, la tecnología operacional (TO), los dispositivos de Internet de las cosas (IoT) y los entornos de nube.

Mito n.º 4: Mi industria está segura.

Cada industria tiene sus riesgos de ciberseguridad y los ciberdelincuentes explotan las necesidades de las redes de comunicación dentro de casi todas las organizaciones gubernamentales y del sector privado. Por ejemplo, los ataques de ransomware (véase más abajo) vulneran más sectores que nunca, incluidos gobiernos locales y organizaciones sin fines de lucro, y también han aumentado las amenazas en las cadenas de suministro, los sitios web ".gov" y la infraestructura importante.

AMENAZAS CIBERNÉTICAS COMUNES

Las últimas amenazas de ciberseguridad están dando un nuevo giro a las amenazas "conocidas", aprovechando los entornos de trabajo desde casa, las herramientas de acceso remoto y los nuevos servicios en la nube. Estas amenazas en evolución incluyen:

Malware

El término "malware" se refiere a variantes de software malicioso, como gusanos informáticos, virus, troyanos y programas espía, que brindan acceso no autorizado o causan daños a una computadora. Los ataques de malware son cada vez más "sin archivos" y están diseñados para evadir métodos de detección familiares, como herramientas antivirus, que escanean archivos adjuntos maliciosos.

Ransomware

Es un tipo de malware que bloquea archivos, datos o sistemas y amenaza con borrar o destruir los datos, o hacer que los datos sean privados o confidenciales al público, a menos que se pague un rescate a los ciberdelincuentes que lanzaron el ataque. Los recientes ataques de ransomware se han dirigido a los gobiernos estatales y locales, que son más fáciles de vulnerar que las empresas y están bajo presión para pagar rescates con el fin de restaurar aplicaciones y sitios web de los que dependen los ciudadanos.

Estafas por correo electrónico / ingeniería social

Las estafas por correo electrónico son una forma de ingeniería social que engaña a los usuarios para que proporcionen su propia PII o información confidencial. En este tipo de estafa, los correos electrónicos o mensajes de texto parecen provenir de una empresa legítima que solicita información confidencial, como datos de tarjetas de crédito o información de inicio de sesión. El FBI ha notado un aumento en las estafas por correo electrónico relacionadas con la pandemia, vinculado al crecimiento del trabajo remoto.

Amenazas internas

Los empleados actuales o anteriores, socios comerciales, contratistas o cualquier persona que haya tenido acceso a sistemas o redes en el pasado se pueden considerar una amenaza interna si abusan de sus permisos de acceso. Las amenazas internas pueden ser invisibles para las soluciones de seguridad tradicionales como firewalls y sistemas de detección de intrusos, que se enfocan en amenazas externas.

Ataques de denegación de servicios distribuidos (DDoS)

Un ataque DDoS intenta bloquear un servidor, sitio web o red sobrecargándolo con tráfico, generalmente de múltiples sistemas coordinados. Los ataques DDoS abruman las redes empresariales a través del protocolo simple de administración de red (SNMP), que se utiliza para módems, impresoras, conmutadores, routers y servidores.

Amenazas persistentes avanzadas (APT)

En una APT, un intruso o un grupo de intrusos se infiltra en un sistema y permanece sin ser detectado durante un período prolongado. El intruso deja las redes y los sistemas intactos para poder espiar la actividad empresarial y robar datos confidenciales mientras evita la activación de respuestas defensivas. La reciente brecha de seguridad de Solar Winds de los sistemas del gobierno de los Estados Unidos es un ejemplo de una APT.

Ataques de intermediario / "Man-in-the-middle"

Los ataques de intermediario son ataques de espionaje, en los que un ciberdelincuente intercepta y transmite mensajes entre dos partes para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante puede interceptar los datos que se transmiten entre el dispositivo del invitado y la red.

PROTECCIÓN DE USUARIO FINAL

La protección del usuario final o la seguridad de endpoints es un aspecto fundamental de la ciberseguridad. Después de todo, a menudo es un individuo (el usuario final) el que accidentalmente carga malware u otra forma de ciberamenaza en su equipo de escritorio, laptop o dispositivo móvil.

Por tanto, ¿de qué manera protegen las medidas de ciberseguridad a los usuarios finales y los sistemas? En primer lugar, la ciberseguridad depende de los protocolos criptográficos para cifrar los correos electrónicos, archivos y otros datos críticos. La ciberseguridad no solo protege la información en tránsito, también ofrece protección contra las pérdidas o el robo.

Además, el software de seguridad del usuario final analiza las computadoras para detectar código malicioso, pone en cuarentena este código y lo elimina del equipo. Los programas de seguridad pueden incluso detectar y eliminar el código malicioso oculto en el registro de arranque maestro (MBR) y están diseñados para cifrar o borrar datos del disco duro de la computadora.

Los protocolos de seguridad electrónica también se enfocan en la detección de malware en tiempo real. Muchos utilizan el análisis heurístico y de comportamiento para monitorear el comportamiento de un programa y su código para defenderse de virus o troyanos que pueden cambiar de forma con cada ejecución (malware polimórfico y metamórfico). Los programas de seguridad pueden restringir los programas que puedan ser maliciosos en una burbuja virtual separada de la red del usuario para analizar su comportamiento y aprender a detectar mejor las nuevas infecciones.

Los programas de seguridad continúan desarrollando nuevas defensas mientras los profesionales de la ciberseguridad identifican nuevas amenazas y formas de combatirlas. Para aprovechar al máximo el software de seguridad del usuario final, los empleados deben aprender a utilizarlo. Lo fundamental es mantenerlo en funcionamiento y actualizarlo con frecuencia para que pueda proteger a los usuarios de las ciberamenazas más recientes.

CONSEJOS DE CIBERSEGURIDAD

¿Cómo pueden las empresas y las personas protegerse contra las ciberamenazas? A continuación, presentamos nuestros mejores consejos de ciberseguridad:

- Actualizar el software y el sistema operativo: esto significa que aprovechará las últimas revisiones de seguridad.

- Utilizar software antivirus: las soluciones de seguridad, detectarán y eliminarán las amenazas. Mantenga su software actualizado para obtener el mejor nivel de protección.

- Utilizar contraseñas seguras, asegúrese de que sus contraseñas no sean fáciles de adivinar.

- No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos: podrían estar infectados con malware.

- No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos: es una forma común de propagación de malware.

- Evitar el uso de redes Wi-Fi no seguras en lugares públicos: las redes no seguras lo dejan vulnerable a ataques del tipo "Man-in-the-middle".

CONCLUSIÓN

Para concluir nos damos cuenta que en esta era digital ya no hay un camino de regreso ni estamos frente a una moda y se puede establecer la viabilidad del aprovechamiento temprano de estas tecnologías, porque ya han sido probadas exitosamente. El mundo de las tecnologías de la información y las telecomunicaciones, permitirá que nos encontremos con una ventaja competitiva en términos de oportunidades, conquista de nuevos mercados, optimización de procesos, reducción de costos y mayor rentabilidad.

2022

PEDET

Otra más de Origo Lab!

ORIGO Lab

WWW.PEDET.CL

Proyecto apoyado por

CORFO

Gobierno de Chile

gob.cl