revista
CISCIG
REVISTA DEL COLEGIO DE INGENIEROS EN SISTEMAS DE COMPUTACI
SEGURIDAD DE LA INFORMACIÓN, CONTROL INTERNO Y G
Año 1, Número 01

IMPLEMENTACIÓN DE CONTROLES GENERALES DE TI EN UNA ORGANIZACIÓN

¿PROCESADORES LOONGSON EN CHINA?

La decisión podría significar menor dependencia de Occidente

Los riesgos de la

Inteligencia Artificial

Aplicaciones de inteligencia artificial que intentan predecir la aceptación o incluso las acciones de las persona

Número ISSN: 2992-7250- Año I, volumen I, septiembre 2023

¿Qué es un colegio de profesionales?

¿Somos una institución educativa?

Somos una instancia de opinión crítica en busca de garantía de calidad y certeza en el ejercicio profesional.

Muchas veces se utilizan como sinónimos por lo que al nombrarnos como colegio se confunde con su acepción educativa. Entendemos que existe una confusión entre ambos conceptos. En el ámbito académico ambas palabras se emplean como sinónimos, sin embargo, nosotros somos un colegio profesional, que es distinto a una institución educativa.

Los colegios profesionales son corporaciones del derecho público de carácter gremial dedicado a quienes ejercen las profesiones.

Así, nuestro Colegio no es una escuela ni una institución educativa, aunque ofrece servicios relacionados con la certificación y preparación profesional, sin embargo, tiene funciones distintas a las de una escuela, universidad o centro educativo. Somos una asociación civil sin fines de lucro avalada ante la Dirección General de Profesiones (SEP), formada por profesionistas de una misma área, interesados en agruparse para trabajar en beneficio de su profesión.

Una instancia de opinión crítica en busca de garantía de calidad y certeza en el ejercicio profesional. Responsable de promover acciones en beneficio de la población a través del servicio social profesional, con la finalidad de elevar la calidad de vida de la comunidad.

Emitimos dictámenes en determinadas situaciones, tanto a organismos públicos como privados y estamos sujetos a la defensa de los intereses profesionales de los colegiados.

El Colegio logró su 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. Y actualmente contamos con más de 800 asociados de los 32 Estados de la República.

Propósitos de los colegios de profesionales

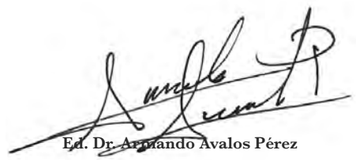
Los colegios de profesionistas son asociaciones civiles no lucrativas formadas por profesionistas de una misma rama académica, interesadas en agruparse para trabajar en beneficio de su profesión.

Desde el Colegio de Ingenieros en Sistemas Computacionales para la Seguridad de la Información, Control Interno y Gobernanza, buscamos coadyuvar a la superación del ejercicio profesional y vigilar que su práctica se realice dentro del más alto plano legal y ético.

Entre las funciones y atribuciones del Colegio se tienen:

- Actividades de consultoría.
- Actualización profesional.
- Vinculación y colaboración con el sector educativo y empresarial
- Emisión de certificaciones
- Promueve la expedición de leyes y reglamentos.
- Servir de árbitro en conflictos.
- Formación de peritos profesionales por especialidad.

Te invitamos a formar parte de esta asociación y participar activamente en nuestros programas de profesionalización.



Ed. Dr. Armando Avalos Pérez
Presidente

Inscríbete al colegio, www.ciscig.mx/registro
Envía tu información a: servicios@ciscig.mx
Comunícate con nosotros
Tel/WhatsApp 55 3516 7586

Ve a ciscig.mx y conoce más sobre nuestro Colegio.

Afíliate al Colegio

El trámite es gratuito por tiempo limitado y se puede realizar en línea. Solo te pedimos algunos datos y en menos de una semana podrás recibir todos los beneficios de ser parte de nuestro colegio.

¿Quieres publicar?

Si te gustaría escribir en esta revista, puedes escribirnos a servicios@ciscig.mx y con gusto te facilitamos toda la información y puedas incorporarte a nuestro equipo de articulistas.

revista
CISCIG
colegio de ingenieros en sistemas computacionales para la seguridad de la información, control interno y gobernanza, a.c

PRESIDENTE DEL COLEGIO Y DIRECTOR DE LA REVISTA	Armando Ávalos
VICEPRESIDENTE DEL COLEGIO	Diana Elías Palacios
JEFE DE INFORMACIÓN Y REDACCIÓN	Jorge García Alonso
DISEÑO EDITORIAL	Omar Camacho Madrigal
MIEMBROS DE LA MESA DIRECITVA DEL COLEGIO	Armando Ávalos Diana Elías Joaquín Ortiz Luis Castillo Israel Fuentes Verónica Bello Moisés Cambranis Jinmy Aké
COLABORADORES Y ARTICULISTAS	Armando Ávalos Joaquín Ortiz Flores Omar Camacho Madrigal Alejandro Heredia Cobos Miguel Angel Gutiérrez Salazar Jorge García Alonso
CONSEJERO JURÍDICO	Ernesto Alvarado

Número ISSN: 2992-7250- Año I, volumen I, Septiembre 2023

REVISTA DEL COLEGIO DE INGENIEROS EN SISTEMAS DE COMPUTACIONALES PARA LA SEGURIDAD DE LA INFORMACIÓN, CONTROL INTERNO Y GOBERNANZA, A.C, año 1, No. 1, octubre 2023, 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: "En trámite", ambos otorgados por el Instituto Nacional de Derecho de Autor, fecha de última actualización, 22 de mayo de 2023.

CONTENIDO

INNOVACIÓN TECNOLÓGICA

¿Procesadores Loongson chinos en Rusia?
Por Armando Ávalos Pérez **9**

EL FUTURO TECNOLÓGICO

Los riesgos de la Inteligencia Artificial
Por Armando Ávalos Pérez **11**

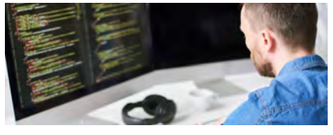
NUESTRO PAÍS

Implementación de Controles Generales de TI en una organización
Por Joaquín Ortiz Flores **16**

NUESTRO MUNDO

Regreso a la Luna
Por Armando Ávalos Pérez **20**

AUDITORÍA Y SEGURIDAD DE INFORMACIÓN



La auditoría y el desarrollo de software
Por Joaquín Ortiz Flores **23**

LO MISMO 30 AÑOS DESPUÉS

Lo mismo 30 años después
Por Armando Ávalos Pérez **27**

MARKETING DIGITAL

Optimización técnica en el posicionamiento SEO como estrategia de marketing
Por Omar Camacho Madrigal **29**

ACTIVIDADES CISCIG

Gestión del Riesgo Operativo: La clave para el éxito de pequeñas empresas
Por Luis Alejandro Heredia Cobos **32**

Importancia de lograr un Título profesional
Por CONAIP **34**

ÉTICA, RESPONSABILIDAD Y MEJORA EN EL SERVICIO PÚBLICO

La mejora del servicio público como objetivo del régimen disciplinario en México
Por Miguel Angel Gutiérrez Salazar **36**

QUÉ PASA EN MÉXICO Y EL MUNDO

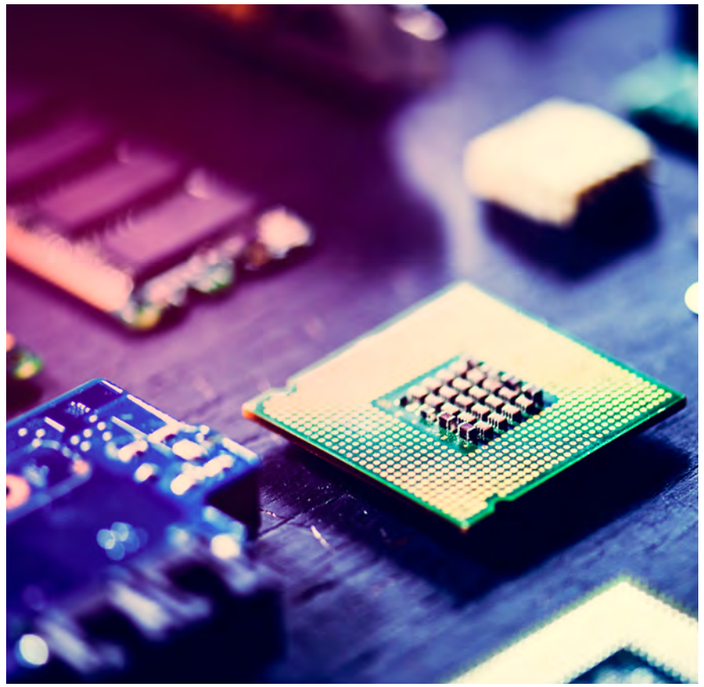
¿Es necesaria la actualización de la Normativa de Control Interno en la administración pública federal?
Por Jorge García Alonso **38**

USER ERROR, ERROR 404

El ingeniero en sistemas y el usuario **42**

¿Procesadores Loongson chinos en Rusia?

El 16 de agosto de 2022, Loongson el fabricante Chino de procesadores y equipos tecnológicos lanza oficialmente el procesador de nueva generación 3A5000 basado en LoongArch.



Según los resultados de las pruebas realizadas por instituciones independientes chinas, el procesador LS3A5000 obtiene más de 26 puntos en operaciones de punto fijo y de punto flotante SPEC CPU2006 de un solo núcleo en un entorno de compilador GCC y más de 80 puntos para cuatro núcleos.

Recientemente, Loongson Technology Co., Ltd. lanzó oficialmente el procesador LS3A5000. Con su importante salto en rendimiento, este producto es el primer procesador que presenta el sistema de instrucciones de desarrollo propio de LoongArch, estableciendo el último hito para las CPU de desarrollo propio de China[1].

El fabricante Loongson tiene previsto la distribución de este procesador solo para China, sin embargo, el desarrollo de un procesador, con un lenguaje y set de instrucciones propios son una noticia relevante ya que presentan una opción a las llamadas "sanciones tecnológicas" establecida por Estados Unidos a la tecnología de ese país.

Por Ed. Dr. Armando Avalos Pérez
armando.avalos@marcg.com.mx

1 *Loongson officially releases the 3A5000 new-generation processor based on LoongArch*. (s. f.). Loongson. https://www.loongson.cn/EN/news/show?id=633

China ha anunciado que siempre sí venderá sus procesadores Loongson a Rusia a casi un año de publicar lo contrario

El desarrollo de un procesador con una capacidad de competir con la tecnología occidental es un tema estratégico para China, ya que es bien sabida la importancia de los procesadores para el desarrollo de la industria militar, en la cual este país también ha sorprendido con su acelerado desarrollo. Es también de pensar y una interrogante válida si este procesador que tiene un gran potencial comercial es el último realmente desarrollado o si existen desarrollos más avanzados que no están disponibles en el mercado común y que explican el desarrollo acelerado de la industria militar y espacial de China, con la cual han sorprendido al mundo.

Durante diciembre del 2022, el ministerio de desarrollo digital de Rusia anuncio que China no vendería sus procesadores Loongson a ese país sin dejar claro el motivo[2]. Se puede suponer que esto es derivado de las sanciones por la guerra de Ucrania, sin que esto sea algo coherente, pero la realidad es que Loongson ha limitado la venta de sus procesadores como ya se ha mencionado solo al mercado chino, por lo que podríamos argumentar también motivos comerciales y estratégicos en vez de una alineación a las sanciones internacionales. Sin embargo, China ha anunciado que siempre si venderá sus procesadores Loongson a Rusia a casi un año de publicar lo contrario[3].

LoongArch recoge la experiencia acumulada durante los 20 años de desarrollo de CPU y construcción del ambiente de Loongson. Desde la microarquitectura de alto nivel hasta funciones de un lenguaje de instrucción y estándares ABI, LoongArch está diseñado de forma independiente sin autorización o licenciamiento de ningún país. Gracias a los últimos logros en la evolución del código de instrucciones, LoongArch cuenta con una eficiencia operativa más alta que nunca. Este procesador considera plenamente los requisitos de un ambiente compatible e integra las principales características funcionales de los principales códigos de instrucción internacionales, como x86 y ARM. Con la acumulación técnica y la innovación de más de 10 años, del equipo de Loongson posé un lenguaje binario, LoongArch que permite la compatibilidad de aplicaciones entre instrucciones y plataformas.

Según los resultados de las pruebas realizadas por instituciones independientes chinas, el procesador LS3A5000 obtiene más de 26 puntos en operaciones de punto fijo y de punto flotante SPEC CPU2006 de un solo núcleo en un entorno de compilador GCC y más de 80 puntos para cuatro

2 Sole, R. (2022, 15 diciembre). *Ni siquiera China venderá sus procesadores a Rusia, ¿qué están ocultando?* HardZone. https://hardzone.es/noticias/procesadores/china-procesador-loongson-distribucion-rusia/

3 Hernández Pablo. (s. f.). *China se retracta: finalmente venderá a Rusia los procesadores Loongson que había prohibido exportar.* Xataca. https://www.msn.com/es-mx/noticias/tecnologia/china-se-retracta-finalmente-vender%C3%A1-a-rusia-los-procesadores-loongson-que-hab%C3%ADa-prohibido-exportar/ar-AA1ituNM

Durante diciembre del 2022, el ministerio de desarrollo digital de Rusia anuncio que China no vendería sus procesadores Loongson a ese país sin dejar claro el motivo.

núcleos. El UnixBench del sistema de escritorio LS3A5000 está basado en un sistema operativo doméstico, obtiene más de 1700 puntos por un solo subproceso y 4200 puntos por los cuatro subprocesos.

LS3A5000 integra profundamente autonomía y seguridad. Todos los módulos en LS3A5000, incluido el núcleo de la CPU, el controlador de memoria y la PHY relacionada, el controlador de interfaz IO de alta velocidad y la PHY, PLL y la pila son registros multipuerto, y están diseñados de forma independiente. LS3A5000 implementa un mecanismo especial en el núcleo del procesador para evitar ataques "Spectre" y "Meltdown", y su núcleo de procesador admite mecanismos de control de acceso, como la protección de la pila del kernel del sistema operativo.

La venta de procesadores Loongson a Rusia representa una importante decisión ya que esto antecede la acelerada demanda y adopción de tecnología "propia" y la cada vez menor dependencia de occidente por los países de Asia.

En respuesta a las demandas de desarrollo de la información, Loongson Technology siempre se mantiene al tanto de las tendencias internacionales de TI y se centra en el desarrollo de la industria y la construcción de sistemas basados en la innovación independiente. Hasta ahora, Loongson se ha centrado en el diseño de la arquitectura del conjunto de instrucciones de la CPU (ISA) (LoongArch®), el núcleo IP del procesador y el sistema operativo. Loongson se ha esforzado por crear un ecosistema de software y hardware y un sistema de industria de la información independientes y abiertos para proporcionar procesadores de desarrollo propio, seguros y confiables para satisfacer las necesidades estratégicas nacionales, así como procesadores de alto rendimiento y bajo costo con soluciones básicas de software y hardware para impulsan el desarrollo innovador de la industria de la información.

La venta de procesadores Loongson a Rusia representa una importante decisión ya que esto antecede la acelerada demanda y adopción de tecnología "propia" y la cada vez menor dependencia de occidente por los países de Asia. La Tecnología como punta de lanza y un elemento estratégico en la independencia comercial de los países europeos y de E.U. es una acción digna de seguirse en los próximos años.

FOTO: Windows1089, CC BY-SA 3.0, via Wikimedia Commons

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.

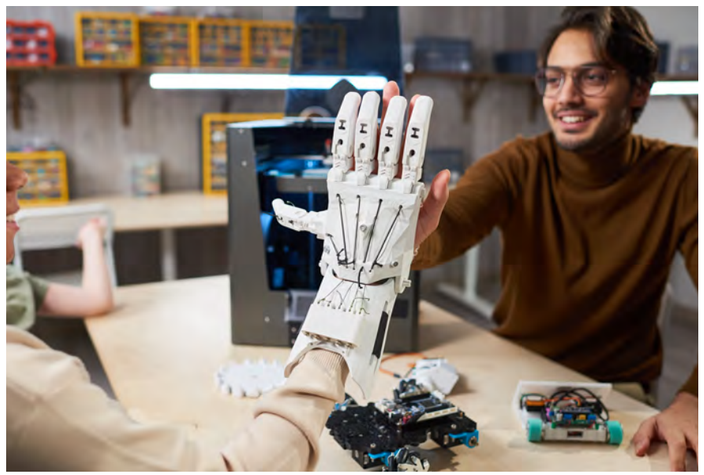
Según la definición de la Comisión Europea define los Tipos de IA de la siguiente manera:

- **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

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.

Por Ed. Dr. Armando Avalos Pérez
armando.avalos@marcg.com.mx

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-inteligencia-artificial-y-como-se-usa



Los sistemas de inteligencia artificial destinados a la atención del público en general, han sido intentos que no han logrado una aceptación.

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

Los sistemas de inteligencia artificial destinados a la atención del público en general, han sido intentos que no han logrado una aceptación.

modelos de inteligencia artificial como el reconocimiento facial en los temas de seguridad pública, ya que representan un área de oportunidad y mejora en al 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 oficial son un hecho que, solventando el costo de implementación, serán adoptados en los siguientes años. El tema de la protección de la identidad es unas inquietudes cada vez más grandes 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 da 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 de 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.

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.

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. Sim 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.

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.

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.

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.

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).

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-ue-primera-normativa-sobre-inteligencia-artificial

Implementación de Controles Generales de TI en una organización

- Introducción a los Controles Generales de TI
- Tipos de CGTI
- Pruebas de CGTI
- Ejemplo de matriz de CGTI
- Recomendaciones finales

Todo entorno corporativo, ya sea de iniciativa privada o del sector público, depende ampliamente de las Tecnologías de la Información como un pilar sumamente importante para su operación del día a día. Pero uno de los retos más importantes a considerar en la rama de las TI, es que estas no deberían operar sin un marco que regule y controle sus procesos tecnológicos que suman al ciclo de negocio de la organización.

Es por eso que las prácticas internacionales recomiendan que sea implementado un marco de Controles Generales de TI (CGTI en español), (ITGC en inglés).

Los CGTI se refieren a las políticas, procedimientos y medidas implementadas en una organización para garantizar la seguridad, integridad y confidencialidad de la información, así como para asegurar el correcto funcionamiento de los sistemas en el entorno organizacional.

Estos controles son importantes porque ayudan a minimizar los riesgos asociados con el uso de la tecnología en los procesos de la organización.

Tipos de CGTI

Dentro de las buenas prácticas recomendadas en los CGTI existen 4 tipos de controles (preventivos, detectivos, correctivos y de aplicación) que toda organización debe de considerar implementar dentro su marco de operación de TI. Son los siguientes.

1. Controles preventivos: Estos controles están diseñados para prevenir o minimizar la aparición de riesgos y problemas de seguridad antes de que ocurran. Su objetivo principal es evitar la ocurrencia de amenazas y vulnerabilidades. Algunos ejemplos de controles preventivos incluyen:

a. *Políticas y procedimientos de seguridad:* Establecimiento de políticas y directrices claras para el uso adecuado de los sistemas y la gestión de la seguridad de la información.

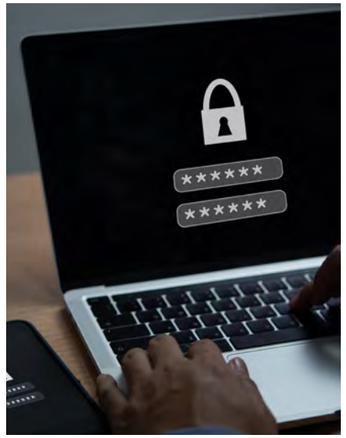
b. *Capacitación y concientización:* Programas de capacitación para educar a los empleados sobre buenas prácticas de seguridad y cómo evitar amenazas potenciales.

c. *Controles de acceso:* Implementación de medidas para controlar y restringir el acceso a sistemas y datos sensibles.

d. *Firewalls y sistemas de detección de intrusos:* Establecimiento de barreras de seguridad para proteger la red contra ataques externos.

Los CGTI se refieren a las políticas, procedimientos y medidas implementadas en una organización para garantizar la seguridad, integridad y confidencialidad de la información.

Por Ing. Joaquin Ortiz Flores
PCATI, PCSI (ciscig.mx), CSX-A (isaca.org)



2. Controles detectivos: Estos controles se enfocan en la identificación y detección de eventos o incidentes de seguridad que ya han ocurrido. Su objetivo principal es detectar amenazas o violaciones de seguridad lo antes posible, para poder responder rápidamente y minimizar los daños. Algunos ejemplos de controles detectivos incluyen:

a. *Monitoreo de seguridad:* Implementación de sistemas y herramientas de monitoreo que registran y analizan actividades sospechosas en la red.

b. *Análisis de registros y registros de auditoría:* Revisión y análisis de registros de actividad para identificar patrones o comportamientos inusuales.

c. *Sistemas de detección de intrusiones:* Utilización de sistemas automatizados que alertan sobre posibles intentos de acceso no autorizado.

d. *Auditorías de seguridad:* Realización de auditorías periódicas para evaluar la eficacia de los controles de seguridad implementados.

3. Controles correctivos: Estos controles se centran en corregir y mitigar los problemas de seguridad identificados. Una vez que se ha detectado una amenaza o una violación de seguridad, los controles correctivos permiten tomar las acciones necesarias para solucionar el problema y restablecer la seguridad. Algunos ejemplos de controles correctivos incluyen:

a. *Parches y actualizaciones de seguridad:* Aplicación de correcciones y actualizaciones para solucionar vulnerabilidades conocidas en los sistemas y aplicaciones.

b. *Eliminación de malware y virus:* Implementación de herramientas y procedimientos para detectar y eliminar software malicioso.

c. *Restauración de sistemas y datos:* Recuperación de sistemas o datos a un estado seguro y confiable después de un incidente de seguridad.

d. *Análisis de causas raíz:* Identificación de las causas subyacentes de un incidente de seguridad para tomar medidas preventivas adicionales y evitar futuros problemas similares.

4. Controles de aplicación: Estos controles se enfocan en garantizar la seguridad y la integridad de las aplicaciones de software utilizadas en la organización. Se centran en la prevención y la detección de vulnerabilidades en el código y en la configuración de las aplicaciones. Algunos ejemplos de controles de aplicación incluyen:

La entidad debe de hacer auditorías de pruebas de control, ya que el resultado de estas pruebas le dará certeza a la organización de las fortalezas y áreas de mejora para su departamento de TI

a. *Pruebas de seguridad de aplicaciones:* Realización de pruebas de seguridad periódicas, como pruebas de penetración, para identificar y corregir posibles vulnerabilidades en el código y en la configuración de las aplicaciones.

b. *Gestión de parches y actualizaciones:* Mantenimiento regular de las aplicaciones para aplicar parches de seguridad y actualizaciones que solucionen las vulnerabilidades conocidas.

c. *Control de cambios en las aplicaciones:* Implementación de un proceso de gestión de cambios para garantizar que las actualizaciones y modificaciones en las aplicaciones se realicen de manera controlada y segura.

d. *Autenticación y control de acceso:* Implementación de mecanismos de autenticación seguros y control

Dentro de las buenas prácticas recomendadas en los CGTI existen 4 tipos de controles: preventivos, detectivos, correctivos y de aplicación.

de acceso adecuado a las aplicaciones para prevenir accesos no autorizados.

Pruebas de CGTI

Cabe resaltar que no todas las organizaciones son iguales en cuanto a su giro de negocio, o tipo de operación, es por eso que la entidad debe de hacer auditorías de pruebas de control, ya que el resultado de estas pruebas le dará certeza a la organización de las fortalezas y áreas de mejora para su departamento de TI. Estas son algunas recomendaciones para realizar pruebas a los CGTI.

1. Planificación: Define los objetivos de las pruebas, establece un alcance claro y selecciona los controles específicos que serán evaluados. También asigna recursos y define un cronograma para llevar a cabo las pruebas.

2. Metodología de prueba: Utiliza una metodología de prueba que se ajuste a tus necesidades y objetivos. Puedes basarte en marcos de referencia reconocidos, como COBIT (Control Objectives for Information and Related Technologies) o NIST SP 800-53 (Framework for Improving Critical Infrastructure Cybersecurity). Estas metodologías te ayudarán a estructurar las pruebas de manera efectiva.

3. Documentación de pruebas: Asegúrate de documentar adecuadamente las pruebas que se realizarán, incluyendo los procedimientos y los pasos a seguir. Esto te permitirá mantener un registro claro de las pruebas realizadas, los resultados obtenidos y las acciones correctivas recomendadas.

4. Selección de muestras representativas: Al elegir qué controles probar, selecciona una muestra representativa que refleje los controles clave y las áreas de riesgo más relevantes para tu organización. Esto te permitirá obtener una visión general de la efectividad de los CGTI sin necesidad de evaluar todos los controles individualmente.

5. Pruebas manuales y automatizadas: Combina las pruebas manuales y automatizadas para obtener resultados más completos. Las pruebas manuales te permiten evaluar aspectos que requieren análisis detallado y comprensión del contexto, mientras que las pruebas automatizadas pueden ayudarte a realizar evaluaciones rápidas y repetitivas.

6. Simulación de escenarios de riesgo: Intenta simular escenarios de riesgo o ataques reales durante las pruebas para evaluar cómo responden los CGTI. Esto puede incluir pruebas de penetración, intentos de acceso no autorizado o simulaciones de desastres.

7. Análisis de los resultados: Una vez que hayas completado las pruebas, analiza los resultados obtenidos. Identifica las debilidades y áreas de mejora en los CGTI y clasifica los hallazgos según su gravedad y prioridad. Estos resultados te ayudarán a desarrollar un plan de acción para abordar las deficiencias identificadas.

8. Seguimiento y acciones correctivas: Es importante realizar un seguimiento de las acciones correctivas recomendadas y garantizar que se implementen de manera oportuna. Establece un mecanismo para monitorear y verificar que las mejoras se lleven a cabo y que los controles se fortalezcan de manera efectiva.

Ejemplo de matriz de CGTI

A continuación, anexo un ejemplo de cómo documentar una matriz de CGTI dentro de una organización que puede ser adaptada según las necesidades de la organización.

Área	Control	Descripción del control	Naturaleza del control	Tipo de control	Pruebas de diseño e implementación	Resultado de pruebas	Fecha de seguimiento
		Se recomienda implementar una suite de antivirus desde los servidores hasta las computadoras de los colaboradores con el propósito de evitar amenazas externas de virus, malware y ramsomware	*(Colocar si es preventivo, detectivo correctivo o de aplicación).* **Control de tipo preventivo**	*(Colocar si es automático, manual o mixto).* **Control automático**	a) Revisión de la correcta configuración del antivirus en servidores y laptops. b) Revisión de actualización de la base de datos del antivirus. c) Revisión de la implementación de escaneos automáticos a nivel servidor y computadora. d) Seguimiento de los informes del sistema de antivirus. e) Revisión de la vigencia de la licencia del antivirus	*(Colocar si el control es efectivo, parcialmente efectivo o inefectivo)* **Efectivo**	*(Colocar una fecha para seguimiento a este control)*

Recomendaciones finales

Cabe destacar que los CGTI, son la carta de navegación de la organización para la mitigación de riesgos de ciberseguridad, y será sumamente importante que la entidad considere la implementación de estos controles. Como último, anexo recomendaciones finales para la implementación de CGTI.

- Toda la organización debe de estar involucrada en el conocimiento de los CGTI, desde la alta dirección hasta las áreas operativas.
- Los CGTI, deben de ser actualizados conforme la organización adquiera nuevas tecnologías o servicios de TI.
- Los CGTI, deben de ser monitoreados constantemente para su evaluación.

Regreso a la Luna

Por Ed. Dr. Armando Avalos Pérez
armando.avalos@marcg.com.mx

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.

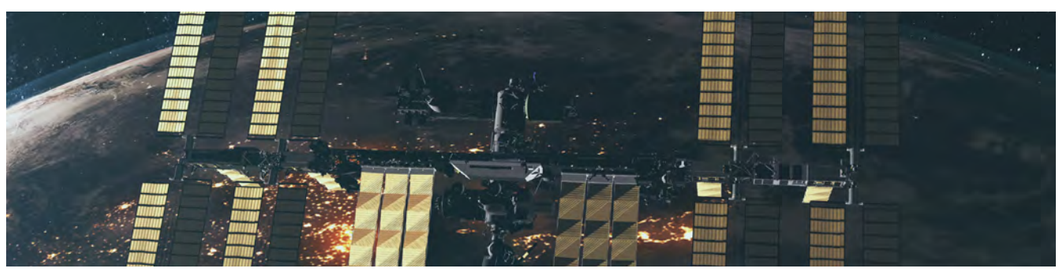
Lo primero que considero es la gran pregunta ¿Por qué?, es inquietante que teniendo enfrente una crisis mundial económica, social, política y un reordenamiento global, los países destinen recursos económicos a una odisea incierta.

Es inquietante que teniendo enfrente 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 explicito, superior al de la exploración terrestre.

Pero el despliegue de satélites en 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[1]. En la Luna hay agua. La Administración Nacional de Aeronáutica y el Espacio (NASA, por sus siglas en inglés) confirmó este lunes que detectaron

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

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 aterrizajeLuna-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.

2 *National Geographic España*. (2023, 7 noviembre). National Geographic. https://www.nationalgeographicla.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-taikonautas-vuelven-de-la-estacion-espacial-china-tras-cinco-meses/

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/c3gzwlq1y33o

La auditoría y el desarrollo de software

- ¿Qué es el ciclo de vida de desarrollo de software?
- Auditando el proceso de desarrollo de software

El desarrollo de software involucra a programadores, diseñadores y otros profesionales de TI que trabajan en equipo para crear soluciones técnicas eficientes y productivas.

Por Ing. Joaquin Ortiz Flores
PCATI, PCSI (ciscig.mx), CSX-A (isaca.org)

El desarrollo de software es el proceso de creación de programas o sistemas usando codificación y diseño. Este proceso consiste en traducir las necesidades de los usuarios en software funcional. Implica varias fases, desde la definición y el desarrollo de los requisitos hasta la codificación, las pruebas y la implementación. El desarrollo de software involucra a programadores, diseñadores y otros profesionales de TI que trabajan en equipo para crear soluciones técnicas eficientes y productivas. El campo está en constante evolución, impulsado por los avances tecnológicos, las demandas del mercado y la necesidad de adaptarse a los cambios y mejoras en curso.

El proceso de vida de desarrollo de software consiste en las siguientes etapas:

1. Requisitos: En esta etapa, se identifican y definen los requisitos del software. Se analizan las necesidades del cliente y se documentan los objetivos, funciones y características que se espera que tenga la aplicación.

2. Diseño: En esta etapa, se crea el diseño de alto nivel y el diseño detallado del software. Se definen la arquitectura, la estructura de datos, la interfaz de usuario y otros componentes necesarios para construir la aplicación.

3. Desarrollo: Aquí es donde se realiza la codificación del software. Los programadores escriben el código fuente utilizando el lenguaje de programación elegido y siguiendo las pautas de diseño establecidas.

4. Pruebas: Después de la fase de desarrollo, se llevan a cabo pruebas para detectar errores y garantizar que el software cumpla con los requisitos definidos. Se realizan pruebas unitarias, de integración y de sistema para validar el funcionamiento correcto de la aplicación.

5. Implementación: Una vez que el software ha pasado las pruebas, se implementa en el entorno de producción. Esto implica instalar el software en los sistemas objetivo y realizar cualquier configuración necesaria.

6. Mantenimiento: Después de la implementación, comienza la fase de mantenimiento. Se realizan correcciones de errores, actualizaciones, mejoras y se brinda soporte técnico a los usuarios.

Cabe mencionar que este es un proceso constante, donde el auditor debe de ser consiente que el proceso de auditoría de software es continuo. Por esta razón, presento algunos puntos importantes a considerar para realizar una auditoría exitosa al proceso de desarrollo de software.

Auditando el proceso de desarrollo de software

I. Auditoría de la etapa de requisitos

Al auditar la etapa de requisitos en el proceso de desarrollo de software, se pueden realizar las siguientes pruebas de auditoría para garantizar la integridad y calidad de los requisitos y necesidades establecidos por las partes interesadas.

1. Revisión de requisitos: Se verifica si los requisitos están claramente definidos, son comprensibles y consistentes, además se analiza la documentación de requisitos para identificar posibles omisiones, ambigüedades o contradicciones.

2. Validación de requisitos: Se verifica si los requisitos establecidos cumplen con las necesidades y expectativas del cliente y/o las partes interesadas. Se deben de comparar los requisitos documentados con los objetivos y funciones esperadas de la aplicación.

3. Evaluación de la documentación: Se revisa la calidad de la documentación de requisitos, se recomienda verificar si la documentación es clara, completa, precisa y comprensible para todas las partes interesadas relevantes.

4. Análisis de riesgos: Se recomienda realizar un análisis de riesgos para identificar posibles eventos adversos asociados con los requisitos. Se evalúa la probabilidad y el impacto de los riesgos para determinar si se han abordado adecuadamente en los requisitos.

Estas pruebas de auditoría ayudan a garantizar que los requisitos establecidos sean sólidos, consistentes y cumplan con las expectativas del cliente, sentando así una base sólida para el desarrollo de software.

El desarrollo de software es el proceso de creación de programas o sistemas usando codificación y diseño.

Cabe mencionar que este es un proceso constante, donde el auditor debe de ser consciente que el proceso de auditoría de software es continuo.

II. Auditoría de la etapa de diseño de software

Algunas pruebas de auditoría que se pueden llevar a cabo son:

1. Revisión de diseño: Se realiza una revisión exhaustiva del diseño de alto nivel y del diseño detallado para verificar si cumplen con los requisitos establecidos, se recomienda evaluar la coherencia del diseño, la adecuación de la arquitectura propuesta, la estructura de datos y la interfaz de usuario.

2. Cumplimiento de estándares y mejores prácticas: Se verifica si el diseño sigue los estándares y las mejores prácticas de la industria. Se debe de analizar si se utilizan patrones de diseño adecuados, se siguen principios de diseño sólidos y se aplican las prácticas recomendadas para garantizar la mantenibilidad y la escalabilidad del software.

3. Verificación de trazabilidad: Se verifica si existe una trazabilidad adecuada entre el diseño y los requisitos establecidos. Se comprueba que cada componente del diseño esté vinculado correctamente con los requisitos correspondientes, asegurando así que el diseño abarque todas las funcionalidades requeridas.

4. Evaluación de la documentación: Se revisa la calidad de la documentación del diseño, verificando si es clara, completa y comprensible para los miembros del equipo de desarrollo y otras partes interesadas relevantes.

Estas pruebas de auditoría ayudan a asegurar que el diseño propuesto sea sólido, cumpla con los requisitos establecidos y esté alineado con los estándares y mejores prácticas de la industria, sentando así las bases adecuadas para la implementación del software.

III. Auditando la etapa de desarrollo de software

Algunas pruebas de auditoría que se pueden llevar a cabo son:

1. Revisión de código: Se realiza una revisión exhaustiva del código fuente para verificar su calidad, legibilidad y estructura. Se recomienda buscar posibles errores de programación además de revisar el uso ineficiente de recursos de infraestructura, código duplicado y otras prácticas indeseables.

2. Cumplimiento de estándares de codificación: Se recomienda verificar si el código sigue los estándares de codificación establecidos. Se debe de analizar si se siguen las mejores prácticas y si se aplican las reglas de estilo de codificación y se utilizan buenas prácticas de programación.

3. Pruebas unitarias: Se debe de verificar la existencia y la calidad de las pruebas unitarias, se debe de evaluar si las pruebas cubren adecuadamente todas las funcionalidades del código y si se proporcionan casos de prueba para los diferentes escenarios posibles.

4. Seguridad: Se recomienda evaluar la seguridad del código y se debe de buscar posibles vulnerabilidades, en el mismo se deben de analizar las prácticas de codificación segura, la protección contra ataques comunes y el manejo adecuado de datos sensibles.

5. Control de versiones: Se verifica si se está utilizado un sistema de control de versiones adecuado y si se siguen los procesos establecidos para gestionar y registrar los cambios en el código fuente.

6. Evaluación de la documentación técnica: Se debe de revisar la calidad de la documentación técnica asociada al código, además de verificar si se proporciona documentación clara y completa que describa el funcionamiento y el uso del código.

IV. Auditando la etapa de pruebas

Algunas pruebas de auditoría que se pueden llevar a cabo son:

1. Implementación de ambientes de pruebas: Se debe de verificar que se implementen ambientes de prueba, antes de que se lancen a operación de la organización, con el fin de evaluar la efectividad del desarrollo y se puedan corregir errores sin interrumpir la operación cotidiana de la organización.

2. Ejecución y registro de pruebas: Se verifica si las pruebas se han ejecutado de manera adecuada y se ha registrado correctamente el resultado de cada evaluación, además se debe de analizar si se han identificado y registrado todos los errores encontrados durante esta etapa.

3. Pruebas de regresión: Se evalúa si se han realizado pruebas de regresión para asegurarse de que los cambios realizados en el software no hayan introducido nuevos errores o afectado la funcionalidad existente.

4. Pruebas de rendimiento: Se verifica si se han realizado pruebas de rendimiento para evaluar el comportamiento del software en términos de tiempos de respuesta, capacidad de carga y eficiencia. Se debe de buscar identificar posibles cuellos de botella y problemas de rendimiento.

5. Integración de sistemas: Se evalúa la efectividad de las pruebas de integración, verificando si los diferentes componentes del software se han integrado correctamente y funcionan de manera conjunta según lo esperado.

Se debe de analizar si se utilizan patrones de diseño adecuados, se siguen principios de diseño sólidos y se aplican las prácticas recomendadas para garantizar la mantenibilidad y la escalabilidad del software.

V. Auditando de la etapa de implementación

En cuanto a la implementación del sistema, se recomienda revisar lo siguiente:

1. Planificación de implementación: Se revisa la planificación de implementación para verificar si se han considerado todos los aspectos relevantes, como los recursos necesarios, el tiempo estimado y los posibles riesgos. Se busca asegurar que se hayan establecido planes de contingencia adecuados para la mitigación de riesgos y fallos.

2. Configuración y ambiente de producción: Se verifica si se han realizado las configuraciones necesarias en el entorno de producción para admitir la implementación del software. Se debe de analizar si el ambiente de producción cumple con los requisitos de hardware, software y red necesarios para el correcto funcionamiento del desarrollo.

3. Instalación y despliegue: Se evalúa la efectividad del proceso de instalación y despliegue del software en los sistemas. Se tiene que verificar si se han seguido los procedimientos establecidos y si se ha realizado una instalación exitosa sin interrupciones o fallos graves.

4. Documentación de implementación: Se revisa si la documentación de la implementación verifica su calidad con el fin de asegurar que se proporcione información clara y detallada sobre los pasos realizados durante la implementación, configuración y puesta en marcha del software.

VI. Auditando el mantenimiento del desarrollo de software

Estas son las pruebas que se pueden llevar a cabo:

1. Gestión de incidencias: Se evalúa la eficacia del proceso de gestión de incidencias para asegurarse de que se estén registrando y gestionando adecuadamente los errores reportados por los usuarios.

2. Actualizaciones y mejoras: Se recomienda revisar el proceso de actualización y mejora del software para verificar si se están implementando adecuadamente las correcciones de errores, las actualizaciones de seguridad y las mejoras funcionales, para asegurar que se siga un proceso controlado para evitar impactos negativos en el sistema en producción.

3. Pruebas de regresión: Se realizan pruebas de regresión para verificar que las correcciones, actualizaciones y mejoras no hayan introducido nuevos errores o hayan afectado negativamente la funcionalidad existente.

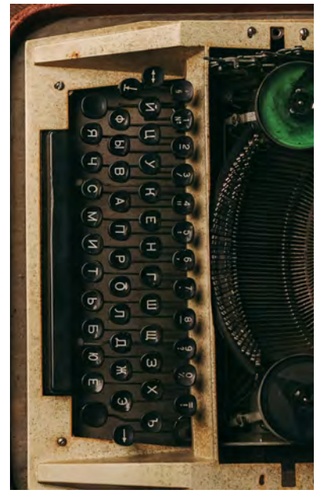
Se debe de revisar la calidad de la documentación técnica asociada al código

4. Control de cambios: Se evalúa el proceso de control de cambios para asegurarse de que los cambios realizados en el software estén debidamente autorizados, registrados y documentados.

5. Gestión de versiones: Se verifica si se está utilizando un sistema de gestión de versiones adecuado y si se siguen las mejores prácticas para gestionar las diferentes versiones del software.

6. Soporte técnico y atención al cliente: Se evalúa la calidad del soporte técnico brindado a los usuarios. Se debe de analizar la capacidad de respuesta, la eficacia en la resolución de problemas y la satisfacción general del cliente con el soporte proporcionado.

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 QUERIAMOS 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.

Es melancólico el recordar aquellas épocas donde conseguir el teléfono del amor platónico era parte del cortejo.

Por Ed. Dr. Armando Avalos Pérez
armando.avalos@marcg.com.mx

Optimización técnica en el posicionamiento SEO como estrategia de marketing

En un mundo cada vez más digitalizado, el marketing se ha convertido en una herramienta fundamental para que las empresas alcancen el éxito.

Por Mtro. Omar Camacho
Consultor en comunicación estratégica en Consultoria Ergo

El posicionamiento SEO (Search Engine Optimization) se ha erigido como una estrategia esencial en este panorama, porque, al entender y aprovechar el SEO de manera efectiva, los negocios pueden mejorar la visibilidad de sus productos y servicios, llegar a un público más amplio y establecer su marca como líder en su campo.

Es desde esta perspectiva, que los ingenieros en sistemas computacionales son grandes aliados en las estrategias de marketing para posicionar los sitios web.

¿Qué es el Posicionamiento SEO?

El SEO es el proceso de optimizar un sitio web para que los motores de búsqueda como Google, Bing y Yahoo lo clasifiquen y lo muestren en los resultados de búsqueda[1] . El objetivo es aparecer en los primeros resultados orgánicos, ya que esto aumenta significativamente la probabilidad de que los usuarios visiten su sitio web. Para los negocios, esto significa que sus proyectos, servicios o productos puedan llegar a un público objetivo más amplio y, en última instancia, generar más ventas o reconocimiento de marca.

Un sitio web bien optimizado para SEO es más visible en los motores de búsqueda.

Beneficios del Posicionamiento SEO

Uno de los principales beneficios de una buena estrategia SEO es que te ofrece mayor visibilidad. Un sitio web bien optimizado para SEO es más visible en los motores de búsqueda. Esto significa que las personas que buscan soluciones o información relacionada con el negocio tienen más probabilidades de encontrar su sitio.

También te permite atraer mayor tráfico orgánico, es decir, el tráfico que llega a su sitio web a través de búsquedas en motores de búsqueda, el cual es altamente relevante y valioso. Estas personas ya están interesadas en lo que el negocio ofrece.

Una parte curcial es la credibilidad y confianza que da el aparecer en los primeros resultados de búsqueda[2]. Los usuarios tienden a confiar en los

1 Mousinho, A. (2022, 14 diciembre). *SEO: la guía completa para que conquistes la cima de Google en el 2022*. Rock Content - ES. https://rockcontent.com/es/blog/que-es-seo/

2 Huertas, C. (2022, 17 febrero). *¿Qué es el posicionamiento SEO y cómo funciona?* PresTeamShop Blog. https://www.presteamshop.com/blog/que-es-seo

El SEO puede reducir la dependencia de la publicidad pagada al generar tráfico orgánico de forma continua.

resultados de búsqueda y consideran a las páginas web bien posicionadas como fuentes confiables.

Para muchos negocios, no descapitalizarse cuando están empezando un proyecto, es fundamental, por lo que una buena estrategia SEO puede ayudar a reducir costos publicitarios. Si bien la publicidad en línea puede ser efectiva, también puede ser costosa. El SEO puede reducir la dependencia de la publicidad pagada al generar tráfico orgánico de forma continua.

Finalmente, la hipersegmentación que permiten los canales digitales ayudan a dirigir de mejor forma las campañas. El SEO permite dirigirse a un público específico utilizando palabras clave relacionadas con la ingeniería. Esto le permite llegar a aquellos que tienen una mayor probabilidad de estar interesados en sus servicios o productos.

La optimización técnica es clave para posicionarse

Para lograr éxito en una estrategia SEO, es necesario:

1. Investigación de Palabras Clave.
2. Optimización de Contenido.
3. Optimización Técnica..
4. Construcción de Enlaces.
5. Seguimiento y Análisis.

Los procesos de investigar palabras clave (o keywords) y a la optimización de contenido, se realizan primordialmente por profesiones afines a la comunicación, mercadotecnia o diseño digital, sin embargo, la optimización técnica requiere conocimientos más especializados.

La optimización técnica en SEO se refiere a la mejora de la estructura y configuración técnica de un sitio web para que sea más amigable para los motores de búsqueda[3] y, en última instancia, se posicione mejor en los resultados de búsqueda. Los elementos más importantes son:

1. Velocidad de Carga del Sitio: La velocidad de carga de un sitio web es un factor crucial en el SEO. Los motores de búsqueda, como Google, prefieren sitios web que se cargan rápidamente. Los usuarios también tienden a abandonar sitios lentos. Para mejorar la velocidad de carga, se recomienda:

- Comprimir imágenes y archivos.
- Utilizar la compresión GZIP.
- Minimizar el uso de scripts y redirigirlos al final del documento HTML.
- Utilizar una red de distribución de contenido (CDN) para servir recursos estáticos desde servidores cercanos al usuario.

2. Optimización Móvil: Con el aumento del uso de dispositivos móviles, Google da prioridad a los sitios web "mobile friendly". Es importante asegurarse de que el sitio sea responsivo y se adapte a pantallas de diferentes tamaños. Google también utiliza la versión móvil de un sitio para indexar y clasificar contenido.

3. Estructura de URL Amigable: Las URL deben ser legibles y descriptivas, con palabras clave relevantes. Se recomienda evitar las URL largas y confusas y utilizar guiones en lugar de caracteres especiales.

4. Jerarquía y Estructura del Contenido: Es importante organizar el contenido de manera jerárquica. Utiliza encabezados HTML (H1, H2, H3, etc.) para indicar la estructura del contenido. Esto facilita la navegación para los motores de búsqueda y los usuarios.

5. Etiquetas Meta: Es fundamental que las páginas tengan etiquetas meta bien escritas. Esto incluye el título y la descripción meta. Utilizar palabras clave relevantes y crear descripciones que atraigan a los usuarios a hacer clic en los resultados de búsqueda puede ser la diferencia.

6. Sitemaps XML: Se recomienda crear un archivo sitemap XML que enumere todas las páginas importantes del sitio. Esto ayuda a los motores de búsqueda a rastrear e indexar el contenido de manera eficiente.

7. Canónico y Etiquetas hreflang: Utilizar etiquetas canónicas ayuda a evitar contenido duplicado y etiquetas hreflang si el sitio está disponible en varios idiomas o regiones.

8. Optimización de Imágenes: Las imágenes deben estar optimizadas para la web. Esto incluye el uso de formatos de imagen adecuados (como JPEG y PNG), la compresión de imágenes y la inclusión de atributos "alt" descriptivos.

9. Estructura de Enlaces Internos: Los enlaces internos ayudan a los motores de búsqueda a comprender la jerarquía de contenido en tu sitio por lo que siempre es útil crear una estructura de enlaces internos lógica y bien organizada.

10. Seguridad y Certificado SSL: Google otorga prioridad a sitios seguros y penaliza los sitios sin SSL, por lo que contar con un certificado SSL debe de ser parte de la estrategia SEO.

11. Eliminación de Errores Técnicos: Periódicamente hay que realizar auditorías técnicas regulares para identificar y corregir errores, como páginas 404, redirecciones rotas y problemas de indexación.

12. Rastreo y Exploración del Sitio: Herramientas como Google Search Console ayudan monitorear cómo Google rastrea e indexa tu sitio. Identifica problemas y toma medidas para solucionarlos.

La optimización técnica en SEO es un proceso continuo que exige mantener el sitio actualizado con las mejores prácticas de SEO técnico y realizar auditorías periódicas para asegurarse de que esté funcionando de manera óptima. Una sólida optimización técnica puede marcar la diferencia en el posicionamiento de un sitio web en los motores de búsqueda y, en última instancia, en el éxito de la estrategia de SEO. ■

3 Castro, R. M. (2023, 23 marzo). ¿Qué es el SEO técnico? conceptos básicos y 10 buenas prácticas. Semrush Blog. https://es.semrush.com/blog/seo-tecnico/

Periódicamente hay que realizar auditorías técnicas regulares para identificar y corregir errores, como páginas 404, redirecciones rotas y problremas de indexación.

Gestión del Riesgo Operativo: La clave para el éxito de pequeñas empresas

Imagina que eres un joven adulto que se encuentra en su primer empleo, lo que te ha permitido ahorrar lo suficiente para comprar tu primer automóvil. Has estado meses guardando dinero con el objetivo de lograr esta meta. Un día, visitas una agencia y encuentras el automóvil de tus sueños: cumple con todas tus necesidades, tiene el color que te gusta y está equipado exactamente como lo necesitas.

En México existen aproximadamente 4.9 millones de PYMES en el país. Estas cifras representan el 72% de las oportunidades de empleo y contribuyen con el 52% del Producto Interno Bruto (PIB) en términos estadísticos.

Dispones del dinero necesario para dar un pago inicial que te permite acceder a una mensualidad que puedes manejar sin afectar tu capacidad de gasto mensual. Todo parece encajar perfectamente para que tu primer coche sea un modelo del año.

Al momento de contratar, te presentan varias opciones de seguro para el automóvil, y decides optar por el seguro más económico del mercado para no aumentar demasiado tus mensualidades. Lo haces con la convicción de que no sufrirás ningún accidente, ya que te consideras un conductor responsable, a pesar de no haber tenido antes un automóvil propio.

Los meses pasan, te sientes cómodo y seguro conduciendo tu vehículo, pero un día desafortunado, sufres un incidente en una carretera principal de tu ciudad. Por suerte, no sufres lesiones, pero el automóvil es declarado como pérdida total. Debido a que no tenías un seguro de cobertura amplia, te encuentras en la amarga situación de perder todo lo que has ahorrado durante meses y el esfuerzo que has invertido para tener tu propio automóvil.

Por Lic. Luis Alejandro Heredia Cobos
Especialista en riesgo operativo
alejandro.hec11@gmail.com
https://www.linkedin.com/in/alejandroheredia96

El último censo nacional, realizado en 2019 por el INEGI, revela que la esperanza de vida promedio de las PYMES mexicanas es de 7.8 años.

Este es un ejemplo que destaca la importancia de conocer y mitigar los riesgos en la vida cotidiana. Según los datos proporcionados por el INEGI (Instituto Nacional de Estadística y Geografía), en México existen aproximadamente 4.9 millones de PYMES en el país. Estas cifras representan el 72% de las oportunidades de empleo y contribuyen con el 52% del Producto Interno Bruto (PIB) en términos estadísticos.

El último censo nacional, realizado en 2019 por el INEGI, revela que la esperanza de vida promedio de las PYMES mexicanas es de 7.8 años. Sin embargo, es importante destacar que este número puede variar según el sector productivo al que pertenezcan.

Las dificultades y fracasos que enfrentan las pequeñas y medianas empresas en México suelen derivarse de causas comunes, que incluyen:

- Falta de planificación estratégica
- Escasez de capital y financiamiento
- Problemas en la gestión financiera
- Baja calidad de productos o servicios
- Obstáculos relacionados con regulaciones y trámites burocráticos
- Problemas de gestión de recursos humanos
- Impacto de ciclos económicos y crisis
- Falta de innovación
- Retos en marketing y ventas
- Problemas legales y fiscales
- Ciberseguridad

El éxito de una PYME suele depender de una combinación de factores, a menudo pasando por alto por emprendedores que son expertos en su producto o servicio, pero no necesariamente en aspectos administrativos y estratégicos.

Es posible mitigar todos estos factores mencionados mediante la implementación temprana de una metodología para la identificación y gestión de los riesgos operativos. A continuación, se presenta una tabla que relaciona estos factores que afectan la operación diaria de las PYMES mexicanas con posibles riesgos operativos identificados, su impacto y las buenas prácticas recomendadas para su mitigación.

Causas comunes de dificultados o fracasos de las Pymes	Riesgo operativo Ligado	Impacto	Buenas prácticas para mitigar el riesgo
Falta de capital y financiamiento	Liquidez	Baja o nula capacidad para cumplir con sus obligaciones financieras a corto plazo	Adoptar una gestión financiera efectiva que incluya la planificación de flujo de efectivo, diversificación de fuentes de financiamiento, mantenimiento de reservas de efectivo y una supervisión constante de situación financiera.
Problemas de Gestión financiera	Mercado	Impacto negativo en el valor de los activos y rentabilidad de la Entidad derivado de las variaciones en los mercados financieros, las fluctuaciones en los precios de insumos y las tasas de interés, así como tipos de cambio	Implementar estrategias de gestión de riesgos, como el uso de instrumentos financieros derivados como futuros u opciones, diversificación de inversiones, planificación financiera sólida y monitoreo constante de los mercados relevantes
Ciclos económicos y crisis	Liquidez	Baja o nula capacidad para cumplir con sus obligaciones financieras a corto plazo	Adoptar una gestión financiera efectiva que incluya la planificación de flujo de efectivo, diversificación de fuentes de financiamiento, mantenimiento de reservas de efectivo y una supervisión constante de situación financiera.
Falta de planificación estratégica **Baja calidad de productos o servicios** **Falta de innovación**	Procesos y operaciones	Posibilidad de pérdidas financieras o interrupciones en las operaciones debido a deficiencias, errores, fallas en los procesos internos, eventos imprevistos o problemas relacionados con el personal	Poner en práctica una gestión de riesgos solida que incluya la identificación proactiva de riesgos, la mejora continua de los procesos, la capacitación y supervisión del personal, la planificación de continuidad de negocios, identificación de actividades de control e inversión en tecnología y sistemas
Problemas de recursos humanos	Recursos humanos	Problemas relacionados con la gestión del personal de la Entidad lo cual deriva en una insatisfacción de la fuerza laboral y una alta rotación de personal	Promover una comunicación efectiva, establecer políticas de recursos humanos sólidas, invertir en el desarrollo de empleados y retención de talento y cumplir con regulaciones laborales a fin de mantener y fomentar la moral y la productividad de los colaboradores
Problemas de MKT y ventas	Reputacional	Deterioro de la percepción pública de la empresa por acciones o eventos negativos que pueden tener consecuencias adversas en la confianza de los clientes, proveedores, empleados y otros grupos de interés	Monitoreo de la percepción pública, respuesta rápida a problemas y crisis, adhesión a buenas prácticas comerciales y la comunicación abierta y transparente con los grupos de interés
Ciberseguridad	Tecnológico	Posibilidad de que los problemas relacionados con la tecnología, como fallos en sistemas informáticos, ciberataques, obsolescencia tecnológica o falta de adopción de tecnología, tengan un impacto negativo en la operación y éxito de la empresa	Invertir en medidas de seguridad cibernética acorde a su operación, mantener los sistemas actualizados, capacitar a los empleados en prácticas seguras de tecnología, desarrollar un plan de continuidad de negocios y estar al tanto de regulaciones aplicables
Regulaciones y trámites burocráticos **Problemas legales y fiscales**	Regulatorio y legal	Probabilidad de enfrentar problemas legales o incumplimientos de regulaciones gubernamentales que pueden resultar en sanciones financieras, litigios, perdida de reputación y otros desafíos	Mantenerse informado sobre las regulaciones aplicables a la operación de la empresa, implementar políticas y prácticas de cumplimiento normativo, buscar asesoramiento legal, un plan de respuesta a crisis legales o regulatorias

Las dificultades y fracasos que enfrentan las PYME suelen derivarse de causas comunes.

La cultura de gestión de riesgo operativo en las PYMES mexicanas representa uno de los desafíos más significativos para este sector empresarial. Durante la pandemia de COVID-19, en México se registró el cierre de aproximadamente 1.6 millones de negocios entre octubre de 2020 y julio de 2021. Esto se debió a los cambios en el mercado y la incapacidad de estas empresas para adaptarse y afrontar la situación que experimentamos en ese período.

¿Qué medidas deben tomar ahora para estar preparadas ante este tipo de crisis? La mayoría de las empresas que quiebran lo hacen debido a una gestión deficiente o nula de los riesgos operativos. Esto se debe a que no cuentan con un panorama completo de los posibles escenarios o eventos que pueden afectar su operación, y, como consecuencia, desconocen su impacto y la forma adecuada de enfrentar y controlar este tipo de eventos.

Si una empresa que está en sus primeros pasos otorga la debida importancia a la cultura de mitigación de riesgos, evitará muchas "sorpresas" que podrían llevar al fracaso o a malas prácticas dentro de su negocio. Esto asegurará la continuidad operativa de la empresa y la mantendrá en un camino sólido hacia el éxito.

Importancia de lograr un Título profesional

Sabemos que conforme avanza el tiempo la necesidad de estar mejor preparados y capacitados en el ámbito laboral es un factor fundamental para el crecimiento dentro de las instituciones y para el momento de buscar un nuevo empleo representa no solo un requisito para el mismo, si no que nos da herramientas que nos hacen destacar sobre los demás candidatos al mismo puesto que nosotros.

La titulación en una carreara profesional nos da la oportunidad de obtener un empleo mejor remunerado, que a su vez nos ofrece una cesación de "estabilidad", sin dejar de lado que la preparación contante debe ser una cultura que todos debemos adoptar, ya sea con cursos, talleres, seminarios, conferencias, certificaciones, etc.

Es importante mencionar que mientras un profesionista esté en constante aprendizaje y preparación, su valor como empleado irá incrementando de manera importante para la empresa o institución a la que pertenezca y que las demás compañías también podrán notar y ofrecer ofertas laborales más atractivas y mejor remuneradas, con la intención de tener personal mejor preparado que aumente su valor como empresa y que los ayude con el cumplimiento de objetivos y la resolución de conflictos.

Las certificaciones representan un roll muy importante en el ámbito laboral, ya que no solo nos dan valor curricular, sino que también nos presentan como un experto en la materia y con conocimientos adicionales a nuestro ámbito laboral que nos hará destacar del resto de los profesionistas que solo se titularon pero no continúan con una preparación profesional.

El Colegio Nacional de Integración Profesional (CONAIP) es una instancia evaluadora con más de 22 años de experiencia evaluando conocimientos y ayudando a las personas a obtener su certificado de bachillerato y 2 años como Autoridad Evaluadora reconocida para acreditar profesionistas en Administración y Pedagogía.

Gracias a lo anterior, aproximadamente hace dos meses nos autorizaron acreditar conocimientos en ingeniaría industrial y computacional con el respaldo del Colegio Nacional De Ingenieros Industriales y el Colegio Nacional De Ingenieros Computacionales. Lo que vuelve al CONAIP la mejor opción para obtener un título profesional o una ingeniaría con la certeza de que somos una autoridad educativa en el ámbito profesional.

Mientras un profesionista esté en constante aprendizaje y preparación, su valor como empleado irá incrementando.

Por CONAIP

Colegio Nacional de Integración Profesional (CONAIP): Un puente hacia la acreditación profesional

En un mundo en constante evolución, la educación y el reconocimiento profesional se han convertido en dos pilares fundamentales para el desarrollo y avance de la sociedad. En este contexto, el Colegio Nacional de Integración Profesional (CONAIP) ha emergido como una institución clave para miles de trabajadores en México, gracias al apoyo y visión de la actual administración de nuestro Gobierno Federal a través de la Secretaría de Educación Pública. La determinación del Gobierno ha impulsado diversas ofertas educativas con el objetivo de profesionalizar a nuestra base trabajadora, motor central de nuestro gran país.

Fundado en el año 2000, el CONAIP ha destinado sus esfuerzos a ofrecer una plataforma sólida para que profesionales de diversas áreas reafirmen y enriquezcan sus conocimientos basándose en su experiencia laboral. La meta principal ha sido proporcionar las herramientas necesarias para que, a través del Acuerdo 286 SEP, estos trabajadores puedan ser reconocidos como licenciados e ingenieros profesionales.

Esto no sólo valida la experiencia y conocimientos adquiridos en el campo laboral, sino que también abre puertas a nuevas oportunidades y un mayor reconocimiento profesional.

Sin embargo, el 2021 marcó un hito en la trayectoria del CONAIP. Transformándose en una instancia evaluadora, la institución expandió su alcance, ofreciendo la posibilidad a profesionistas de toda la República mexicana de obtener un título profesional. Esto ha representado un cambio revolucionario, acercando la educación y el reconocimiento formal a aquellos que, por diversas razones, no habían tenido la oportunidad de acceder a ellos.

Entre los niveles educativos que el CONAIP tiene la capacidad de evaluar se encuentran el Bachillerato General, Ingeniería en Computación, Ingeniería Industrial, Licenciatura en Administración y Licenciatura en Pedagogía. Esta variedad refleja la diversidad de campos en los que los profesionales mexicanos se desempeñan y la importancia de ofrecer acreditaciones válidas en distintas áreas.

Es fundamental subrayar que, para acceder a este proceso de evaluación y acreditación, el interesado debe poseer experiencia profesional comprobable dentro del área a evaluar. Este requisito garantiza la calidad y legitimidad del título otorgado, asegurando que los profesionistas acreditados por el CONAIP cuenten con el conocimiento y habilidades necesarios para ejercer su profesión.

En conclusión, el Colegio Nacional de Integración Profesional no sólo valida la experiencia de miles de profesionistas en México, sino que también brinda una oportunidad invaluable de crecimiento y reconocimiento. En tiempos donde la educación y la experiencia laboral son más valiosas que nunca, el CONAIP, respaldado por las iniciativas del Gobierno Federal, se erige como un aliado esencial para el desarrollo profesional del país.

La mejora del servicio público como objetivo del régimen disciplinario en México

Estimados lectores, reciban la más cordial bienvenida a la columna "ÉTICA, RESPONSABILIDAD Y MEJORA EN EL SERVICIO PÚBLICO", en la cual -a partir de esta primera publicación- tendremos la oportunidad de conocer, analizar y proponer acciones orientadas a fomentar la ética, el compromiso, la eficiencia y la responsabilidad tanto de las instituciones públicas del gobierno mexicano (Estado y entidades federativas) como del cuerpo de servidores públicos que lo integran.

Aspectos torales, tales como la integridad pública; la prevención de irregularidades penales y administrativas; la fiscalización de los recursos públicos; la gobernanza; el control interno; la transparencia y el acceso a la información; el combate a la corrupción y la rendición de cuentas formarán parte -enunciativa más no limitativamente- de los principales temas acerca de los cuales esta columna, brindará un espacio y oportunidad para su reflexión.

En este sentido, el propósito de esta columna consiste en ampliar los alcances de la comunicación y la difusión de las ideas relacionadas con los temas que estudiaremos, de tal manera que los artículos aquí publicados permitirán:

a) Identificar aquellos aspectos centrales o problemáticos vinculados con las temáticas de nuestro interés, en los que -desde la experiencia del autor de estas líneas- podremos contribuir individualmente a través de la reflexión, el estudio, el análisis y la formulación de propuestas puntuales y precisas.

b) Reseñar trabajos, estudios, reformas normativas, mejores prácticas, libros y textos que permitirán contribuir a sentar las bases teórico-prácticas para la mejora del servicio público en México.

c) Entrevistar a actores fundamentales en nuestras materias de estudio, los cuales, al contar con una sólida formación académica y profesional, con motivo del ejercicio de la función pública, a través de sus ideas y opiniones, podrán aportar y sumar a la discusión informada de los temas más relevantes para el Estado Mexicano y nuestra sociedad.

Así, estimado lector, te reiteramos la más cordial bienvenida a esta tu columna, al tiempo de agradecer tu interés e invitarte a participar con tu opinión de los artículos que aquí se publicarán, a través de la cuenta de correo electrónico zelda600@hotmail.com en la que podrás ser escuchado, proponer temáticas sobre las que desees que abundemos y también formular áreas de oportunidad para que podamos mejorar este espacio abierto a la reflexión.

Por Dr. Miguel Angel Gutiérrez Salazar

Sentado lo anterior, en esta primera publicación, la temática que nos convoca guarda relación con un tema fundamental para el servicio público mexicano y tiene que ver precisamente con los fines del régimen disciplinario de los servidores públicos y su eficacia.

Cuando hablamos de régimen disciplinario tradicionalmente lo asociamos con el castigo y la sanción que puede imponerse a los integrantes del servicio público federal, estatal o municipal, por realizar inadecuadamente su labor (errores o descuidos en el ejercicio de sus funciones) o, incluso, por vulnerar el marco legal que rige su actuación a través de actos de corrupción que afectan el patrimonio público y -desde luego- a todos los mexicanos.

En ese sentido, a esa postura o enfoque desde el cual se concibe al régimen disciplinario lo podríamos denominar de carácter punitivo o sancionador y tiene como principal objetivo la reacción contundente orientada a castigar a los servidores públicos que se alejaron de la legalidad por descuido o dolosamente la vulneraron.

Ejemplo de esta postura puede advertirse claramente en los informes o reportes anuales, semestrales e, incluso, de menor periodicidad que son publicados por la Secretaría de la Función Pública a nivel federal y por las dependencias que ejercen funciones semejantes en las entidades federativas de nuestro país.

Tan solo en el primer semestre de 2023, según un comunicado de la Secretaría de la Función Pública, **se impusieron más de 900 sanciones a personas servidoras públicas, desglosado de la manera siguiente**[1]:

- 379 inhabilitaciones.
- 331 suspensiones.
- 192 amonestaciones públicas y privadas.
- 40 destituciones.
- 9 sanciones económicas por un monto de 690 mil pesos.

El origen de esas sanciones provino de 607 quejas y denuncias ciudadanas, 342 procedimientos sancionadores iniciados por el incumplimiento a la presentación oportuna de las declaraciones de situación patrimonial y 2 derivadas de auditorías.

En tanto que las causas que motivaron dichos procedimientos y sanciones tuvieron que ver con 402 negligencias administrativas, 334 incumplimientos en la presentación de las declaraciones patrimoniales, 30 violaciones a procedimientos de contratación y 178 por causas diversas.

En ese sentido, puede apreciarse un volumen importante de sanciones aplicadas a los servidores públicos de la Administración Federal, aunque la mayoría por aspectos que se podrían considerar de carácter menor, como son las negligencias o descuidos administrativos y omisiones o extemporaneidades en la presentación de declaraciones patrimoniales, aspectos que si bien son importantes, no constituyen faltas de carácter administrativo grave ni elementos que de manera efectiva contribuyan al combate a la corrupción o a la mejora del servicio público.

Sobre el combate a la corrupción o la sanción de faltas administrativas graves, el mismo reporte señala que en el referido primer semestre de este año, se remitieron 204 expedientes por faltas graves al Tribunal Federal de Justicia Administrativa (TFJA), para que, si así lo determina, continúe con la substanciación y resolución de los procedimientos disciplinarios correspondientes.

Es decir, menos de la tercera parte de las faltas administrativas que se detectan constituyen faltas administrativas graves y, si bien es cierto que esto podría deberse a su falta de ocurrencia, lo cierto es que también puede deberse a mecanismos no idóneos para la denuncia de las mismas o a mecanismos de identificación que hagan posible su investigación y castigo.

Tomemos en cuenta que del total de las más de 900 sanciones en materia de responsabilidad administrativa, solo 2 derivaron de faltas administrativas -no graves- identificadas con motivo de auditorías, por lo que valdría la pena valorar la eficacia de dicho procedimiento como medio para la identificación de faltas administrativas.

No obstante, lo que deseamos enfatizar es que, más allá de esta perspectiva de carácter punitivo del régimen disciplinario del servicio público mexicano, es necesario entenderlo por parte de las autoridades del gobierno mexicano desde otras perspectivas más amplias, concretamente desde el enfoque preventivo y correctivo.

Dichos enfoques, aunque fáciles de mencionar, no resultan tan sencillos de poner en marcha y medir su cumplimiento, puesto que no es a través de una medición cuantitativa sino cualitativa que puede percibirse su efecto positivo en el servicio público mexicano.

La prevención guarda relación con el cuidado y protección del entorno de integridad y el cumplimiento de las reglas que establecen las funciones de los servidores públicos, en tanto que la corrección de las irregularidades tiende a resarcir los efectos nocivos de las faltas administrativas y procurar que las mismas no vuelvan a acontecer.

En ese contexto, desde el punto de vista del autor de estas líneas, el régimen disciplinario mexicano ha abandonado en buena medida dichos enfoques que son complementarios al punitivo y ello se debe en gran medida en que resulta más fácil castigar hechos ya ocurridos que prevenir posibles irregularidades que no se conoce el momento exacto en que puedan suceder.

Sin embargo, para ello existen modelos de control interno que sirven de base para procurar la integridad, correcto funcionamiento y la mejora permanente de las instituciones públicas. Si estos modelos se observaran correctamente y se contara con perfiles adecuados que vigilaran su operación, sería más sencillo evitar la ocurrencia de faltas administrativas que -por más que se sancionen todos los años y así se reporten frecuentemente- lo importante es lograr que ya no ocurran.

La experiencia nos marca como ejemplos de este tipo de faltas administrativas las omisiones y extemporaneidades en la presentación de declaraciones patrimoniales, así como el incumplimiento o retraso de trámites administrativos menores, los cuales, a través de una gestión adecuada del riesgo (factor propio de un modelo de control) permitirían disminuir dichas conductas y procurar su inexistencia. Esta disminución puede lograrse por medio de campañas de mayor difusión, procesos amplios de capacitación y concientización, así como con la identificación de áreas, servidores públicos incumplidos y factores que inhiben el cumplimiento de dichas obligaciones.

Pero además de lo asentado, creemos que las **instituciones públicas deben aprender de sí mismas y de los riesgos y errores que conducen a la materialización de faltas administrativas**. Tal es el caso -por poner un ejemplo más- de incumplimientos en la autorización de documentos y trámites (verbigracia el uso de viáticos o la autorización en el empleo de parque vehicular), que se generan a partir de lagunas o vacíos normativos que las propias instituciones podrían subsanar y, de esa manera, disminuir el riesgo de una falta administrativa, así como la ralentización o perjuicio en su operación, con la sola expedición de reglas claras y completas que prevengan y eviten las mismas (el ambiente de control o normativo es también un factor que compone los sistemas de control interno).

Por ello, regresando a nuestro punto de partida, estimamos indispensable que el derecho disciplinario mexicano no se vea eminentemente como un régimen sancionatorio, sino también como un mecanismo de carácter preventivo y correctivo, orientado a garantizar la prestación de un servicio público óptimo, sustentado en un ambiente de integridad y eficacia, que procure la mejora continua en favor de la ciudadanía.

Ese es -para nosotros- el fin de un régimen de disciplina interna y su eficacia -desde luego- no atañe solo a quienes ocupan altos cargos en la función pública, sino a toda la estructura y a todos los servidores públicos que integran las organizaciones públicas de nuestro país.

Y como todo derecho que corresponde a la ciudadanía, asegurar la prestación de un servicio público de calidad también está en sus manos, demandándolo mediante los canales de denuncia y comunicación que hoy en día existen (incluso los de carácter académico como la presente columna) y que es pertinente mantener permanentemente abiertos, en favor de procurar la rendición de cuentas de nuestro gobierno para todos los mexicanos.

1 De La Función Pública, S. (s. f.). *En el primer semestre de 2023, la SFP impone más de 900 sanciones a personas servidoras públicas*. gob.mx. https://www.gob.mx/sfp/prensa/en-el-primer-semestre-de-2023-la-sfp-impone-mas-de-900-sanciones-a-personas-servidoras-publicas

Cuando hablamos de régimen disciplinario tradicionalmente lo asociamos con el castigo y la sanción.

La prevención guarda relación con el cuidado y protección del entorno de integridad.

¿Es necesaria la actualización de la Normativa de Control Interno en la administración pública federal?

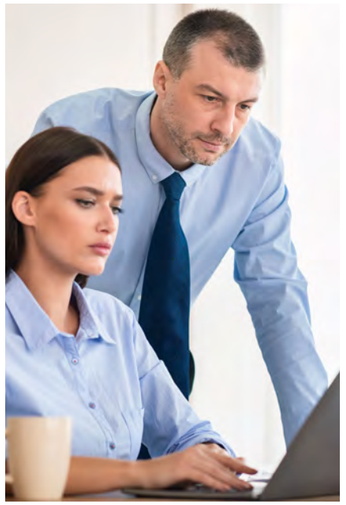
Por Jorge García Alonso

En 2013, el Committe os Sponsoring Organizations of the Treadway Commission (en adelante COSO), emite el documento denominado Control Interno - Marco Integrado (en adelante COSO 2013) el cual provee un enfoque integral y herramientas para la implementación de un sistema de control interno efectivo y en pro de la mejora continua.

De manera general, COSO 2013, se compuso por cinco componentes (Entorno de control, Evaluación de riesgos, Actividades de control, Sistemas de información y Supervisión del sistema de control – Monitoreo) y diecisiete principios o puntos de interés.

Consideramos que la parte principal para que el Control Interno se interiorice, fortalezca y forme parte en la administración pública, se basa en tres temas fundamentales.

Con base este documento, en 2014 el grupo integrante del Sistema Nacional de Fiscalización, emitió el documento denominado "Marco Integrado de Control Interno para el Sector Público" (en adelante MICI), el cual tuvo la finalidad de ser "un modelo general de control interno, para ser adoptado y adaptado por las instituciones en los ámbitos Federal, Estatal y Municipal, mediante la expedición de los decretos correspondientes".



De igual forma, la Secretaría de la Función Pública (en adelante SFP), publicó el cinco de septiembre de 2018, la actualización del "ACUERDO por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno" (en adelante Acuerdo de Control Interno), que tiene por objeto "implementar y mejorar las disposiciones jurídicas reguladoras en materia de control interno para la Administración Pública Federal (APF)", la publicada en el Diario Oficial de la Federación.

Ambos documentos, el Acuerdo de Control Interno y el MICI, definen que están basados en COSO 2013.

En Junio de 2017, COSO emite un nuevo documento denominado Gestión de Riesgo Empresarial – Integrando Estrategia y Desempeño (en adelante COSO 2017), el cual, de acuerdo con los antecedentes del proyecto, es una actualización del Marco Integrado de Gestión de Riesgos Empresarial (en adelante COSO ERM 2004) y sirve, entre otras cosas, para proporcionar una mayor comprensión de la estrategia y del papel que desempeña la gestión del riesgo empresarial en el establecimiento y la ejecución de la estrategia, la mejora en la alineación entre el desempeño organizacional y la gestión del riesgo empresarial y satisface las expectativas en materia de gobierno y supervisión.

En el mismo documento, COSO aclara que no se trata de un "nuevo marco de control" que deje fuera el COSO 2013, sino mas bien, es un complemento para fortalecer la gestión de riesgos, mayormente, para empresas donde los riesgos externos (financieros, políticos, etc.) deban ser administrados de una manera más puntual y en el que se fortalece, entre otras cosas, la idea de tener una "cultura del riesgo" institucional.

Lo anterior, se sustenta en los siguientes párrafos sustraídos de dos documentos oficiales emitidos por COSO:

1. De documento denominado Gestión de Riesgo Empresarial – Integrando Estrategia y Desempeño de Apéndices, en su página 5, en la sección "Relación entre gestión de riesgo empresarial y control interno", especifica lo siguiente:

"El nuevo marco aclara ahora la relación entre la gestión del riesgo empresarial y el control interno e identifica aquellos casos en los que se basa en conceptos establecidos en el Control Interno – Marco Integrado (COSO 2013). Dado que Control Interno – Marco Integrado se utiliza como norma reglamentaria, y para evitar que se amplie sin querer el alcance de ese marco para su aplicación reglamentaria, el Consejo de COSO decidió seguir disponiendo de dos marcos separados y distintos. Por tanto, el Consejo de COSO no ha incluido en esta actualización componentes comunes a ambos marcos (por ejemplo, actividades de control) para evitar redundancias y animar a los usuarios a que se familiaricen con ambos. Sin embargo, algunos conceptos introducidos en Control Interno – Marco Integrado (COSO 2013), como el Gobierno de la gestión del riesgo empresarial se desarrollan mas adelante en el presente Marco…"

2. En el documento denominado Enterprise Risk Management Aligning Risk with Strategy and Performance - Frequently Asked Questions, se menciona lo siguiente respecto de la relación entre los Marcos 2013 y 2017:

"¿Cómo se relaciona el Marco actualizado con el Marco integrado de control interno de COSO de 2013?

El control interno se posiciona dentro del Documento Actualizado como un aspecto fundamental de la gestión del riesgo empresarial. Por lo tanto, el Marco Integrado de Control Interno de 2013 constituye un componente esencial para la gestión de riesgos empresariales. Los dos documentos COSO se complementan entre sí, sin que ninguno reemplace al otro. El documento actualizado se centrará en las áreas necesarias que van más allá del control interno; sin embargo, el Marco Integrado de Control Interno sigue siendo un marco viable y adecuado para diseñar, implementar, realizar y evaluar la eficacia del control interno y para la presentación de informes, como se requiere en algunas jurisdicciones". (traducción libre)

Es necesario que el personal de los OIC´s se capacite de manera constante, en temas de control interno, administración de riesgos, temas éticos, legales y de corrupción.

Propuesta

En virtud de lo anterior, y derivado de que no son documentos que se contrapongan sino por el contrario, se complementan, es recomendable que, en caso de una posible actualización al ACUERDO por el que se emiten las Disposiciones y el Manual Administrativo de Aplicación General en Materia de Control Interno, se considere la actualización del componente de Administración de Riesgos y del componente Ambiente de Control, y que, como como parte de su actualización, se verifiquen aquellas áreas de oportunidad que la SFP haya detectado o le hayan informado y que en su conjunto, coadyuven a un fortalecimiento integral de los Sistemas de Control Interno de las instituciones gubernamentales en México.

Sin embargo, consideramos que la parte principal para que el Control Interno se interiorice, fortalezca y forme parte en la administración pública, se basa en tres temas fundamentales:

• **Fortalecer la capacitación en temas de Control Interno al interior de las instituciones públicas**. – Es necesario e indispensable que, desde los puestos directivos hasta los operativos, se capacite de forma constante

Es necesario que el OIC cuente con una estructura que le permita realizar todas las funciones que tiene a su cargo, tanto por parte del Reglamento Interno de la SFP, así como de la normativa interna de la Institución donde realiza sus funciones.

El nuevo marco aclara ahora la relación entre la gestión del riesgo empresarial y el control interno.

a las personas servidoras públicas, realizando talleres o cursos especializados que no sólo sean teóricos, sino en el que los servidores públicos puedan tener idea de como implementar el control interno en sus áreas sin que sea un "re - trabajo" o un trabajo adicional a sus actividades diarias.

En este sentido, no puede pasar desapercibido que la Administración Pública cuenta con una gran cantidad de instrumentos normativos que guían su actuar, instrumentos que, por sí mismos, incluyen controles en sus actividades, los cuales, de llevarse a cabo por las personas servidoras públicas ejecutoras, de las actividades, estarían contribuyendo a la implementación y fortalecimiento del Sistema de Control Interno Institucional.

• **Fortalecer a los Órganos Internos de Control (OIC´s).** – Derivado de la importancia que conllevan las funciones relacionadas con la verificación del control interno que realizan los OIC´s en las instituciones gubernamentales, es necesario que el OIC cuente con una estructura que le permita realizar todas las funciones que tiene a su cargo, tanto por parte del Reglamento Interno de la SFP, así como de la normativa interna de la Institución donde realiza sus funciones.

En ese sentido, es necesario que el personal de los OIC´s se capacite de manera constante, en temas de control interno, administración de riesgos, temas éticos, legales y de corrupción, con la finalidad de que sus revisiones de control, generen valor a las Instituciones en el fortalecimiento del control interno, la mitigación de sus riesgos y el fomento a evitar los actos de corrupción al interior de la institución.

• **Fortalecer el uso de las tecnologías de la información (TI).** – Si bien es por todos conocido el gran apoyo que brindan las tecnologías de la información en la fiscalización, también es necesario el saber que a estas fechas, aún hay muchos procesos – procedimientos y actividades, que las áreas realizan de forma completamente manual, situación que hace que dicha función, esté proclive al error humano, ya sea de forma inconsciente o en la búsqueda de un beneficio personal.

En este sentido, el que las instituciones cuenten con una herramienta tecnológica o sistema de administración que integre los procesos principales (adquisiciones, recursos humanos, almacén, etc.) y realice la afectación de las cuentas contables y la ejecución de su presupuesto – adicional o como parte del Sistema de Contabilidad que exige la CONAC se debe tener – generaría la posibilidad de, entre otras cosas, implementar en los sistemas "alertas" sobre partidas o conceptos específicos, así como una revisión más exhaustiva tomando como base para determinar una muestra representativa, las bases de datos que pudieran descargarse del sistema en comento.

Es necesario estar muy atentos al rumbo que tomará la fiscalización de los OIC´s en la Administración Pública Federal.

Finalmente, es necesario estar muy atentos al rumbo que tomará la fiscalización de los OIC´s en la Administración Pública Federal, ya que, con la publicación en el Diario Oficial de la Federación el 04 de septiembre de 2023 de la actualización del Reglamento Interno de la SFP, nacen dos tipos de Órganos Internos de Control, los "Específicos" (Articulo 93) los cuales, pueden ser creados, modificados o extinguidos por la persona titular de la Secretaria en cualquier tiempo y en cualquiera de los casos que el mismo reglamento menciona y los "Especializados" (Artículo 102), los cuales son competentes para actuar en dependencias, incluidos sus órganos administrativos desconcentrados, y entidades que no cuenten con un órgano interno de control especifico, y exclusivamente en la materia que indique su denominación.

Lo cual, desde el punto de vista del autor, podría suponer una posible extinción de OIC´s "pequeños" y la generación de Órganos Interno de Control Especializados que presten "servicios" a diversas instituciones, muy probablemente del mismo sector.

Por lo anterior, se deberá estar muy atento a la forma en que estos nuevos conceptos se implementarán y las consecuencias de ello.

El ingeniero en sistemas y el usuario

Estaban reunidos un contador, un arquitecto, administrador de empresas, y un ingeniero en sistemas.

Empieza el contador:

La profesión más vieja del mundo es la mía.

¡No!, Le dice el arquitecto, al principio no existía nada, así que todo tuvo que ser construido, por tanto, Dios es arquitecto.

El administrador de empresas le dijo al arquitecto:

Nada que ver, al principio todo era un caos y tuvo que ser organizado tal como una empresa por tanto Dios era administrador.

Interviene el de sistemas:

No, no, no, tú dijiste que había caos al principio, si había caos ya había alguien de sistemas allí.

¡Lo que hacemos por ser Ingenieros de Sistemas!

1. Cuando el ingeniero de sistemas le diga que acude en su ayuda, desconéctese de la red y vaya por un café. No nos espere, para nosotros no es ningún problema acordarnos de todAs las claves de usuario.

2. Cuando nos llame para decirnos que cambiemos su computador de sitio, asegúrese de que lo deja bien enterrado bajo media tonelada de postales, fotos de sus niños, animales de toda clase, flores secas, trofeos varios, etc. A nosotros, como no tenemos vida privada, nos encanta echar un vistazo a la suya.

3. Cuando el ingeniero de sistemas le envíe un correo electrónico de importancia alta, bórrelo inmediatamente sin leer: Lo más probable es que estemos haciendo pruebas.

4. Cuando el ingeniero de sistemas esté almorzando, entre sin ninguna consideración y explíquele sus problemas esperando a que se le responda en el acto. Estamos aquí para servirle y siempre a punto para solucionar problemas.

5. Cuando el ingeniero de sistemas esté tomando un café tranquilamente, pregúntele algo acerca de los computadores. La única razón por la que nos vamos a tomar café, es para atender a las personas que no tienen correo electrónico o teléfono.

6. Mande todos sus mensajes en mayúsculas. El servidor de correo lo recogerá inmediatamente y lo tratará como mensaje urgente.

7. Cuando llame al teléfono del ingeniero de sistemas, pulse el número 5 para saltarse el mensaje que le dice que está de vacaciones y grabe su mensaje. Entonces, espere exactamente 24 horas antes de mandar un correo electrónico directamente a su jefe quejándose de que no ha recibido ninguna respuesta a su llamada. Usted no se merece este trato.

8. Cuando la fotocopiadora no funcione, llame al ingeniero de sistemas. Al fin, la fotocopiadora tiene cable, ¿no?

9. Cuando su módem le dé el mensaje: 'No hay tono de marcado', en casa, llame al ingeniero de sistemas. Podemos solucionar problemas de teléfono desde donde sea.

10. Cuando su computador no funcione, tírelo encima de la silla del ingeniero de sistemas y no deje ningún papel con su nombre ni la descripción del problema. Nos encanta el misterio.

Ah, ¡y discúlpennos por ser ingenieros de sistemas!

Murió un ingeniero y se fue a las puertas del Cielo.

Sabido es que los ingenieros por su honestidad siempre van al cielo.

San Pedro buscó en su archivo, pero últimamente andaba un poco desorganizado y no lo encontró en el montón de papeles, así que Le dijo:

- Lo lamento, no estás en listas...

De modo que el ingeniero se fue a la puerta del i**..., rápidamente le dieron albergue y alojamiento. Poco tiempo pasó y el ingeniero se cansó de padecer Las miserias del i**..., así que se puso a diseñar y construir mejoras.

Con el Paso del tiempo, ya tenían ISO 9000, 14000, 18000, 21000, SAP R3, monitoreo de cenizas, aire acondicionado, inodoros automáticos, escaleras eléctricas, redes de comunicaciones con fibra óptica, programas de mantenimiento predictivo, sistemas de control field bus y Hart, sistemas de control de acceso mediante huella digital, Wi-fi, I-PODs, etc etc etc etc

Y el ingeniero se convirtió en la adquisición más rentable en millones de años para el i**.....

Un día Dios llamó al Diablo por teléfono y con tono de sospecha le preguntó:

- ¿Y cómo estan por allá en el i**...?

- ¡Estamos a toda madre! - contestó el diablo - Estamos certificados ISO 9000, 14000, 18000, 21000, tenemos sistema de monitoreo de cenizas, aire acondicionado, inodoros con drenaje mediante sensor infrarrojo, escaleras eléctricas con control automático de carga, equipos electrónicos para controlar el ahorro de energía, Internet inalámbrico 811.02.g. etc.

Apunta por favor mi dirección de email: eldiablofeliz@i**....com por si algo se te ofrece...

Dios preguntó entonces:

- ¿Qué acaso TIENEN un ingeniero allí?

El diablo contestó:

- Si!

- Esto es un ENORME y GARRAFAL error, nunca debió haber llegado ahí un ingeniero! Los ingenieros siempre van al cielo, eso está escrito y resuelto para todos los casos. ¡Me lo mandas inmediatamente!

- ¡Ni loco! - dijo el diablo. Me gusta tener un ingeniero de planta en esta organización. Y me voy a quedar con él eternamente.

- Mándamelo o ... ¡TE DEMANDARÉ!

Y el Diablo, con la vista nublada por la tremenda carcajada que soltó, le contestó a Dios:

- ¿Ah Sí?? Y por curiosidad... ¿DE DÓNDE VAS A SACAR UN ABOGADO? ¡Si todos estan aqui!

Hay que entender a los ingenieros, amarlos, bendecirlos, y darle gracias a Dios por haberlos creado.

1. Un Ingeniero no es que sea prepotente, es que está rodeado de incompetentes.

2. Un Ingeniero no tiene el ego muy Grande, es que el cuarto es muy chiquito.

3. No es que quieran tener la razón siempre, es que los otros siempre hablan tonterías.

4. Un Ingeniero no es que carezca de sentimientos, es que los demás son muy débiles.

5. Un Ingeniero no tiene vida desorganizada, es solo que tiene un ritmo de vida particular.

6. Un Ingeniero no ve el mundo, lo cambia.

7. Un Ingeniero no es que sea un creído, es que los simples mortales no lo comprenden.

8. Un Ingeniero no es un ser calculador y frío, simplemente su cerebro es más fuerte que su bobo.

9. Un Ingeniero no es un crítico, es que los errores de la gente son muy evidentes.

10. Un Ingeniero no es un inútil para hacer tareas cotidianas, es que para que gastar sus valiosas energías en tonterías.

11. Un Ingeniero no comete errores, solo prueba si los demás estaban prestando atención!!

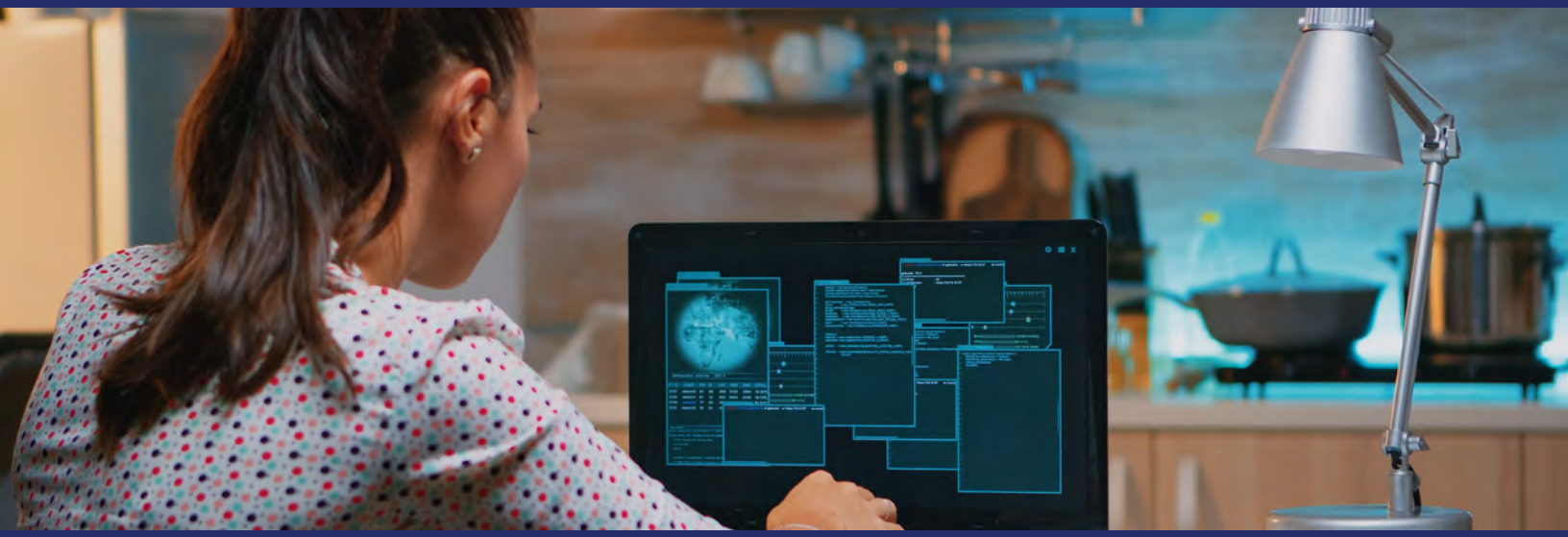
12. Un ingeniero no es aquel que tenga un titulo sino que hace valer su ingenio y esto le da valor al titulo.

15. No es que se crea un pesado, es que lo es!

Pero recuerden, ser tan cercano a la perfección tiene sus problemas así que los que no son ingenieros comprendan a estas tristes almas torturadas entre la genialidad y la incomprensión.

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

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



CISCIG 2023

Revista editada por el Colegio de Ingenieros en Sistemas Computacionales para la Seguridad de la Información, Control Interno y Gobernanza A.C.

55 73 75 3239

CISCIG
Colegio de Ingenieros
en Sistemas

CISCIG
Colegio de Ingenieros
en Sistemas

@ciscig

(55) 5038 8820

www.ciscig.mx

servicios@ciscig.mx