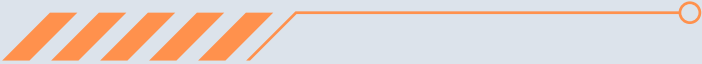




REVISTA DEL COLEGIO
DE INGENIEROS EN
SISTEMAS DE
COMPUTACIONALES
PARA LA SEGURIDAD DE
LA INFORMACIÓN,
CONTROL INTERNO Y
GOBERNANZA, A.C.

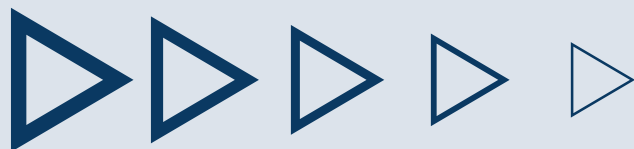




CONTENIDO

Revista CISCIG

INNOVACIÓN TECNOLÓGICA POR JOAQUÍN ORTIZ COBIT 2019: Un entendimiento general	4
FUTURO TECNOLÓGICO POR ARMANDO ÁVALOS Los riesgos de la Inteligencia Artificial	11
NUESTRO PAÍS POR LA REDACCIÓN Comunidad de Aprendizaje.	20
NUESTRO MUNDO POR ARMANDO ÁVALOS PÉREZ Regreso a la Luna	23
AUDITORÍA Y SEGURIDAD DE LA INFORMACIÓN POR LA REDACCIÓN Contraseñas fuertes y únicas	29
LO MISMO 30 AÑOS POR ARMANDO AVALOS Lo mismo 30 años después	32
ACTIVIDADES CISCIG POR EL CONSEJO DIRECTIVO Un año más de Actividades del Colegio de Ingenieros en Sistemas Computacionales para la seguridad de información el control interno y la gobernanza.	35



**TU INFRAESTRUCTURA DEBE ESTAR
LISTA PARA LO QUE VIENE**

**SIEMPRE
ACTUALIZADO.**

**SIEMPRE UN
PASO ADELANTE
EN EL JUEGO.**

**Solicita una evaluación
SIN COSTO**

POWERSTORE





WhatsApp:

+52 55 6736 9071

+ 52 55 3516 7586

+52 55 6502 1522



servicios@ciscig.mx



www.ciscig.mx

PRESIDENTE DEL COLEGIO Y DIRECTOR DE LA REVISTA

Armando Ávalos

VICEPRESIDENTE DEL COLEGIO

Joaquín Ortiz

JEFE DE INFORMACIÓN Y REDACCIÓN

Jorge García Alonso

DISEÑO EDITORIAL

Jedidia Ortiz

MIEMBROS DE LA MESA DIRECTIVA DEL COLEGIO

Armando Ávalos

Diana Elías

Joaquín Ortiz

Luis Castillo

Israel Fuentes

Verónica Bello

Moisés Cambranis

COLABORADORES Y ARTICULISTAS

Armando Ávalos

Joaquín Ortiz Flores

Alejandro Heredia Cobos

Jorge García Alonso

Jedidia Ortiz

Andrea Reyes

CONSEJERO JURÍDICO

Ernesto Alvarado

Número ISSN: 2992-7250- Año II, volumen IV, Marzo 2024.

REVISTA DEL COLEGIO DE INGENIEROS EN SISTEMAS DE COMPUTACIONALES PARA LA SEGURIDAD DE LA INFORMACIÓN , CONTROL INTERNO Y GOBERNANZA, A.C, año 2, No. 4, marzo 2024, es una publicación trimestral editada por el Colegio de Ingenieros en Sistemas de Computacionales para la Seguridad de la Información Control Interno y Gobernanza, A.C. (CISCIG), Calle Parral # 6, Colonia Condesa, Alcaldía Cuauhtémoc, C.P. 06140, Ciudad de México, Tel (55) 3516 7586, www.ciscig.mx, jorge.garcia@marcg.com.mx Editor y responsable de la última actualización de este Número Armando Avalos Pérez, Calle Parral # 6, Colonia Condesa , Alcaldía Cuauhtémoc , C.P. 06140 , Ciudad de México armando.avalos@marcg.com.mx Reserva de Derechos al Uso Exclusivo No. 04-2023- 033115290800-102, ISBN: 2992-7250, ambos otorgados por el Instituto Nacional de Derecho de Autor, fecha de última actualización, 31 marzo 2024



COBIT 2019: UN ENTENDIMIENTO GENERAL

NO, NO ESTAMOS HABLANDO DEL VIRUS DE LA PANDEMIA DEL 2020. EN LA PRÁCTICA DE LA INDUSTRIA DE TI, SE HA MANEJADO UN CONCEPTO LLAMADO "GOBIERNO DE TI", QUE ES COMO LAS ORGANIZACIONES GESTIONAN SUS SERVICIOS, ACTIVOS Y A LA VEZ COMO LAS TI, SE ALINEAN AL MODELO DE NEGOCIO.

UNO DE LOS MARCOS MÁS ACEPTADOS POR LA INDUSTRIA ES EL MODELO COBIT 2019 (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES) COBIT ES UN MARCO DE REFERENCIA DESARROLLADO POR ISACA (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION). DESDE SU CREACIÓN, COBIT HA EVOLUCIONADO SIGNIFICATIVAMENTE, PASANDO POR VARIAS REVISIONES PARA ADAPTARSE A LOS CAMBIOS DE LA TECNOLOGÍA Y LAS NECESIDADES EMPRESARIALES.

BREVE HISTORIA DE LA EVOLUCIÓN DE COBIT

COBIT 1.0 (1996):

La primera versión de COBIT fue lanzada en 1996. Se centró en la auditoría de sistemas de información, proporcionando un conjunto de objetivos de control diseñados para ayudar a las organizaciones de auditoría a evaluar la efectividad de sus sistemas de TI.

COBIT 3.0 (2000)

La tercera edición expandió el marco para incluir prácticas de gestión, ofreciendo guías más detalladas sobre cómo implementar y gestionar los controles de TI en las organizaciones. Se enfatizó en la importancia del alineamiento entre los objetivos de negocio y la tecnología.

COBIT 4.0 (2005) y 4.1 (2007)

Estas versiones introdujeron el concepto de gobierno de TI, enfocándose en la responsabilidad de los ejecutivos y los consejos de administración en la supervisión de las TI. COBIT 4.1 consolidó más este enfoque, ofreciendo una guía detallada sobre procesos de gestión de TI y marcos de control.

COBIT 5 (2012)

COBIT 5 marcó una revisión significativa, integrando todos los marcos y guías de ISACA (incluyendo Val IT y Risk IT) en un solo marco unificado. Introdujo cinco principios para el gobierno y la gestión de TI empresarial y se basó en un enfoque de gestión de stakeholders (partes interesadas) para asegurar el valor desde las TI.

COBIT 2019

La última versión, COBIT 2019, fue lanzada para proporcionar una guía más flexible y adaptable. Introduce un enfoque modular, permitiendo a las organizaciones personalizar el marco según sus necesidades específicas. COBIT 2019 se basa en seis principios de gobierno y tres principios de diseño, ofreciendo una estructura que puede evolucionar con los cambios tecnológicos y de negocio. Se enfoca en la gestión de la información y la tecnología en un entorno empresarial, reconociendo la importancia de la agilidad y la innovación.

PRINCIPIOS PARA EL SISTEMA DE GOBIERNO COBIT 2019

1. Proporcionar Valor a los Stakeholders (partes interesadas)

Este principio se centra en maximizar el valor para los stakeholders, asegurando que las inversiones en TI generen los beneficios esperados a un costo adecuado, mientras se gestionan los riesgos asociados. Un equilibrio entre beneficios, riesgos y recursos es esencial para satisfacer las expectativas de los stakeholders.

2. Enfoque Holístico

Un enfoque holístico significa que la gobernanza de TI debe considerar todos los componentes del sistema de gobierno de manera integral, incluyendo procesos, estructuras organizativas, información, cultura, personas y tecnologías. Este principio reconoce que estos componentes están interconectados y que los cambios en uno de ellos pueden afectar a los demás. Un enfoque holístico asegura que la gobernanza de TI se integre de manera efectiva en toda la organización y contribuya al logro de sus objetivos estratégicos.

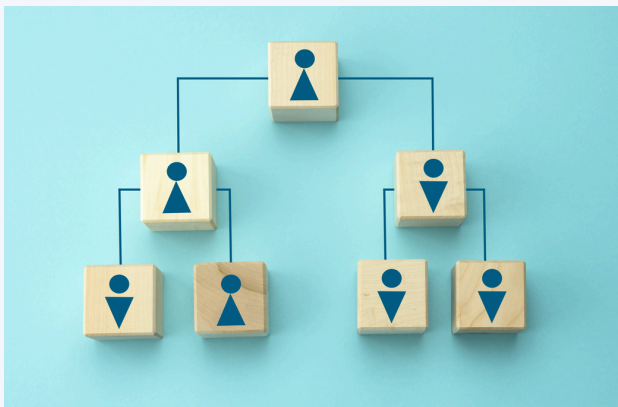


3. Sistema de Gobierno Dinámico

La gobernanza de TI no es estática; es un sistema dinámico que debe adaptarse a los cambios en el entorno empresarial, tecnológico y regulatorio. Los factores de diseño de COBIT 2019, como los objetivos de la organización, la estrategia de TI, las necesidades de los stakeholders y los riesgos de TI, influyen en cómo se configura y opera el sistema de gobernanza.

4. Separar el Gobierno de la Gestión

Este principio establece una clara distinción entre gobernanza y gestión. La gobernanza se encarga de establecer las direcciones estratégicas, los objetivos y los mecanismos de supervisión, mientras que la gestión se ocupa de la planificación, la construcción, la operación y el monitoreo de las actividades de TI en alineación con la dirección establecida por la gobernanza. Esta separación promueve la claridad de roles, responsabilidades y procesos dentro de la organización.



5. Adaptarse de Acuerdo con las Necesidades de la Empresa

COBIT 2019 se diseñó para ser flexible y adaptable a las necesidades específicas de cualquier organización, independientemente de su tamaño, sector o geografía.

Los factores de diseño permiten a las organizaciones personalizar el marco para que se alinee mejor con sus objetivos estratégicos, cultura organizacional, requisitos regulatorios y otras condiciones específicas.

6. Sistema Integrado de Gobierno

Este principio enfatiza que la gobernanza debe abarcar todo el procesamiento de información y la tecnología utilizada por la organización, no solo los sistemas de TI tradicionales. Esto incluye tecnologías emergentes, servicios en la nube, big data, y cualquier otra forma de tecnología de la información y comunicación.



PRINCIPIOS PARA UN SISTEMA DE DISEÑO COBIT 2019

1. Basado en un Modelo Conceptual

Un marco de gobierno debe estar fundamentado en un modelo conceptual sólido que defina claramente los componentes clave. En el contexto de COBIT 2019, esto se traduce en la identificación y estructuración de los componentes del marco de gobierno y gestión de TI, como procesos, políticas, objetivos de control, prácticas de gestión y métricas. Este modelo conceptual también incluye la definición de las relaciones entre estos componentes, cómo interactúan entre sí y con el entorno empresarial y de TI.



El modelo conceptual permite una comprensión clara de cómo se puede lograr el gobierno y la gestión de la TI, facilitando la identificación de áreas de fuerza y oportunidades de mejora.

Es la base sobre la cual se construye todo el sistema de gobierno, asegurando que todas las partes del marco trabajen juntas de manera cohesiva para apoyar los objetivos de la organización.



2. Abierto y Flexible

La tecnología y el entorno empresarial están en constante cambio, lo que requiere que los marcos de gobierno de TI sean abiertos y flexibles para adaptarse a nuevos desafíos, tecnologías y metodologías. Un marco abierto permite la incorporación de nuevas prácticas, herramientas y enfoques conforme emergen, asegurando que el marco permanezca relevante y útil a lo largo del tiempo.

COBIT 2019 ha sido diseñado con esta flexibilidad, permitiendo a las organizaciones adaptar y ajustar el marco a sus necesidades específicas. Esto incluye la capacidad de integrar otros marcos, estándares y regulaciones, así como adaptarse a cambios en el entorno empresarial o tecnológico.

La apertura y flexibilidad de COBIT 2019 garantizan que las organizaciones puedan seguir un enfoque de gobierno y gestión de TI que sea contemporáneo y alineado con sus estrategias y objetivos específicos.

3. Alineado con las Principales Normativas

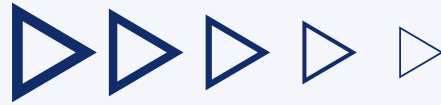
Para maximizar su efectividad y asegurar la coherencia en toda la organización, un marco de gobierno de TI debe estar alineado con las principales normativas, estándares, marcos y regulaciones internacionales. Esto incluye estándares como ISO/IEC 27001 para seguridad de la información, ITIL para gestión de servicios de TI, ISO 31000 para gestión de riesgos, entre otros.

COBIT 2019 ha sido diseñado para alinearse y complementarse con estas normativas, proporcionando un enlace entre los requisitos de gobernanza de TI y las prácticas operativas. La alineación asegura que las organizaciones puedan cumplir con los requisitos reglamentarios y de cumplimiento, mientras utilizan las mejores prácticas globales para la gestión y gobernanza de TI. Esto no solo mejora la eficiencia y efectividad de las operaciones de TI, sino que también facilita la auditoría y el cumplimiento normativo.



ESTRATEGIAS DE IMPLEMENTACIÓN COBIT 2019

Si bien la implementación de un marco como COBIT 2019, no es fácil, te dejo algunas consideraciones estratégicas para un bien kick off de implementación:



1. Comprensión y Compromiso de la Alta Dirección

Comprensión: Antes de comenzar la implementación, es crucial que la alta dirección comprenda los beneficios de COBIT 2019 y cómo puede apoyar los objetivos de negocio de la organización.

Compromiso: Obtener el compromiso de la alta dirección para apoyar la implementación, proporcionando los recursos necesarios y liderando por el ejemplo.



2. Evaluación de la Situación Actual

Análisis de Brechas: Realizar un análisis de brechas para entender la situación actual de la gobernanza y gestión de TI en comparación con los objetivos y prácticas recomendadas por COBIT 2019.

Priorización: Identificar y priorizar las áreas que necesitan mejoras basadas en su impacto en los objetivos de negocio.



3. Planificación de la Implementación

Objetivos Específicos: Definir objetivos específicos de implementación que sean medibles y alineados con los objetivos de negocio de la organización.

Hoja de Ruta: Desarrollar una hoja de ruta de implementación que detalle las acciones, los plazos y los recursos necesarios.



4. Personalización de COBIT para la Organización

Factores de Diseño: Utilizar los factores de diseño de COBIT 2019 para adaptar el marco a las necesidades y características específicas de la organización, como su tamaño, sector, cultura y tecnología.

Enfoque Modular: Aprovechar el enfoque modular de COBIT 2019 para implementar primero las áreas más críticas o con mayor retorno de inversión.



5. Desarrollo de Competencias y Capacitación

Capacitación: Asegurar que el personal relevante reciba capacitación sobre COBIT 2019 y cómo se aplicará en la organización.

Desarrollo de Competencias: Desarrollar competencias internas para la gestión y gobernanza de TI, incluyendo la formación de un equipo dedicado de COBIT, si es necesario.



6. Implementación Gradual y Revisión Continua

Implementación por Fases: Implementar COBIT 2019 de manera gradual, comenzando con proyectos piloto o áreas de alto impacto.

Revisión y Ajuste: Realizar revisiones periódicas para evaluar el progreso y hacer ajustes en la implementación según sea necesario.



7. Gestión del Cambio y Comunicación

Gestión del Cambio: Aplicar principios de gestión del cambio para ayudar a la organización a adaptarse a los nuevos procesos y prácticas.

Comunicación Efectiva: Mantener líneas de comunicación abiertas con todas las partes interesadas para informar sobre el progreso, los beneficios y los desafíos de la implementación de COBIT 2019.



8. Uso de Herramientas y Recursos

Herramientas de Apoyo: Considerar el uso de herramientas de software para facilitar la implementación y el seguimiento de COBIT 2019.

Recursos de ISACA: Aprovechar los recursos, guías y formación ofrecidos por ISACA para apoyar la implementación de COBIT 2019.

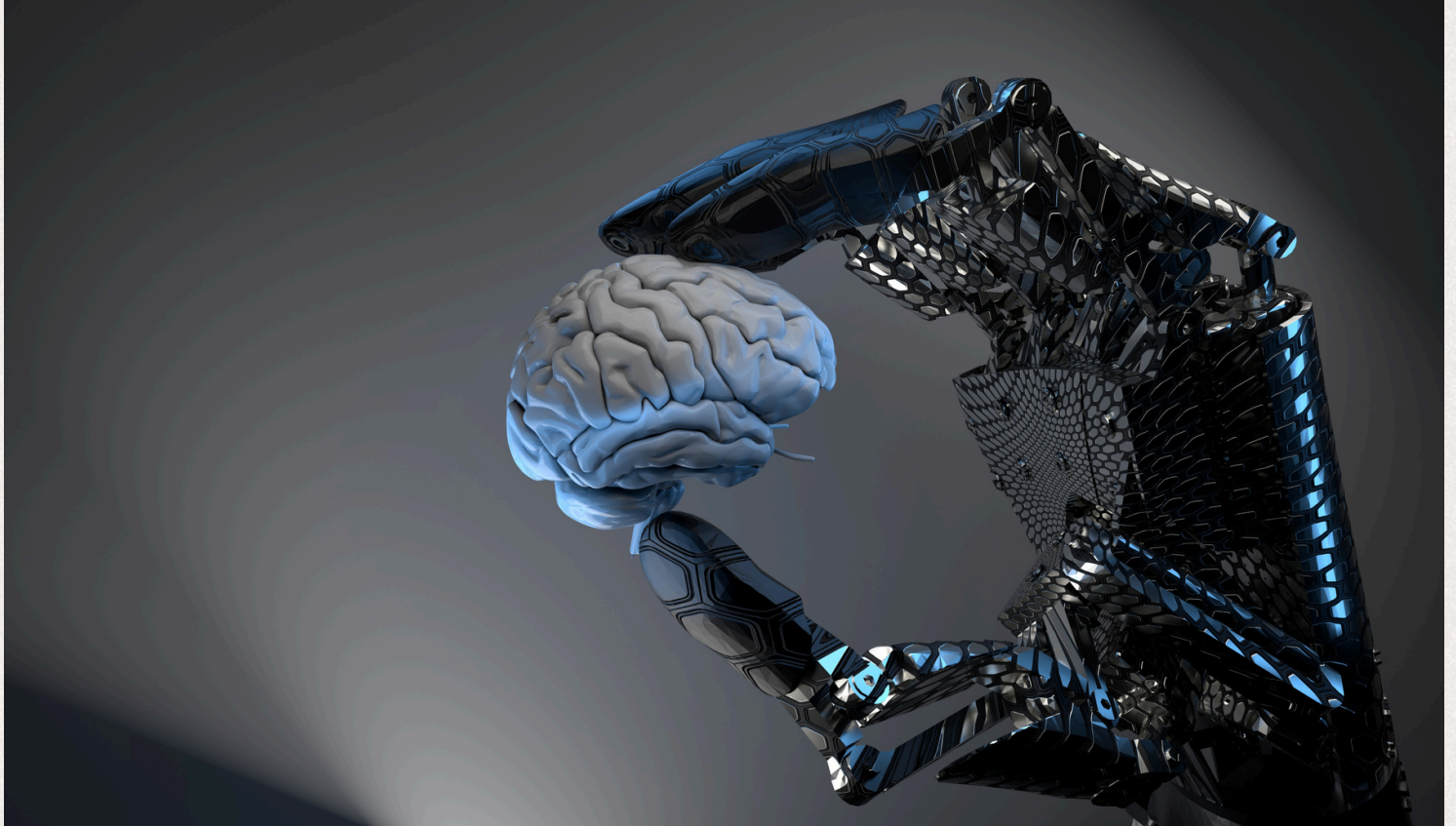
LA IMPLEMENTACIÓN Y ADAPTACIÓN DE COBIT 2019 EN LAS ORGANIZACIONES REPRESENTA UNA ESTRATEGIA FUNDAMENTAL PARA EL ALINEAMIENTO EFECTIVO ENTRE TI Y LOS OBJETIVOS DE NEGOCIO.

A TRAVÉS DE SUS PRINCIPIOS FUNDAMENTALES, MARCO DE GOBIERNO Y ESTRATEGIAS DE IMPLEMENTACIÓN, COBIT 2019 OFRECE UNA GUÍA INTEGRAL PARA LA GOBERNANZA Y GESTIÓN DE LA TI, ASEGURANDO QUE LAS INVERSIONES EN TECNOLOGÍA GENEREN VALOR REAL Y ESTÉN ALINEADAS CON LAS METAS EMPRESARIALES. SU ENFOQUE FLEXIBLE Y HOLÍSTICO PERMITE UNA PERSONALIZACIÓN SEGÚN LAS NECESIDADES ESPECÍFICAS DE CADA ORGANIZACIÓN, FACILITANDO ASÍ LA ADAPTACIÓN A CAMBIOS CONSTANTES EN EL ENTORNO TECNOLÓGICO Y EMPRESARIAL, GARANTIZANDO UNA MEJORA CONTINUA EN LOS PROCESOS DE TI.



LOS RIESGOS DE LA INTELIGENCIA ARTIFICIAL

¿QUÉ ES LA INTELIGENCIA ARTIFICIAL (IA)? LA PÁGINA DEL PARLAMENTO EUROPEO DEFINE LA INTELIGENCIA ARTIFICIAL COMO LA HABILIDAD DE UNA MÁQUINA DE PRESENTAR LAS MISMAS CAPACIDADES QUE LOS SERES HUMANOS, COMO EL RAZONAMIENTO, EL APRENDIZAJE, LA CREATIVIDAD Y LA CAPACIDAD DE PLANEAR



La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico (1) . La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos. Los sistemas de IA son capaces de adaptar su comportamiento en cierta medida, analizar los efectos de acciones previas y de trabajar de manera autónoma. La misma página describe una serie de aplicaciones de la IA. Según la definición de la Comisión Europea define los Tipos de IA de la siguiente manera:

- Software: asistentes virtuales, software de análisis de imágenes, motores de búsqueda, sistemas de reconcomiendo de voz y rostro
- Inteligencia artificial integrada: robots, drones, vehículos autónomos, Internet de las Cosas.

(1) ¿Qué es la inteligencia artificial y cómo se usa? | Noticias | Parlamento Europeo. (2020, 9 agosto).

<https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligenciaartificial-y-como-se-usa>

Sin duda la introducción de parámetros biométricos en las identificaciones oficial son un hecho que, solventando el costo de implementación, serán adoptados en los siguientes años...

Consideramos necesario hablar de las aplicaciones de inteligencia artificial que son las más controversiales, porque se enfocan en el control y “orientación” (por no decir manipulación) de las masas, comentemos algunos ejemplos de ellas. Empecemos por las aplicaciones de inteligencia artificial que por medios estadísticos y la explotación de datos de redes sociales intentan predecir la aceptación o incluso las acciones de las personas, una de estas aplicaciones es la que permite predecir las tendencias electorales por medio de las redes sociales. La polémica se deriva de la posibilidad de sesgar el criterio de la gente por medio de las mismas redes sociales al introducir noticias, comentarios, reportajes con acciones o declaraciones contrarias a las que los votantes les gustaría escuchar.

La inteligencia artificial también desafortunadamente permite crear situaciones falsas, cambiar los mensajes e incluso crear escenarios completamente ficticios enfocados a confundir a los votantes. Otras aplicaciones controversiales están enfocadas al reconocimiento facial y biométricos, mucho hemos escuchado la oposición de asociaciones civiles que se pronuncian en contra de la implementación de cámaras con reconocimiento facial y a una base de datos nacional que contenga los parámetros biométricos para la identificación por medio de la inteligencia artificial, sin embargo, algunos pasaportes y visas, o sistemas de migración ya cuentan con esos parámetros y son usados discrecionalmente.

Es necesario realizar un estudio del porqué la oposición a implementar modelos de inteligencia artificial como el reconocimiento facial en los temas de seguridad pública, ya que representan un área de oportunidad y mejora en el abatimiento de los actos delictivos. De esto hablaremos un poco más adelante en la sección de retos.

Existen limitaciones legales, leyes, jurisprudencias, reglamentos y criterios jurídicos que no permiten hacer una explotación de las bases de datos nacionales como se hacen con las redes sociales.



Sin duda la introducción de parámetros biométricos en las identificaciones oficiales son un hecho que, solventando el costo de implementación, serán adoptados en los siguientes años. El tema de la protección de la identidad es una inquietud cada vez más grande de la sociedad, pero en contraparte es necesario garantizar el derecho a la identidad de las personas de la manera más eficiente y segura posible. Los sistemas de inteligencia artificial destinados a la atención del público en general, han sido intentos que no han logrado una aceptación. La realidad es que cualquier persona ha caído en la frustración de hacer una llamada telefónica y encontrarse con una máquina contestadora que da opciones interminables sin que se puedan exponer sus motivos, deberá considerarse la implementación de la IA en materia de difusión y orientación, pero nunca para sustituir una atención personalizada y menos cuando se requiera una solución discrecional ética que beneficie al ciudadano.



¿QUÉ CAMBIOS, OPORTUNIDADES O AMENAZAS REPRESENTA PARA LA IP Y GOBIERNO LA PROLIFERACIÓN EN EL USO DE LA INTELIGENCIA ARTIFICIAL?

La IA al igual que cualquier tecnología representa una infinidad de aplicaciones para el ciudadano, sin embargo, la misma tecnología puede ser utilizada para cometer o facilitar delitos. Pienso que el principal riesgo es la falta de seguridad en los sistemas gubernamentales, que se han visto vulnerados más de una vez, recordemos que en varias ocasiones se han denunciado la venta de base de datos que contienen nuestra información privada. Entonces lo primero es garantizar al ciudadano que su información biométrica está resguardada con los niveles de seguridad adecuados, y que solo es usada con fines lícitos y éticos.

Haciendo una similitud con lo que pasa en iniciativa privada, son muchos los litigios y cuestionamientos que se han hecho en contra de diferentes redes sociales por exponer los datos personales y pérdida de información de los usuarios, que representa un gran valor para otras empresas privadas que desean hacer una publicidad enfocada. En Estados Unidos y Europa, las bases de datos con la información privada que contiene la movilidad (enfermedades) de las personas tiene un alto valor, es similar en México, pero pocos somos los que nos preocupamos de que nuestro expediente médico del hospitales públicos o privados sea vendido a empresas farmacéuticas.

Es importante destacar que es necesario la regulación de la inteligencia artificial, sobre todo porque es posible realizar videos, audios, imágenes que son falsas y que es muy difícil ya en este momento el poder distinguir a simple vista, lo que puede causar un daño reputacional muy grave tanto para las personas comunes como para los funcionarios públicos.

Una oportunidad que también genera mucho debate es el uso de la inteligencia artificial en los procesos de fiscalización y rendición de cuentas. Existen limitaciones legales, leyes, jurisprudencias, reglamentos y criterios jurídicos que no permiten hacer una explotación de las bases de datos nacionales como se hacen con las redes sociales, podemos mencionar algún ejemplo: Es completamente viable el poder integrar la información del sistema financiero, con la declaración de hacienda, el registro público de la propiedad e incluso el registro vehicular, para identificar incongruencias en las declaraciones, ingresos y bienes. Sin embargo, aclaro, esto no es legal en este momento y solo puede tenerse acceso a esta información por un mandato judicial.

Los procesos de fiscalización de la cuenta pública pueden ser indiscutiblemente realizados apoyados por la inteligencia artificial aprovechando la información contenida en los diferentes entes públicos, la armonización contable, los estados de cuenta en formato XML, así como las facturas electrónicas nos permiten hacer un análisis de la cuenta pública utilizando la inteligencia artificial y haciendo eficiente el proceso de fiscalización, destinando los recursos disponibles solo a aquellas operaciones que son incongruentes.

¿CUÁLES CONSIDERAN SON LOS PRINCIPALES RETOS Y OBSTÁCULOS A VENCER PARA IMPLEMENTAR SOLUCIONES QUE UTILICEN INTELIGENCIA ARTIFICIAL?

Como ya mencionamos es indispensable el que las entidades privadas y gubernamentales inviertan en seguridad de información, que sean actualizados los sistemas y bases de datos donde se encuentra la información privada de los ciudadanos con sistemas encriptados, y con una rastreabilidad detallada que permita identificar cualquier fuga de información. Se debe entender el día de hoy que la seguridad de la información no es gasto opcional es una inversión que debe estar presente en el presupuesto de egresos, incluso de manera explícita como una partida presupuestal específica. Falta de una legislación específica, que el día de hoy en todo el mundo está en proceso de diseñarse es sin duda una herramienta necesaria para regular el uso.

El entendimiento de que la IA no debe reemplazar el criterio humano, y estar conscientes que algunos softwares de inteligencia artificial están diseñados para buscar información de manera autónoma en la red, por lo tanto, esta información puede ser no fiable, e incluso contener información falsa o tendenciosa, ya que se considera aquella información que aparece con más recurrencia.

Personalmente pienso que la IA debe considerarse para aumentar la capacidad de servicio, la seguridad pública y privada, las predicciones y escenarios que puedan apoyar la toma de decisiones, la IA nunca deberá ser considerada para reemplazar al personal humano y menos su criterio en operaciones de seguridad, salud, y menos militares.

Por su parte, el uso de la inteligencia artificial en la UE estará regulado por la Ley de Inteligencia Artificial, la primera ley integral sobre IA del mundo (2).

Como parte de su estrategia digital, la UE quiere regular la inteligencia artificial (IA) para garantizar mejores condiciones de desarrollo y uso de esta tecnología innovadora. La IA puede aportar muchos beneficios, como lo son una mejor asistencia sanitaria, un transporte más seguro y limpio, una fabricación más eficiente y una energía más barata y sostenible.

(2) Ley de IA de la UE: primera normativa sobre inteligencia artificial | Noticias | Parlamento Europeo. (2023, 6 diciembre). Parlamento Europeo. <https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ueprimera-normativa-sobre-inteligencia-artificia>

En abril de 2021, la Comisión propuso el primer marco regulador de la UE para la IA. Propone que los sistemas de IA que puedan utilizarse en distintas aplicaciones se analicen y clasifiquen según el riesgo que supongan para los usuarios. Los distintos niveles de peligro implicarán una mayor o menor regulación. Una vez aprobadas, serán las primeras normas del mundo sobre IA.

Ley de IA: normas diferentes para niveles diferentes de riesgo

La nueva normativa establece obligaciones para proveedores y usuarios en función del nivel de riesgo de la IA. Aunque muchos sistemas de IA plantean un riesgo mínimo, es necesario evaluarlos todos.

Riesgo inaceptable

Los sistemas de IA de riesgo inaceptable son los que se consideran una amenaza para las personas y serán prohibidos. Incluyen:

- manipulación cognitiva del comportamiento de personas o grupos vulnerables específicos: por ejemplo, juguetes activados por voz que fomentan comportamientos peligrosos en los niños
- puntuación social: clasificación de personas en función de su comportamiento, estatus socioeconómico o características personales
- sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial.

- Aunque existen algunas excepciones a esta calificación. Por ejemplo, los sistemas de identificación biométrica a distancia “a posteriori”, en los que la identificación se produce tras un retraso significativo, se permitirán para perseguir delitos graves y sólo cuando haya previa aprobación judicial.

Alto riesgo

Los sistemas de IA que afecten negativamente a la seguridad o a los derechos fundamentales se considerarán de alto riesgo y se dividirán en dos categorías.

1. Los sistemas de IA que se utilicen en productos sujetos a la legislación de la UE sobre seguridad de los productos. Esto incluye juguetes, aviación, automóviles, dispositivos médicos y ascensores.

2. Los sistemas de IA pertenecientes a ocho ámbitos específicos que deberán registrarse en una base de datos de la UE:

- a) identificación biométrica y categorización de personas físicas
- b) gestión y explotación de infraestructuras críticas
- c) educación y formación profesional
- d) empleo, gestión de trabajadores y acceso al autoempleo
- e) acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas
- f) aplicación de la ley

- g) gestión de la migración, el asilo y el control de fronteras
- h) asistencia en la interpretación jurídica y aplicación de la ley.

Todos los sistemas de IA de alto riesgo serán evaluados antes de su comercialización y a lo largo de su ciclo de vida.

LOS SISTEMAS DE IA DE RIESGO LIMITADO DEBEN CUMPLIR UNOS REQUISITOS MÍNIMOS DE TRANSPARENCIA QUE PERMITAN A LOS USUARIOS TOMAR DECISIONES CON CONOCIMIENTO DE CAUSA.

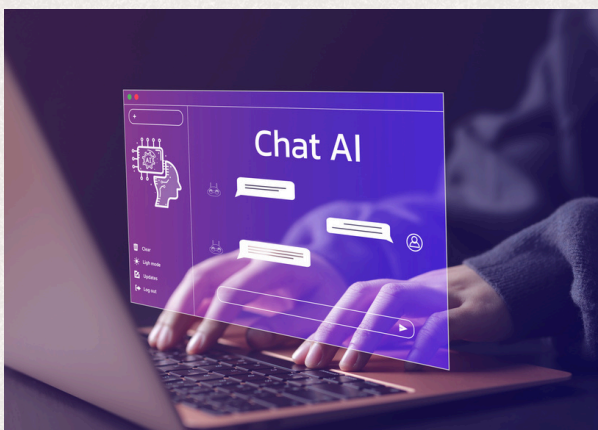
IA generativa

La IA generativa, como ChatGPT, tendría que cumplir requisitos de transparencia:

- revelar que el contenido ha sido generado por IA
- diseñar el modelo para evitar que genere contenidos ilegales
- publicar resúmenes de los datos protegidos por derechos de autor utilizados para el entrenamiento

Riesgo limitado

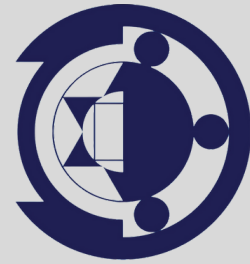
Los sistemas de IA de riesgo limitado deben cumplir unos requisitos mínimos de transparencia que permitan a los usuarios tomar decisiones con conocimiento de causa. Tras interactuar con las aplicaciones, el usuario puede decidir si desea seguir utilizándolas. Los usuarios deben ser conscientes de cuándo están interactuando con la IA. Esto incluye los sistemas de IA que generan o manipulan contenidos de imagen, audio o vídeo (por ejemplo, deepfakes).



SÉ PARTE DE NOSOTROS

AFÍLIATE A NUESTRO COLEGIO **CISCIG**

Intégrate a la red más importante en México de ingenieros en sistemas computacionales para la seguridad de la información, control interno y gobernanza



BENEFICIOS

- Networking
- Capacitación y actualización
- Apoyo y acompañamiento
- Participación y redacción en la Revista CISCIG



Suscripción anual \$3,000 mxn

REGÍSTRATE EN WWW.CISCIG.MX

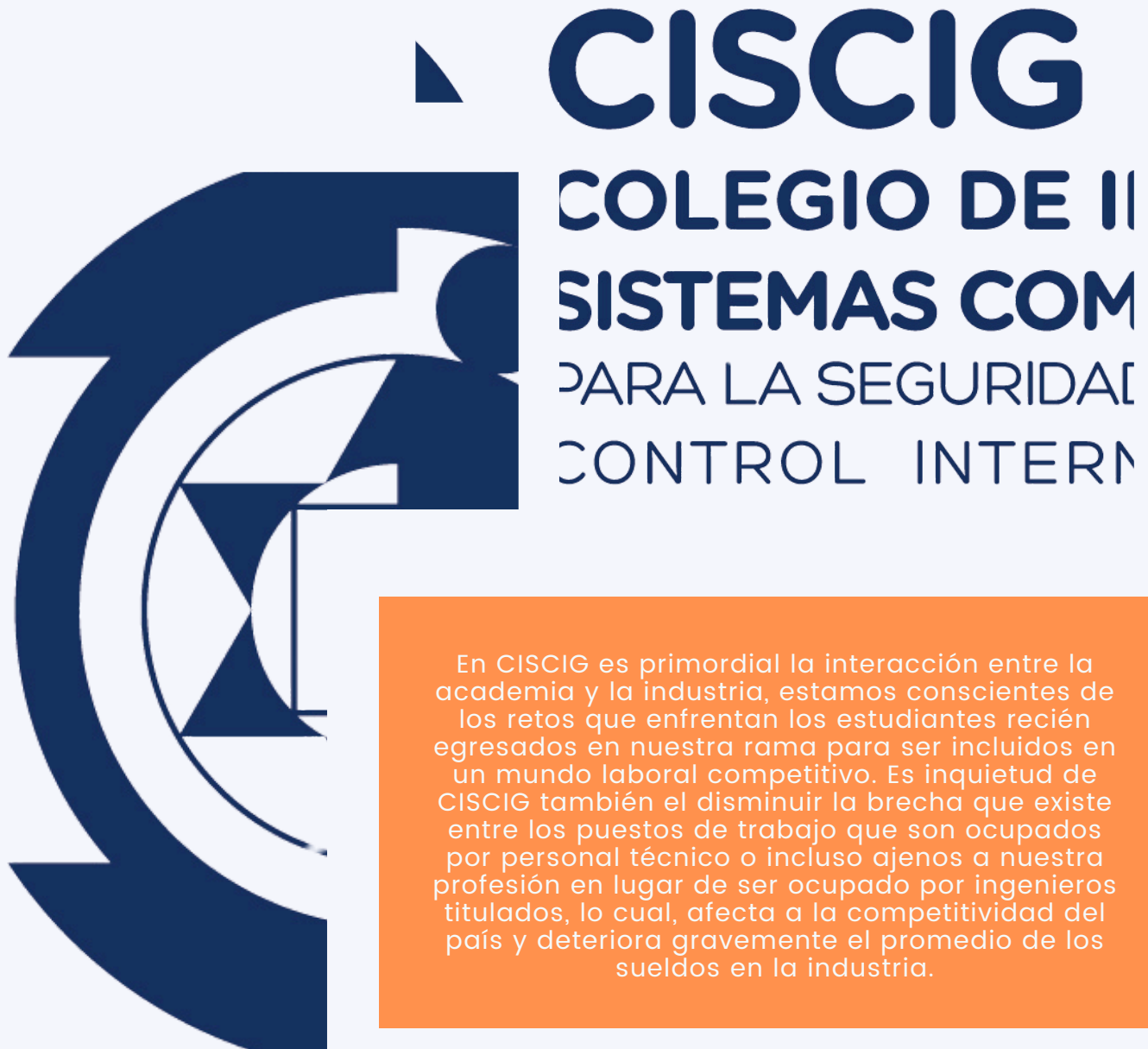
Contamos con reconocimiento por la Dirección de Profesiones de la SEP, el mes de 2 de mayo de 2019, con el oficio F-469, DGP/363-11/2019.



COMUNIDAD DE APRENDIZAJE

EN NUESTRO MODELO, UNA ENTIDAD EDUCATIVA ADECUA LOS PROYECTOS DE SUS MATERIAS MAS AVANZADAS PARA QUE LOS ESTUDIANTES DESARROLLEN UN PROYECTO QUE SERÁ DE APLICACIÓN INMEDIATA EN UNA EMPRESA O ENTIDAD PÚBLICA.





CISCIG

COLEGIO DE INGENIEROS EN
SISTEMAS COMPUTACIONALES
PARA LA SEGURIDAD Y
CONTROL INTERNO

En CISCIG es primordial la interacción entre la academia y la industria, estamos conscientes de los retos que enfrentan los estudiantes recién egresados en nuestra rama para ser incluidos en un mundo laboral competitivo. Es inquietud de CISCIG también el disminuir la brecha que existe entre los puestos de trabajo que son ocupados por personal técnico o incluso ajenos a nuestra profesión en lugar de ser ocupado por ingenieros titulados, lo cual, afecta a la competitividad del país y deteriora gravemente el promedio de los sueldos en la industria.

¿COMO FUNCIONA UNA "COMUNIDAD DE APRENDIZAJE"?

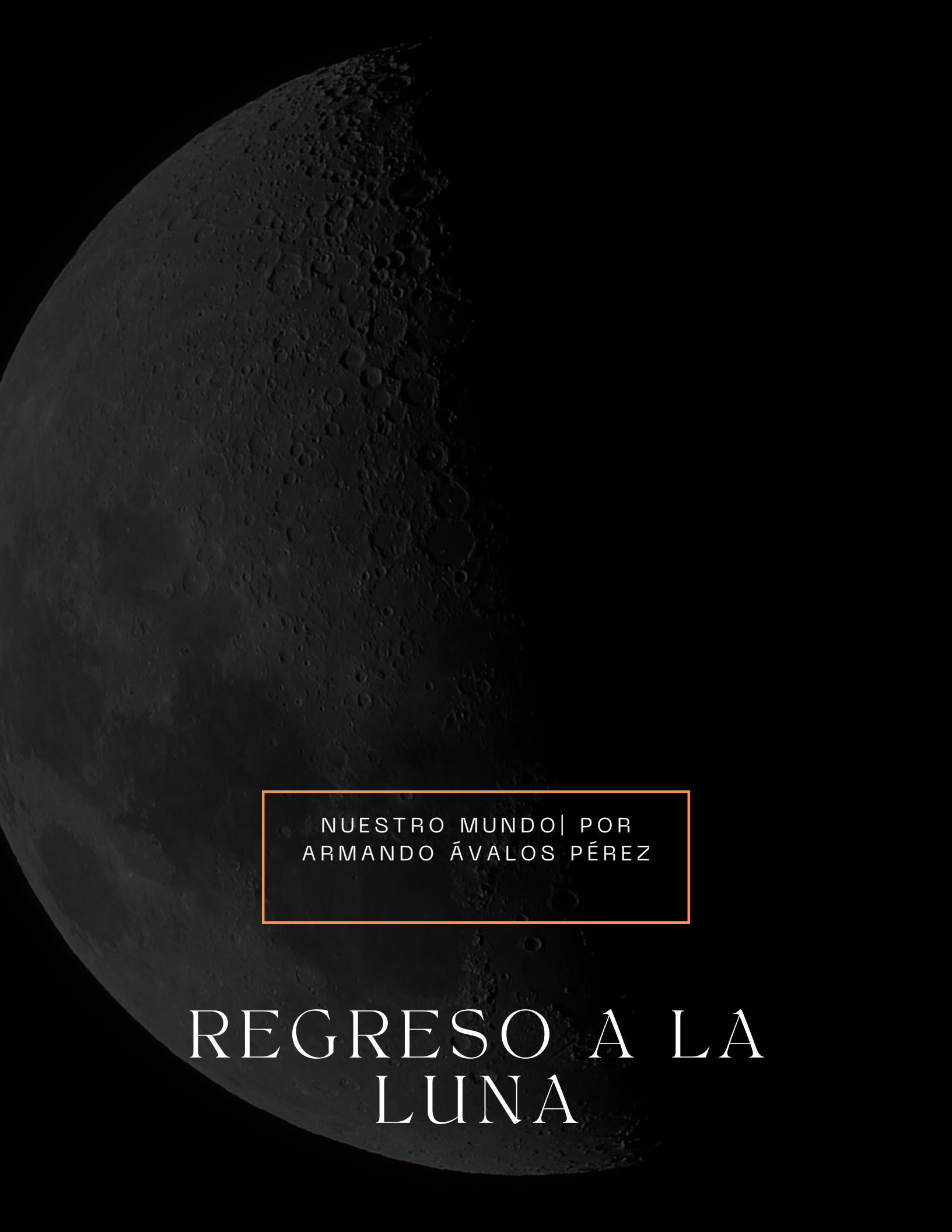
En nuestro modelo, una entidad educativa adecua los proyectos de sus materias mas avanzadas para que los estudiantes desarrollen un proyecto que será de aplicación inmediata en una empresa o entidad pública. En esta comunidad se tienen cuatro actores principales:

- La entidad educativa y profesores de la asignatura
- Los profesionales voluntarios que orientarán el proyecto
- El CISCIG como facilitador
- Los alumnos que desarrollarán el proyecto.

Los alcances del proyecto, metodología a utilizar, aspectos técnicos, así como acuerdos de seguimiento son acordados entre los profesores, los profesionales voluntarios y CISCIG; los alumnos serán encargados de materializar el proyecto siguiendo de manera estricta la metodología acordada y las mejores prácticas a implementar.



SI ERES UN
PROFESIONISTA
CON AMPLIA
EXPERIENCIA,
TRABAJAS EN EL
SECTOR
PÚBLICO O
PRIVADO Y
TIENES LA
NECESIDAD DE
UNA
APLICACIÓN O
SISTEMA O BIEN,
EN TU
FACULTAD
REQUIEREN
OBTENER
EXPERIENCIA A
TRAVÉS DE
CASOS
PRÁCTICOS,
PONTE EN
CONTACTO CON
EL **CISCIG**.



NUESTRO MUNDO | POR
ARMANDO ÁVALOS PÉREZ

REGRESO A LA LUNA

Los últimos años hemos visto como se ha incrementado el presupuesto de los programas gubernamentales de diferentes países en su carrera por establecer estaciones espaciales, sondas lunares y futuras bases lunares. Todo lo anterior hace despertar una serie de interrogantes que abarcan desde las tendencias de conspiraciones gubernamentales a desarrollo tecnológicos y explotación de recursos fuera de nuestro planeta. Lo primero que considero es la gran pregunta ¿Por qué?, es inquietante que teniendo enfrente una crisis mundial económica, social, política y un reordenamiento global, los países destinen recursos económicos a una odisea incierta.

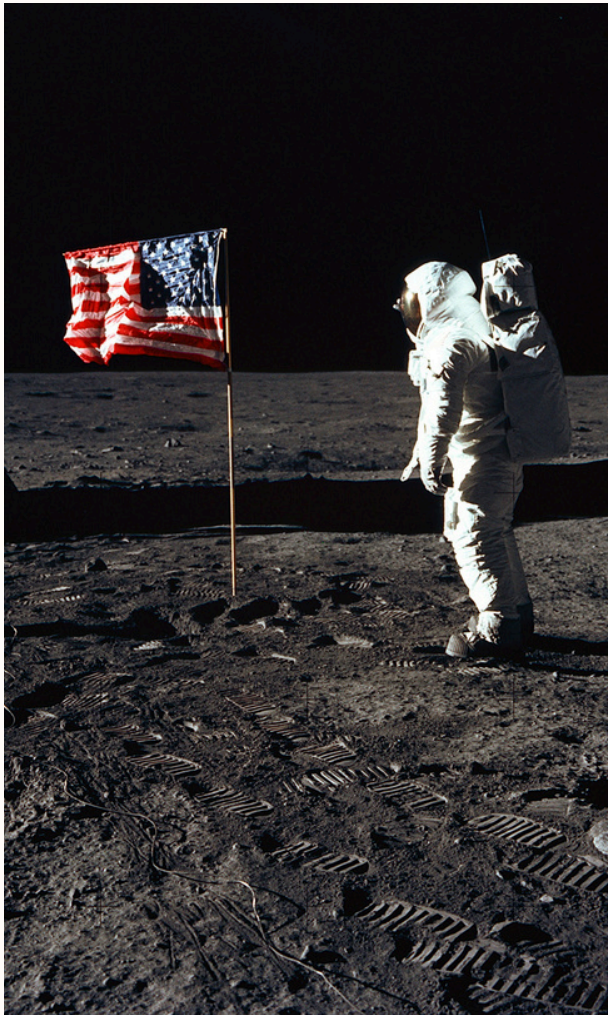
ES INQUIETANTE QUE TENIENDO ENFRENTA UNA CRISIS MUNDIAL ECONÓMICA, SOCIAL, POLÍTICA Y UN REORDENAMIENTO GLOBAL, LOS PAÍSES DESTINEN RECURSOS ECONÓMICOS A UNA ODISEA INCIERTA



¿Qué responde mi razonamiento?

Mi lógica me indica que a través de las nuevas tecnologías de exploración que han evolucionado desde finales de los años 60's y 70's, (recordemos que el último viaje de la serie Apolo fue el Apolo 17 el 7 de diciembre de 1972) estos nuevos métodos de exploración a través de satélite han permitido identificar los yacimientos de petróleo, minerales y hasta usos en antropología, logrando escanear densas selvas en el centro y sur de América mapeando antiguos restos de ciudades desaparecidas en medio de la maleza. Bajo mi razonamiento, no existiría una inversión de semejante magnitud si no hubiera un beneficio económico explícito, superior al de la exploración terrestre. Pero el despliegue de satélites es otro tema que abordaré en otro artículo, ya que en este despliegue visualizo riesgos y fines que van más allá de las comunicaciones y que podrían estar enfocados a espionaje e incluso con fines militares.

LA CARRERA POR REGRESAR A LA LUNA NO ES ÚNICA DE ESTADOS UNIDOS Y LOS PAÍSES DE LA OTAN, PAÍSES COMO CHINA, INDIA Y RUSIA HAN ENVIADO SUS PROPIAS SONDAS LUNARES.



¿Entonces, cuál es el fin real de las exploraciones a la luna y marte?

La anterior es una pregunta que solo podré plantearme, mas no podría contestarse en este artículo de manera concreta y verás. Antes de hablar de la finalidad de las sondas espaciales y los eventos recientes, pongamos en contexto la realidad global; Las generaciones presentes estamos viviendo eventos sin precedentes, que algunos ya consideran con el adjetivo de “apocalípticos” en el que vemos un creciente descontento social, que no está siendo exclusivo del llamado “tercer mundo”, en donde las llamadas “oleadas de migración” han tomado por sorpresa a los países desarrollados con grandes cantidades de migrantes desplazados por el hambre, la guerra y el colapso de sistemas fallidos.

En otra mano tenemos una clase cada vez menos de empresas y personas que acumulan la riqueza global, y que las crisis globales y bien conocida pandemia de COVID han dejado con mayor riqueza. Entonces porque destinar miles de millones en exploración a la luna y marte.

Sin embargo, los países “desarrollados” también se encuentran en una situación financiera grave, similar a la que precedió el famoso jueves negro de 1929 hace ya casi un siglo, y podemos ver por ejemplo en EU el creciente número de “homeless” más parecido a los años 30’s que a los “vagos” de finales de siglo.



La carrera por regresar a la luna no es única de estados unidos y los países de la OTAN, países como China, India y Rusia han enviado sus propias sondas lunares, y en el caso de Rusia y China creando sus propias “estaciones espaciales” separándose de la estación internacional, lo que tiene el fin evidente el de proteger el conocimiento y datos obtenidos de las sondas propias.

Mencionemos algunas actividades espaciales de relevancia recientes:

1. [BBC News Mundo, 26 octubre 2020](#) . [En la Luna hay agua](#). La Administración Nacional de Aeronáutica y el Espacio (NASA, por sus siglas en inglés) confirmó este lunes que detectaron presencia del líquido en varios cráteres del satélite natural de la Tierra. El hallazgo fue realizado en la superficie iluminada de la Luna con ayuda del observatorio SOFIA, un telescopio infrarrojo aerotransportado, el más grande de su tipo en el mundo.

2. El 16 de noviembre de 2022, el cohete más poderoso jamás lanzado [La misión no tripulada, conocida como Artemis I](#), es un paso crítico en la campaña de la NASA para llevar humanos a la Luna por primera vez en más de 50 años. Si todo sale según lo planeado, los primeros astronautas aterrizarán en la superficie lunar en 2025, seguidos de una serie de misiones para establecer una presencia sostenida (2).

3. [China lanzó la nave espacial tripulada Shenzhou-16](#) el 30 de mayo de 2023. Fue la primera misión tripulada de la etapa de aplicación y desarrollo de la estación espacial china. Su tripulación, que permaneció en órbita durante 154 días, realizó un total de 70 experimentos espaciales, realizó una caminata espacial, pronunció una conferencia desde la estación espacial y ayudó en varias ocasiones con el movimiento de carga (3).

4. BBC News Mundo, 20 agosto 2023. Luna-25, la primera sonda lanzada por Rusia hacia la Luna desde 1976, se estrelló contra el satélite terrestre. Roscosmos, la empresa espacial estatal rusa, comunicó que había perdido contacto con la nave el sábado, tras un problema en el momento de ponerla en órbita antes del aterrizaje. Luna-25 de Rusia se estrelló contra la Luna después de perder el control, dicen las autoridades. Se suponía que la nave espacial no tripulada sería la primera en aterrizar en el polo sur de la Luna, pero no lo consiguió (4).

5. BBC News Mundo, 23 agosto 2023, “¡India está en la Luna!”. Con estas palabras el primer ministro indio, Narendra Modi, celebró que su país se convirtiera este miércoles en la primera nación en aterrizar una nave no tripulada cerca del polo sur del satélite natural de la Tierra. La misión Chandrayaan-3 consiguió llevar un módulo, el cual contiene un vehículo guiado a control remoto que recorrerá esta inexplorada zona de la Luna, para buscar hielo a base de agua (5).

Resulta evidente que la explotación de recursos minerales es el fin de la nueva etapa de exploración a la Luna, pero ¿qué minerales han sido encontrados?, ¿cómo puede ser posible que la explotación lunar sea más lucrativa que un sustituto o explotación en la tierra? En un futuro artículo hablaremos de los “Acuerdos de Artemisa” que plantea las “reglas” para la explotación de minerales en la luna, propuesto por Estados Unidos.



1 BBC News Mundo. (2020, 26 octubre). Agua en la Luna: La NASA confirma la existencia de agua en la superficie iluminada del satélite de la Tierra. BBC News Mundo. <https://www.bbc.com/mundo/noticias-54697135>

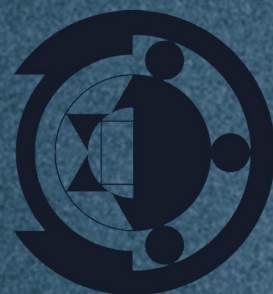
2 National Geographic España. (2023, 7 noviembre). National Geographic. <https://www.nationalgeographic.com/espacio/2022/11/regreso-a-la-luna-el-artemis-i-finalmente-fue-lanzado>

3 Newsroom Infobae. (2023, 31 octubre). Tres taikonautas vuelven de la estación espacial China tras cinco meses. infobae. <https://www.infobae.com/america/agencias/2023/10/31/tres-taikonautasvuelven-de-la-estacion-espacial-china-tras-cincomeses/>

4 Redacción. (2023, 20 agosto). Viaje a la Luna: La nave rusa Luna-25 se estrelló contra el satélite terrestre cuando se dirigía a explorar el Polo Sur. BBC News Mundo. <https://www.bbc.com/mundo/articles/cv230jyd737o>

5 Redacción. (2023b, agosto 23). Luna: India hace historia al convertirse en el primer país en aterrizar una nave no tripulada en el polo sur de nuestro satélite. BBC News Mundo. <https://www.bbc.com/mundo/articles/c3gzwlqly33o>

CISCIG



SOMOS UNA AGRUPACIÓN OFICIAL DE INGENIEROS EN SISTEMAS COMPUTACIONALES AVALADOS POR LA DIRECCIÓN DE PROFESIONES DE LA SEP ORGANIZADOS COMO GREMIO PARA TOMAR DECISIONES SOBRE NUESTRO QUEHACER PROFESIONAL, CERTIFICAR AL SECTOR EN TEMAS DE INGENIERÍA EN SISTEMAS COMPUTACIONALES Y TECNOLOGÍA Y PROMOVER LAS MEJORES PRÁCTICAS EN LA INDUSTRIA.



CONTRASEÑAS FUERTES Y ÚNICAS



02

- Tu contraseña debe tener al menos 12 caracteres.
- Usa una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Evita usar palabras comunes, nombres, fechas de nacimiento o patrones obvios.
- Cada cuenta debe tener una contraseña diferente.

01

¿POR QUÉ ES IMPORTANTE?

Es la primera línea de defensa
contra el acceso no autorizado a
tus cuentas.

HERRAMIENTAS PARA GESTIONAR CONTRASEÑAS

Considera un gestor de contraseñas. Estas aplicaciones almacenan de manera segura y te ayudan a generar contraseñas fuertes para cada cuenta. Algunos populares incluyen:

- LastPass
- 1Password
- Dashlane
- Bitwarden

03

04

CONSEJOS ADICIONALES

- Activar la autenticación de dos factores (2FA): Requiere no solo la contraseña sino también un 2º factor.
- Actualizar tus contraseñas regularmente: Periódicamente y no reutilices.
- Evitar el uso de redes Wi-Fi públicas: Considera utilizar una Red Privada Virtual (VPN) para cifrar tu conexión.
- Mantener tu software actualizado: Para protegerte contra las vulnerabilidades.



LO MISMO 30 AÑOS DESPUÉS

Hace ya demasiados años, diría yo “Vidas pasadas”, trabajaba para una empresa de logística, en la frontera norte, aunque la telefonía celular empezaba a ser de uso común en ese tiempo no era “obligado” tener un teléfono celular y mucho menos que lo pusiera uno a disposición de la empresa o patrón. Los “bíper” eran de uso más generalizados para la gente de tecnología de información. Entre los mas bellos recuerdos que tengo esta la sensación de poder hacer y estar donde yo quisiera, sentimiento que ha ido desapareciendo tan lentamente que no fue perceptible su pérdida, permítanme explicarles. Cuando entre los compañeros de trabajo se distribuían el bíper y los radios de comunicación, había cierto estrés y angustia por NO SER SELECCIONADO para tan innovadora herramienta tecnológica, si han leído bien, NO QUERÍAMOS que se nos asignara uno de estos dispositivos ya que era una indudable condena a perder la tan anhelada libertad que se tenía.

El ser condenado a usar uno de esos dispositivos era equivalente a tener una cadena sujeta al tobillo con una bola de hierro, castigo medieval para los prisioneros.



El tener un bíper o radio facilitaba a los gerentes y directores la localización en todo tiempo y sin excusa del colaborador, para literalmente, solicitar todo lo que se les pudiera ocurrir a lo hora que se ocurriera. El personal de tecnología de información vivíamos con la angustia de los llamados “sistemas de misión crítica” que no pueden ser interrumpidos por ninguna circunstancia ya que causaban pérdidas millonarias, y uno comprometido y con la camiseta bien puesta, tomaba la interrupción como algo personal, imposible de suceder.

La pregunta es; ¿En qué momento de mi vida, estuve tan locamente aturdido que yo mismo me puse un dispositivo de este tipo?, ¿te has preguntado eso?

Es melancólico el recordar aquellas épocas donde conseguir el teléfono del amor platónico era parte del cortejo, esos días donde tenías una comunicación con tus familiares, amigos y colegas sin que estos tuvieran el teléfono pegado a la cintura, y que decir de las maravillosas citas con la persona amada, que se concretaban con una llamada de apenas un minuto y llegar a los reuniones, oficinas, tiendas, y cualquier lugar con un mapa impreso o las típicas instrucciones incompletas, y aun así, nos reuníamos y llegábamos puntuales.



Claro que también hacíamos esas llamadas interminables por las noches con nuestros seres queridos, a pesar de lo costoso del pago por minuto.

Lo que me indigna el día de hoy es la posición generalizada que se ha adoptado, en la que por enviar un mensaje se da por hecho inequívocamente que será atendido, cuando fue sustituyendo la comunicación efectiva por las “dos palomitas azules” del WhatsApp; el abuso ha llegado a todos los ámbitos, no solo el laboral, también el personal, en el que se ha perdido la comunicación efectiva por un abuso de la tecnología y un mensaje es un “hecho”.

¿Volverá el tiempo cuando podamos dejar el celular del trabajo y limitarlo a horarios laborales? ¿Será posible que la gente entienda que no tienes el celular en la mano y que lo atenderás cuando en un tiempo prudente y efectivo?

No lo creo, irónicamente las aplicaciones que diariamente se desarrollan para los llamados teléfonos inteligentes están enfocadas a mantener la atención de las personas. Pero lo más triste es que le gente se ha hecho una doble vida, con imágenes falsas, descripciones falsas y ahora hasta rostros falsos y que poco a poco, esa vida falsa se ha tornado incluso en si vida real.

Yo por mi parte, sigo disfrutando y agradeciendo las horas que he pasado con mi pareja, con mi hija, mis amigos; los caminos por el parque, los largos viajes y paseos, las comidas y anheladas sobre mesas, en las que, de común acuerdo sin decirlo explícitamente, los celulares permanecen apagados o solo son usados para reproducir una amena, adecuada y placentera melodía.

Sin duda, escucho los reclamos, “no él no contesta, solo cuando quiere”, o “te envíe un mensaje URGENTE anoche y no me atendiste”. Si, es verdad, llegué a la edad en donde comprendí que el concepto URGENTE solo aplica a los intereses propios



UN AÑO

MÁS DE



ACTIVIDADES

Hemos concluido un
año más de
operaciones en CISCIG
y queremos agradecer
a nuestros socios por
su participación y
colaboración en las
diferentes actividades
que hemos realizado a
lo largo del presente
año.



Participa en nuestros
diferentes proyectos y
lleva tu carrera profesional
al siguiente nivel
Pregunta cómo puedes
participar en:

- Comités Nacionales
- Comités Técnicos
- Articulista para nuestra revista
- Instructor y Conferencista
- Webinar
- Comunidades de Aprendizaje
- Comités de mejores prácticas

**Se parte de la
red de
profesionales
a nivel
nacional.**



CISCIG
COLEGIO DE INGENIEROS EN
SISTEMAS COMPUTACIONALES
PARA LA SEGURIDAD DE LA INFORMACIÓN,
CONTROL INTERNO Y GOBERNANZA.

Costos: \$15,000 más 16% de iva y \$200 de costo de envío



CISCIG
COLEGIO DE INGENIEROS EN
SISTEMAS COMPUTACIONALES
PARA LA SEGURIDAD DE LA INFORMACIÓN,
CONTROL INTERNO Y GOBERNANZA.

Certificaciones por experiencia



1

**PROFESIONAL
CERTIFICADO EN
ADMINISTRACIÓN DE
CENTROS DE DATOS
(PCACD)**



2

**PROFESIONAL
CERTIFICADO
EN REDES Y
COMUNICACIONES
(PCRC)**



3

**PROFESIONAL
CERTIFICADO
EN SEGURIDAD
DE
INFORMACIÓN
(PCSI)**



4

**PROFESIONAL
CERTIFICADO EN
AUDITORÍA DE
TECNOLOGÍAS DE
INFORMACIÓN
(PCATI)**



5

**PROFESIONAL
CERTIFICADO EN
ADMINISTRACIÓN
DE PROYECTOS DE
TECNOLOGÍAS DE
INFORMACIÓN
(PCAPT)**



6

**PROFESIONAL
CERTIFICADO
EN
DESARROLLO
DE SOFTWARE
(PCDS)**



7

**PROFESIONAL
CERTIFICADO
EN ANÁLISIS Y
MINERÍA DE
DATOS
(PCAMD)**



8

**PROFESIONAL
CERTIFICADO
EN CONTROL
INTERNO Y
GOBERNANZA
(PCCIG)**



9

**PROFESIONAL CERTIFICADO EN
MARKETING DIGITAL (PCAMD)**

SERVICIOS@CISCIG.MX

WHATSAPP: : + 52 55 3516 7586

PARA MAYOR INFORMACIÓN, COMUNÍCATE CON NOSOTROS.



CISCIG

**COLEGIO DE INGENIEROS EN
SISTEMAS COMPUTACIONALES**
PARA LA SEGURIDAD DE LA INFORMACIÓN
CONTROL INTERNO Y GOBERNANZA



+52 55 6736 9071

+ 52 55 3516 7586



servicios@ciscig.mx



www.ciscig.mx



CISCIG 2024

Las opiniones expresadas por los autores no necesariamente reflejan la postura del Colegio de Ingenieros en Sistemas Computacionales para la Seguridad de la Información, Control Interno y Gobernanza A.C. El propósito de la revista es presentar la opinión de ponentes, divulgar información científica y tecnológica. La Revista CISCIG NO cobra por la publicación de artículos a los autores ni por la lectura de sus contenidos a los lectores vía web, y está adherida a la filosofía de acceso abierto y permite la divulgación libre del contenido de los artículos por parte de los autores y los lectores siempre y cuando sea citado su contenido con rigor de acuerdo a las normas de citación APA 6ta edición. Esta práctica es equivalente a la licencia Creative Commons tipo Atribución-No Comercial CC BY-NC. Revista editada por el Colegio de Ingenieros en Sistemas Computacionales para la Seguridad de la Información, Control Interno y Gobernanza A.C.