CUARTO TRIMESTRE 2025

ENERO , 2026

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

LA ACTUALIZACIÓN DE LA ISO 37001

UNA MIRADA AL PASADO Y AL FUTURO DEL COLEGIO

HACIA UNA CULTURA EN MATERIA DE DESEMPEÑO Y ADMINISTRACIÓN DE RIESGOS EN EL MARCO DE CONTROL DE LA ADMINISTRACIÓN PÚBLICA FEDERAL

CONTROLES DE CIBERSEGURIDAD EN SERVIDORES: HARDENING Y BUENAS PRÁCTICAS

DESCÁRGALA EN: HTTPS://WWW.CISCIG.MX/PUBLICACIONES/

CONTENIDO

CISCIG

WhatsApp:

+52 55 6736 9071

+ 52 55 3516 7586

+52 55 6502 1522

servicios@ciscig.mx

www.ciscig.mx

Número ISSN: 2992-7250- Año 3, volumen XI, Octubre – Diciembre 2025

REVISTA DEL COLEGIO DE INGENIEROS EN SISTEMAS DE COMPUTACIONALES PARA LA SEGURIDAD DE LA INFORMACIÓN , CONTROL INTERNO Y GOBERNANZA, A.C, año 3, No. XI, Octubre – Diciembre 2025, 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 Ilama # 333, Colonia Pedregal de Santo Domingo , Alcaldía Coyoacán, C.P. 04369, Ciudad de México, Tel (55) 3516 7586, www.ciscig.mx, represente legal Jorge García Alonso, jorge.garcia@ciscig.org, Editor y responsable de la última actualización de este Número Armando Avalos Pérez,armando.avalos@ciscig.org, Calle Ilama # 333, Colonia Pedregal de Santo Domingo , Alcaldía Coyoacán, C.P. 04369, Ciudad de México Reserva de Derechos al Uso Exclusivo No. 04-2023- 033115290800-102, ISBN: 2992-7250, ambos otorgados por el Instituto Nacional de Derecho de Autor, fecha de última actualización, 19 de enero de 2026.

SERVICIOS DE

consultoría

CIBERSEGURIDAD
AUDITORÍA
DESARROLLO DE SOFTWARE
DRP
CERTIFICACIÓN DE LA FUNCIÓN TECNOLÓGICA

CERTIFÍCATE CON NOSOTROS

Asegura la transparencia y la integridad en tus procesos de adquisiciones de TI. Nuestro equipo de consultores posee vasta experiencia y cuenta con certificaciones de diversos institutos tanto nacionales como internacionales.

CISCIG

CISCIG
MARCG-AVALOS, GARCÍA
Y ASOCIADOS S.C.

Como todas las cosas que valen la pena, en un momento mundial complicado pero lleno de oportunidades, a finales del 2019 con el inicio de la pandemia COVID-19, mediante el oficio DGP/363-II/2019, la Dirección General de Profesiones de la Secretaria de Educación Pública nos informó que con número de registro F-469, se autorizaba y daba inicio formal el Colegio de Ingenieros en Sistemas Computacionales para la seguridad de información, el control interno y gobernanza A.C. (en adelante CISCIG).

Si bien parecía que el inicio era también el fin, ya que el arrancar con una pandemia mundial generó que prácticamente los primeros dos años el Colegio no tuviera operaciones, también nos enseño a trabajar de otra forma o modalidad, y a ser resilientes y adaptarnos a los cambios.

En estos cinco años de actividades reportadas, nos hemos encontrados retos, ante los cuales hemos tomado acciones para apoyar y fortalecer la profesionalización de nuestra rama, entre los retos más destacados mencionamos:

1.Hemos identificado que una gran cantidad de servicios entregados por fabricantes, cargos públicos, así como direcciones y gerencias que debieran ser puestos ocupados por ingenieros en computación o sistemas están siendo ocupados por profesionales de otras ramas, carreras truncas e incluso, personal que no cuentan con las capacidades técnicas para entregar un servicio profesional.

2.Los fabricantes han inundado el mercado de la capacitación realizando “”certificaciones”” que carecen de las bases necesarias para un entendimiento de los servicios requeridos de manera integral por los consumidores de tecnologías, realizando capacitaciones sesgadas a sus productos y cuyas “certificaciones” están limitadas únicamente a la venta de sus propios productos.

3.El principal problema es que estimamos que aproximadamente un 70% de los profesionales que se encuentran en el campo laboral, no cuentan con una cédula profesional. Esta estadística se agrava con la edad, pues a mayor edad, menor probabilidad de contar con una cédula profesional.

Por lo anterior, y en un ejercicio de transparencia y rendición de cuentas, presentaremos a todos nuestros asociados e interesados, un breve informe de las actividades, logros y compromisos realizados desde el inicio de operaciones hasta diciembre del 2025:

I.ACTIVIDADES REALIZADAS
INTEGRACIÓN DE PROFESIONISTAS

Durante estos cinco años, hemos logrado captar una gran cantidad de profesionales en la rama, y hemos colaborado activamente con otros colegios e instituciones educativas. Estamos seguros de que seguiremos creciendo y ganando el reconocimiento de nuestra sociedad, impactándola de manera profunda.

Por lo anterior, a septiembre de 2025, el Colegio cuenta con 263 asociados de pleno derecho y 126 asociados (sin cédula profesional).

CONVENIOS CELEBRADOS

Como parte de la estrategia se ha buscado la colaboración con otros colegios e instituciones educativas, así como entidades gubernamentales y privadas, logrando acuerdos de colaboración con algunos de ellos.

Destacamos que la relación con los fabricantes se ha limitado a la promoción de la tecnología y no a la venta de productos específicos, por lo que, a pesar de contar con una amplia colaboración de estos, no hemos aceptado acuerdos de colaboración que limiten la participación y eventos a solo una marca en específico.

Algunas de las instituciones con las que hemos hecho convenios son las siguientes:

·ORGANISMO PROMOTOR DE INVERSIONES EN TELECOMUNICACIONES

·CENTRO DE ESTUDIOS SUPERIORES DE VERACRUZ (CESUVER)

·INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, A.C. (INAP)

·COLEGIO NACIONAL DE INTEGRACIÓN PROFESIONAL, S.C. (CONAIP)

·INSTITUTO ESPECIALIZADO EN COMPUTACIÓN Y ADMINISTRACIÓN GAUSS JORDÁN, A.C.

·INSTITUTO TECNOLÓGICO DE TLÁHUAC

·INSTITUTO TECNOLÓGICO DE ZACATECAS

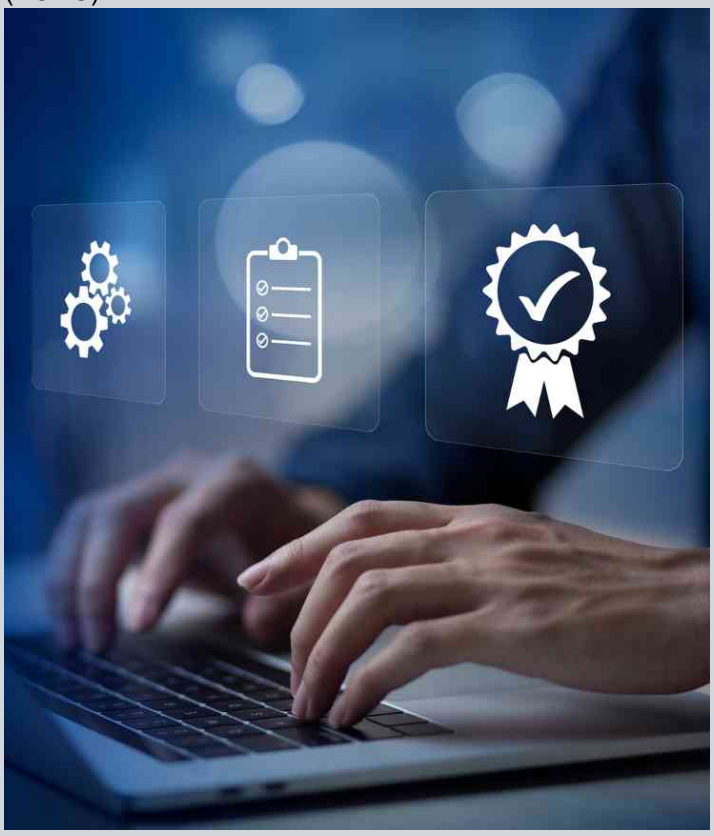
CERTIFICACIONES TÉCNICAS

Como parte de la especialización y diferenciación, el CISCIG ha generado ocho certificaciones técnicas, las cuales avalan la experiencia de nuestros asociados en diversas área de la ingeniería, incluido el control interno y la gobernanza:

Profesional Certificado en Administración de centros de datos (PCACD).

El profesional certificado ha demostrado sus conocimientos y habilidades para integrar, administrar, operar y actualizar los centros de datos de manera eficiente, demostrando las mejores prácticas desde la planeación, adquisiciones e implementación.

Profesional Certificado en Redes y Comunicaciones (PCRC).



El profesional certificado ha demostrado sus conocimientos y habilidades en la integración de soluciones de redes y comunicaciones a través de la integración de redes locales, nube, hiperconvergencia o sistemas de comunicación híbridos.

Profesional Certificado en Seguridad de Información (PCSI).

El profesional certificado ha demostrado sus conocimientos y habilidades para evaluar el sistema de seguridad, las actividades de control y las herramientas implementadas para garantizar la seguridad perimetral, interna y operativa de los sistemas de información.

Profesional Certificado en Auditoría de tecnologías de información (PCATI).

El profesional certificado ha demostrado sus conocimientos y habilidades para auditar al área de tecnología de información con base a las normas internacionales aceptadas, en cada uno de sus procesos y proyectos, con el fin de emitir una opinión sobre la gobernanza, el sistema de control interno, la eficacia, eficiencia y economía del área. El profesional está también habilitado en metodologías forenses.

Profesional Certificado en Administración de Proyectos de Tecnologías de Información (PCAPTI).

El profesional certificado ha demostrado sus conocimientos y habilidades para diseñar, planear, administrar, ejecutar y supervisar los proyectos de tecnología de información, priorizando el uso eficiente y eficaz de los recursos, así como el cumplimiento del alcance en tiempo y forma, haciendo énfasis en la debida documentación de cada etapa del proceso.

Profesional Certificado en Desarrollo de Software (PCDS).

El profesional certificado ha demostrado sus conocimientos y habilidades, basado en las mejores prácticas internacionales, en el desarrollo de software, priorizando la debida documentación de cada etapa y papel de trabajo, así como garantizando la continuidad e integridad de futuras modificaciones, el profesional debe asegurar que el código y sus procesos han sido debidamente documentados y la propiedad intelectual del patrocinador del proyecto asegurada.

Profesional Certificado en Análisis y Minería de Datos (PCAMD).

El profesional certificado ha demostrado sus conocimientos y habilidades aplicando métodos cuantitativos y cualitativos a las bases de datos, metadatos y cualquier información recopilada para establecer tendencias e identificar información relevante para los procesos de negocio.

Profesional Certificado en Control Interno y Gobernanza (PCCIG).

El profesional certificado ha demostrado sus conocimientos y habilidades para diseñar y/o evaluar un marco de control interno para una entidad o para un proceso específico, aplicando un análisis detallado de los diferentes marcos de control aceptados internacionalmente, a fin de lograr una identificación y mitigación de riesgos eficiente.

REVISTA DIGITAL DEL COLEGIO

Desde 2023 se publica la revista digital del Colegio, la cual cuenta con un número importante de colaboradores y que ha sido bien recibida no solo por nuestros socios y público en general, ya que hemos detectado la referencia en nuestra revista en diferentes fabricantes e instituciones educativas.

Es una publicación trimestral de carácter científico, de investigación y docente como medio de difusión oficial del Colegio de Ingenieros en Sistemas de Computacionales para la Seguridad de la Información Control Interno y Gobernanza, A.C. con el fin de promover la innovación científica, metodologías y mejores prácticas en entre los socios e interesados en las Tecnologías de la Información, el Control Interno y la Gobernanza.

El propósito de la revista es presentar la opinión de ponentes, divulgar información científica y tecnológica. La Revista CISCIG NO cobra por la publicación de artículos a los autores ni por la lectura de sus contenidos a los lectores vía web, y está adherida a la filosofía de acceso abierto y permite la divulgación libre del contenido de los artículos por parte de los autores y los lectores siempre y cuando sea citado su contenido con rigor de acuerdo a las normas de citación APA 6ta edición.

Nuestra cuenta con los derechos de autor, así como registro ISSN.

Te invitamos a colaborar escribiendo artículos, así como seguir cada publicación trimestral

CONFERENCIAS Y COLABORACIÓN ACADÉMICA

Como parte de nuestra difusión hemos colaborado con diferentes entidades públicas y privadas a través de conferencias, paneles y cursos, que se han impartido de manera gratuita.

Te invitamos a seguir estar actividades por internet y nuestros webinars, los cuales iniciaron desde el año 2024 con especialistas en cada uno de los temas revisados.

Asimismo, contamos con capacitación especializada en temas relacionados con la Tecnología de la Información, la Ciberseguridad, Auditoría a la T.I, servidores, administración de proyectos así como el Control Interno y la Gobernanza corporativa, si requieres mayor información, no dudes en buscarnos, nuestros especialistas tienen mas de 20 años de experiencia en sus diversas áreas.

REGISTRO DE PERITOS PARA EL PODER JUDICIAL

La Suprema Corte de Justicia de la Nación, nos ha invitado a formar parte de su catálogo de peritos a fin de fortalecer la justicia digital en México.

Por lo que a finales de 2025, el Colegio propuso a 4 peritos para el catálogo de la Suprema Corte de Justicia de la Nación, todos ellos certificados por el mismo Colegio y por instituciones internacionales.

El propósito de la revista es presentar la opinión de ponentes, divulgar información científica y tecnológica.

ACUERDO 286

Desde 2023, diferentes evaluadoras nos han solicitado una opinión referente a la aprobación de las capacidades de los aspirantes de la carrera de ingeniería en computación y sistemas para el cumplimiento del Acuerdo 286.

Cada trimestre recibimos las solicitud y se han realizados los esfuerzos para responder en tiempo y forma, así como el tener reuniones con los titulares de las evaluadoras a fin de lograr acuerdos sobre los criterios que determinan la capacidad técnica de los aspirantes.

De enero 2023 a septiembre de 2025, se han emitido más de 250 opiniones para aspirantes al ACUERDO 286 para la titulación de Ingeniería en Sistemas Computacionales, para las evaluadoras CONAIP, GAUSS – JORDÁN, CESUVER Y CENEVAL.

I. PROYECTOS PARA 2026

PLATAFORMA DE CAPACITACIÓN

Si bien ya contamos con una plataforma que apoya con los conocimientos elementales la capacitación para el programa 286 para cualquier evaluadora, nuestra intensión para 2026 es que cuente con un mayor número de cursos y diplomados para nuestros asociados e interesados.

CERTIFICACIÓN DE IDONEIDAD

Nuestro primer contacto para iniciar la certificación de idoneidad fue en 2019, sin embargo, al tener un costo privativo para nuestro Colegio, se buscó el acuerdo con otra entidad evaluadora, logrando dicho acuerdo en 2022.

Cabe destacar que desde esa fecha un equipo multidisciplinario de profesionales en la rama como ingenieros especializados en seguridad de información, desarrollo de software, auditoría, centro de datos, administración de proyectos, así como asesores pedagogos, y especialistas de otros institutos han colaborado para lograr la integración de los Syllabus, materiales, preguntas modelo, materiales de referencia, modelo de evaluación, código de ética, convocatorias y metodología para integrar los comités nacionales.

Se espera que dichos comités validen los trabajos realizados y representa al colegio a nivel nacional. A continuación, mencionamos las propuestas y acuerdos que se presentaron para este proyecto.

CREACIÓN DE SIETE COMISIONES HONORÍFICAS

Con la finalidad de coadyuvar y dar continuidad a los proyectos estratégicos del Colegio, se propuso en la última Asamblea General Ordinaria, la creación de siete Comisiones Honoríficas siguientes:

1. Comisión de Ciberseguridad.
2. Comisión de Seguridad de Información.
3. Comisión de Auditoría de Tecnología de Información.
4. Comisión de Nube y servicios en internet.
5. Comisión de Desarrollo de software.
6. Comisión de Data Center.
7. Comisión de Redes y Comunicaciones.

Por lo cual, si eres especialista en alguna de esas ramas, te invitamos a proponerte y proponer a tu equipo de trabajo.

RELACIÓN CON FABRICANTES DE TECNOLOGÍA

Nuestro colegio tiene como objetivo estratégico mantenerse agnóstico ante cualquier marca o producto específico, sin embargo, el acercamiento con los fabricantes de tecnología es indispensable para lograr una comunicación con los profesionales y mantener un programa de profesionalización “fresco” y de vanguardia.

Por lo anterior, y buscando siempre potenciar el talento nacional en el ámbito de las tecnologías de información, la Seguridad de la Información, el Control Interno y la Gobernanza en México, queremos agradecer a nuestros asociados, amigos y profesionistas de otras carreras que han brindado su tiempo, esfuerzo y conocimiento para que el CISCIG continue en crecimiento continuo, buscando siempre generar valor tanto a nuestros asociados, como a nuestra sociedad.

Sin otro particular, reciba un cordial saludo.
Ed. Dr. Armando Avalos Pérez
Presidente Fundador
MBA, Ingeniero en Computación

CONAIP®

Colegio Nacional de Integración Profesional

Instancia Evaluadora Acuerdo 286 02/04/17

¡CONCLUYE TUS ESTUDIOS!

PROCESO REGIDO BAJO ACUERDO

286 / SEP

NUESTRO PROCESO ES RECONOCIDO POR LA SECRETARÍA DE EDUCACIÓN PÚBLICA.

TENEMOS MÁS DE 20 AÑOS PROFESIONALIZANDO A 10 TRABAJADORES DE MANERA DIARIA.

INGENIERÍA

- INDUSTRIAL
- COMPUTACIONAL

BACHILLERATO EN UN SOLO EXAMEN

LICENCIATURA POREXPERIENCIA LABORAL

- PEDAGOGÍA
- ADMINISTRACIÓN

¡TERMÍNALOYA!

¿QUÉ ESTÁS ESPERANDO?

OBTÉN TU CERTIFICADO DE BACHILLERATO O TÍTULO PROFESIONAL CON VALIDEZ OFICIAL SEP.

¡CONTÁCTANOS!

¡INSCRÍBETE YA!

GM
GRUPO

UN GRUPO DE EMPRENDEDORES MEXICANOS DEDICADOS AL **ÉXITO DE TU EMPRESA.**

EXPERTOS EN TU TRANQUILIDAD FISCAL

Soluciones contables, administrativas y financieras que **generan resultados** para tu empresa.

ASESORÍA LEGAL
Protección jurídica total para tu empresa.

SISTEMAS
Implementamos la tecnología que tu giro necesita para mayor eficiencia.

AHORRO ESTRATÉGICO
Reducimos al mínimo el pago de impuestos de forma legal y estratégica.

FINANZAS SANAS
Expertos en regularización de empresas con sobre-endeudamiento.

NUESTROS SERVICIOS

- Determinación de pago de impuestos y Contabilidad Electrónica
- Auditorías y Planeación Financiera
- Flujos de Efectivo y Estados Financieros proyectados
- Gestión de nóminas a costo preferencial

¿QUIÉNES SOMOS?

Somos un grupo de emprendedores mexicanos enfocados en el éxito de tu empresa.

Impulsamos la productividad, rentabilidad y efectividad de tu negocio con procesos profesionales y resultados reales.

Nos encargamos de la administración contable, financiera y de personal para que tú te enfoques en lo más importante: **hacer crecer tu empresa**.

NUESTROS PROCESOS CONTABLES

- Identificar el giro de la empresa
- Asignarle el sistema adecuado al giro y volumen de facturación
- Hacer papeles de trabajo y relacionarlo al sistema
- Determinar el pago de impuestos en relación al flujo de efectivo
- Realizar el pago de contribuciones
- Determinar estados financieros y proyectarlos
- Determinar cuotas obrero patronales exactas
- Análisis financiero para finanzas sanas
- Regularizar empresas con sobre-endeudamiento

VENTAJAS DE CONTRATAR NUESTROS SERVICIOS

- Mejor precio del mercado
- Asesoría legal completamente incluida
- Reportes de sus finanzas de forma mensual
- Contacto continuo con nuestros clientes
- Sistemas incluidos según las necesidades de tu giro
- Servicios de gestión de nóminas a costo preferencial

¡AGENDA TU CITA AHORA!

Recibe tu cotización a un precio especial.

WHATSAPP 5514970322

WHATSAPP 5564351002

EMAIL grupo-gm19@outlook.es

COL. CUAUHTÉMOC, ALCALDÍA CUAUHTÉMOC, CP. 06500 CDMX

NUESTRA MISIÓN

Ser líderes en México en la administración de servicios contables en empresas PYMES.

NUESTRA VISIÓN

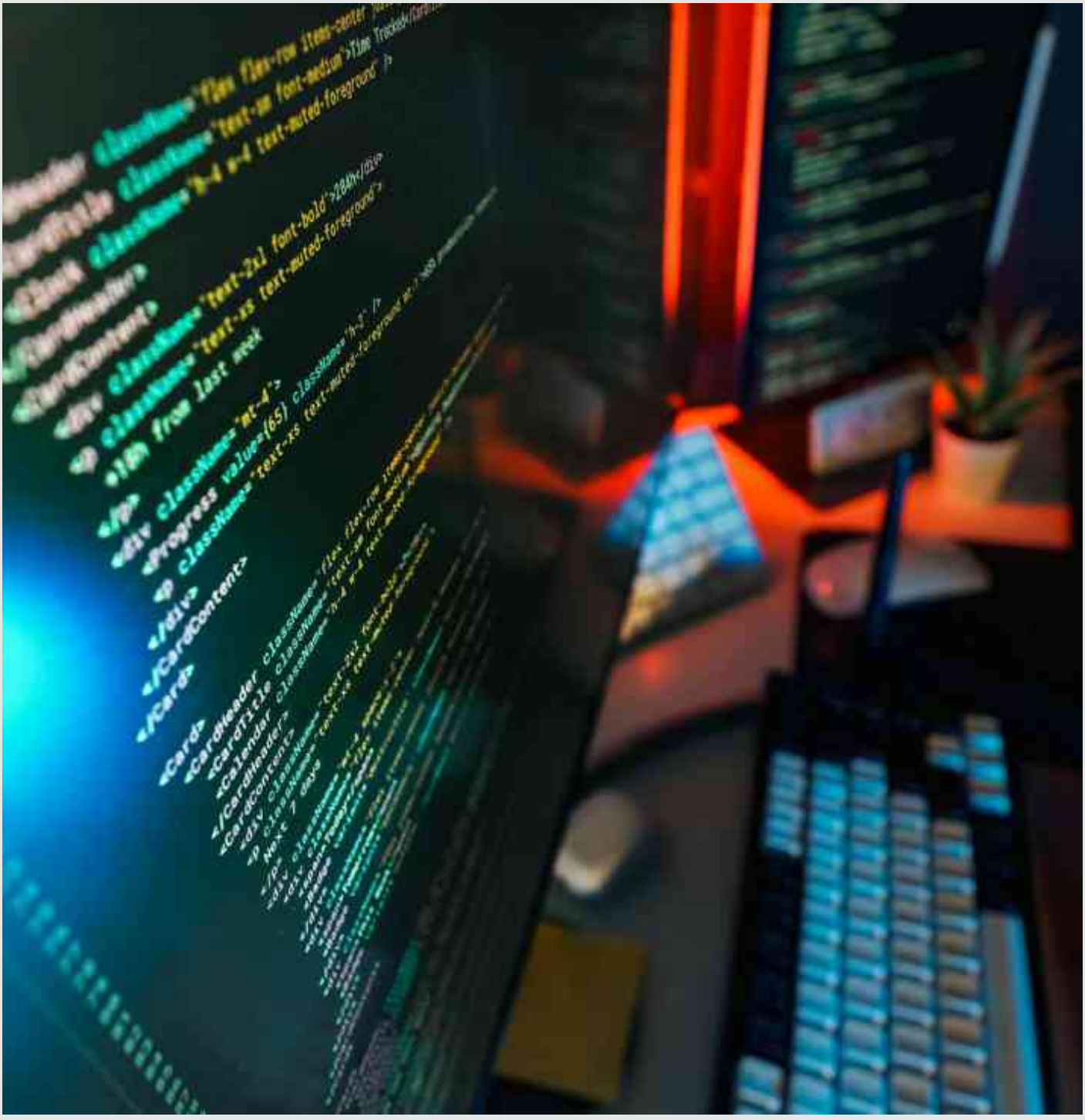
Lograr organizaciones más competitivas, eficaces y eficientes en la gestión contable y financiera.

TU ÉXITO ES NUESTRO COMPROMISO

CONTROLES DE CIBERSEGURIDAD EN SERVIDORES: HARDENING Y BUENAS PRÁCTICAS

Los servidores son la columna vertebral de la infraestructura TI, alojando servicios críticos y datos sensibles que los convierten en blancos frecuentes de ataques

ING. JOAQUÍN ORTÍZ FLORES, CISA



EL ENFOQUE ES ANALÍTICO Y RIGUROSO, CON FUENTES OFICIALES CLAVE CITADAS PARA SUSTENTAR CADA RECOMENDACIÓN.

Resumen ejecutivo

Los servidores son la columna vertebral de la infraestructura TI, alojando servicios críticos y datos sensibles que los convierten en blancos frecuentes de ataques[1]. El hardening busca reducir la superficie de ataque de estos sistemas aplicando configuraciones seguras, eliminando componentes innecesarios y reforzando controles de acceso[2][3]. Este artículo aborda en detalle los objetivos del hardening, los marcos normativos relevantes (CIS, NIST, ISO, OWASP, SANS), y presenta controles técnicos y administrativos esenciales: gestión de parches, configuración segura de SO (Linux/Windows), servicios mínimos, cuentas/privilegios, MFA, cifrado, gestión de claves, auditoría (logging/SIEM), detección de intrusiones, respaldo y recuperación, segmentación de red, fortalecimiento de aplicaciones/contenedores, virtualización y cloud, así como pruebas y auditorías. Se incluyen comandos y ejemplos concretos (Linux/Windows), métricas de éxito, una lista de verificación operativa, una plantilla de políticas y diagramas de flujo en formato mermaid. El enfoque es analítico y riguroso, con fuentes oficiales clave citadas para sustentar cada recomendación.

Contexto y objetivos del hardening

Los servidores suelen venir por defecto configurados para facilidad de uso, lo cual expone vulnerabilidades. El hardening implica ”reducir la exposición de un sistema para dificultar su ataque”, cerrando servicios y configurando sólo lo necesario[2]. Según NIST, los servidores proveen múltiples servicios (bases de datos, autenticación, aplicaciones web, etc.) y son atacados tanto por la gran cantidad de datos que albergan como por las consecuencias de comprometerlos[1]. Por ello se recomienda aplicar seguridad desde la fase de planificación, integrando controles organizativos (políticas, capacitación, gestión de cambios, planes de contingencia) y técnicos, y validar configuraciones antes del despliegue[4][5]. El objetivo fundamental del hardening es asegurar la confidencialidad, integridad y disponibilidad de la información del servidor mediante políticas y prácticas concretas: aplicar parches, restringir privilegios, proteger credenciales, cifrar datos, activar auditoría y contención de la red, entre otros[6][7]. Un sistema reforzado reduce la probabilidad de explotación y limita el daño en caso de compromiso, facilitando también la detección de incidentes.

MARCOS Y ESTÁNDARES RELEVANTES

Existen varios marcos y estándares que guían las buenas prácticas de seguridad, cada uno con distinto ámbito y aplicabilidad:

Marco/Estándar	Alcance	Aplicabilidad	Prioridad
CIS Benchmarks	Guías prescriptivas de configuración segura para cientos de sistemas (OS, bases de datos, redes, etc.)[8].	Enfoque práctico; aplicables a sistemas específicos (Linux, Windows, routers, cloud). Creados por consenso global.	Alta – base de referencia para endurecimiento OS y apps.
CIS Controls (SANS)	18 controles priorizados de ciberseguridad (antes SANS Top 20) de alcance general[9].	Enfocado a organizaciones de cualquier sector. Ayuda a lograr higiene básica (parches, inventario, restricción de acceso).	Alta – punto de partida general y alineación regulatoria.
NIST SP 800-53	Catálogo extensivo de controles de seguridad y privacidad para sistemas y organizaciones[10].	Federal EUA y empresas grandes; cubre políticas, procedimientos, controles técnicos integrales.	Alta – marco completo de gestión de riesgos.
NIST SP 800-123	Guía de seguridad específica para servidores (OS, aplicaciones, parches, auditoría) [5].	Servidores en general; ideal para equipos de TI corporativos.	Media – complemento al SP 800-53 para servidores.
NIST SP 800-70	Programa Nacional de Checklists (configuraciones seguras) de NIST.	Publica listas de chequeo de sistemas (OS, aplicaciones) para cumplir estándares.	Baja – recurso técnico auxiliar de configuración.
ISO/IEC 27001	Estándar internacional de SGSI; exige gestión de riesgos y controles organizativos (Anexo A)[11].	Para organizaciones que buscan certificación de seguridad.	Alta – marco de gestión, requiere selección basada en riesgos.
OWASP Top 10	Lista de los 10 riesgos críticos de seguridad en aplicaciones web[12].	Desarrolladores y equipos de seguridad de aplicaciones.	Media – prioriza seguridad de apps web específicas.
SANS/CIS Controls	Mismas "CIS Controls" ya mencionadas, jerarquizando 20 controles críticos.	Uso amplio para mejorar postura general.	Alta – proporciona prioridades claras para acción.

El tablero comparativo anterior sintetiza las diferencias. Por ejemplo, CIS Benchmarks ofrece directrices muy específicas de configuración segura (primera línea de defensa técnica), mientras que ISO 27001 provee un marco de gestión más amplio. NIST 800-53 es integral (incluye configuraciones, pero también capacitación, gestión de cambios, etc.)[10]. OWASP y CIS Controls están más focalizados en riesgos de aplicaciones y ciberhigiene respectivamente. En la práctica, estos marcos suelen combinarse: por ejemplo, se puede usar NIST o ISO para gobernanza y CIS Benchmarks para endurecer los sistemas.

Controles técnicos y administrativos

Gestión de parches

Mantener los servidores parcheados es fundamental. Los atacantes explotan vulnerabilidades conocidas a los pocos días de difundirse, por lo que los sistemas sin parches acumulan riesgos que ningún ciclo de actualización posterior puede eliminar[6]. La política de parches debe incluir: inventario de software activo; alertas automáticas de nuevos parches (ej. WSUS, repositorios, suscripciones de seguridad); priorización (criticidad/CVSS); pruebas controladas en entornos de staging; despliegue escalonado; e informes de cumplimiento. Ejemplo concreto (Linux Ubuntu):

```
sudo apt update && sudo apt upgrade -y # Actualiza listas de paquetes e instala parches críticos
```

En Windows Server, puede usarse PowerShell y WSUS/SCCM:

```
# Obligatorio: habilitar actualizaciones automáticas
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" -Name AUOptions -Value 4
# o usar Automate Updates (Autopatch) / Intune
```

Riesgos: sistemas sin parches son vulnerables a exploits publicados y malware. *Métricas:* porcentaje de servidores al día con parches, tiempo medio de aplicación tras release, número de vulnerabilidades críticas sin corregir.

Configuración segura del sistema operativo (Linux / Windows)

Consiste en aplicar guías de endurecimiento. En Linux se recomienda eliminar paquetes no usados (“minimizar huella de software” reduce vectores de ataque[3]), deshabilitar servicios (systemd) y cerrar puertos. Por ejemplo:

```
# Linux: deshabilitar servicios inútiles (ej. servicio Avahi)
sudo systemctl stop avahi-daemon.service
sudo systemctl disable avahi-daemon.service
# Establecer políticas firewall base (iptables/nft)
sudo iptables -P INPUT DROP
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT # permitir SSH
```

En Windows Server se aconseja eliminar Roles y Características innecesarias y cerrar puertos no esenciales. Por ejemplo, si no se requiere Servidor Web, desinstalar IIS. Las mejores prácticas incluyen: cambiar nombre de la cuenta Administrador local, deshabilitar la cuenta Invitado, restringir grupos integrados (Administradores, Usuarios) a lo mínimo[13]. En PowerShell:

```
# Deshabilitar cuenta Guest
Disable-LocalUser -Name Guest
# Renombrar Administrador Local
Rename-LocalUser -Name "Administrator" -NewName "srv-admin-$(Get-Random)"
```

Y en GPO: aplicar plantillas administrativas para reforzar configuraciones (por ejemplo, “Security Options” para bloqueo de cuentas, encriptación SMB, etc.). Riesgos:configuración por defecto (por ejemplo, servicios de red abiertos, Remote Desktop sin restricción) facilitan ataques como fuerza bruta. Métricas: número de servicios/minutos de escucha deshabilitados (auditoría); porcentaje de servidores configurados según benchmark (CIS).

Servicios mínimos

Un servidor debe ejecutar sólo los servicios necesariospara su función. Cada servicio adicional amplía la superficie de ataque. En Linux conviene revisar systemctl list-unit-files --type=service --state=enabled y deshabilitar lo no esencial. En Windows, funciones como File and Printer Sharing,NetBIOS o Web Browser no deben instalarse salvo uso requerido[14]. Por ejemplo:

```
# Linux: eliminar paquetes orfanos
sudo apt purge nombre_paquete
sudo apt autoremove
# Windows: deshabilitar servicio de Registro Remoto si no se usa
Stop-Service -Name RemoteRegistry
Set-Service -Name RemoteRegistry -StartupType Disabled
```

Riesgos: servicios innecesarios pueden incluir vulnerabilidades (p. ej. servidor web local que nunca se actualiza). Métricas: Reducción en número de puertos abiertos.

Gestión de cuentas y privilegios

Aplicar el principio de mínimo privilegio. Cada usuario debe tener la menor autoridad necesaria. Se recomienda: políticas de contraseñas fuertes (p.ej. mínimo 15 caracteres y cambios periódicos[15]), bloqueo de cuentas tras intentos fallidos, autenticación multifactor (ver siguiente sección) y revisión frecuente de cuentas inactivas. Ejemplos:

Linux: utilizar /etc/sudoers (visudo) para asignar permisos específicos. Asegúrese que /etc/sudoers es propiedad de root y sólo legible (chmod 440). Se pueden agregar restricciones:

```
# Solo el grupo 'admin' puede ejecutar todo con sudo y debe autenticarse cada vez:
%admin ALL=(ALL) PASSWD: ALL
Defaults timestamp_timeout=0  # obligar re-autenticación cada vez[16]
Defaults requiretty  # sudo sólo en terminal local
```

Windows: crear usuarios y grupos administrativos separados; auditar membresías de Administradores/Domain Admins. En GPO puede aplicar bloqueo de cuentas (ej. 5 intentos en 15 minutos)[15].

Justificación: Minimizar cuentas reduce riesgos de credenciales robadas. Riesgos: contraseñas débiles o cuentas huérfanas facilitan accesos no autorizados. Métricas: % de cuentas con MFA, % de cuentas inactivas eliminadas, tiempo medio de detección de cuentas huérfanas.

Autenticación multifactor (MFA)

Implementar MFA en accesos críticos (especialmente administrativos y accesos remotos). Por ejemplo, exigir token o app de autenticación para RDP, SSH o portales web internos. Muchos proveedores (Azure AD, Duo, etc.) integran MFA con entornos Windows/Linux. Justificación:atenúa el riesgo de credenciales comprometidas.Implementación: habilite MFA en servidores RDP (Directiva de Seguridad o Azure MFA Server), configure SSH para usar libpam-google-authenticator o authy, etc. Riesgos: sin MFA, solo password = mayor chance de intrusión; con MFA, el atacante necesitaría el dispositivo/token.

Cifrado en tránsito y en reposo, gestión de claves

En tránsito: forzar HTTPS/TLS en aplicaciones web y administración remota (SSH, RDP). Por ejemplo, en SSH:

```
# Linux: asegurar SSH con cifrado fuerte
echo "Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com" >> /etc/ssh/sshd_config
echo "MACs hmac-sha2-256,hmac-sha2-512" >> /etc/ssh/sshd_config
systemctl restart sshd
```

En Windows: habilitar Require strong SSL/TLS en servicios IIS, RD (Ej. en GPO 'Sistema: Configurar canales de cifrado TLS').

En reposo: cifrar discos completos (Linux LUKS, Windows BitLocker) y bases de datos (Transparent Data Encryption). Por ejemplo, en Linux puede usarse LUKS para particiones sensibles; en Windows, BitLocker con TPM para OS y datos[17].

Gestión de claves: usar un servicio de gestión de claves (si aplica, HSM) o políticas de rotación. Nunca almacenar claves en texto plano.

Justificación: protege información si la máquina o disco es robado. Riesgos: datos sin cifrar son triviales de extraer.Métricas: % discos cifrados, comprobación de exp. de certificados/CAC.

Logging y monitoreo (SIEM)

Configurar registro centralizado y monitoreo continuo. Todos los eventos críticos (logins, cambios de configuración, errores de autenticación) deben ser enviados a un servidor de logs seguro o SIEM (p.ej. Elastic, Splunk, EDR comercial). Por ejemplo, en Linux editar/etc/rsyslog.conf para reenviar logs a servidor remoto; en Windows activar Subcriptor de eventos hacia un syslog/ADX/Defender for Cloud. Es vital retener logs con integridad: Red Hat recomienda montar /var/log/audit en partición separada y configurar acciones (disk_full_action = HALT) para evitar sobreescritura[7][18]. Adicionalmente, habilitar auditd en Linux:

```
sudo systemctl enable auditd && sudo systemctl start auditd
# Ejemplo de regla para monitorear cambios en /etc/passwd
sudo auditctl -w /etc/passwd -p wa -k passwd_changes
```

Si se registra un cambio, se podrá buscar con ausearch -k passwd_changes. En Windows, activar Auditoría Avanzadaen GPO (eventos de inicio de sesión exitoso/erróneo, cambios en usuarios) y dirigir eventos a SIEM. Riesgos: sin logs adecuados es casi imposible investigar incidentes.Métricas: cobertura de monitoreo (p.ej. % de eventos críticos detectados), tiempo de alerta promedio ante anomalías.

Detección/prevención de intrusiones

Complementario al SIEM, desplegar IDS/IPS (snort, Suricata en Linux; NSM/EDR comerciales en todos los servidores). Estas soluciones analizan tráfico o comportamientos anómalos (p.ej. conexiones externas inusuales, procesos sospechosos) y generan alertas. Configurar reglas básicas de IDS para ataques comunes (escaneos de puertos, intentos de exploit). Implementación:por ejemplo, instalar Snort/Suricata en servidor dedicado o como sensor de red, actualizar firmas. Justificación: detecta ataques que log por sí mismo no identificaría. Métricas:cantidad de alertas legítimas / false positives, tiempo de respuesta a eventos de IDS.

Backups y recuperación

Implementar un plan de copia de seguridad y recuperaciónrobusto. Incluir: copias regulares (full/diferenciales) de datos y sistemas, almacenamiento seguro (mejor fuera de línea o en sitio remoto cifrado), pruebas periódicas de restauración y política de retención. Por ejemplo, en Linux puede usarsersync --archive --delete hacia un NAS, en Windows la herramienta Windows Server Backup o scripts PowerShell con wbadmin. Además, mantener respaldos de logs críticos y claves de cifrado. Riesgos: falta de recovery post-incidente.Métricas: % backups exitosos, tiempo medio de restauración (RTO).

Segmentación de red

Separar la red en segmentos según funciones y niveles de confianza. Por ejemplo, servidores críticos en VLAN separadas, DMZ para sistemas expuestos (web/mail), y subredes aisladas entre sí. Aplicar ACLs/Firewalls internos para limitar tráfico. Una buena segmentación impide que un atacante que comprometa un servidor se mueva lateralmente fácilmente. Justificación: "segmentar es limitar la exposición" (p.ej. aislar RDP solo desde direcciones IP confiables)[19]. Métricas: número de segmentos implementados, tiempo de containment ante un ataque simulado.

Hardening de aplicaciones y contenedores

Además del SO, las aplicaciones deben reforzarse. Seguir estándares como OWASP Top 10 para desarrollo seguro[20]. Para contenedores Docker/Kubernetes, usar imágenes oficiales minimizadas, no ejecutar procesos como root, y aplicar los CIS Docker Benchmarks[21]. Docker publica"Hardened Images" que cumplen CIS Benchmark sección de imágenes[22]. Ejemplos: usar contenido trust (firmas de imágenes), limitar capacidades del contenedor. Riesgos:aplicaciones con fallos (inyección SQL, desbordamientos) permiten acceso al servidor. Métricas: % aplicaciones escaneadas en SAST/DAST, número de CVEs en imágenes base.

Virtualización y nube

En entornos virtualizados (VMs) o multi-nube, aplicar principios similares. Asegure hipervisores y plataformas de virtualización: mantenerlos actualizados y configurados seguro (por ejemplo, en VMware o Hyper-V deshabilitar servicios innecesarios). En la nube, seguir el modelo de responsabilidad compartida: proteger las instancias con firewall/cloud security groups, cifrado de volúmenes y gestión de identidades (IAM). Use herramientas de gestión centralizada (Azure Arc, AWS Systems Manager) para parches/configuración multicloud (como señala Microsoft[23]). Riesgos: sobredependencia de la infraestructura cloud puede causar mala configuración; por ello auditar configuraciones con herramientas automatizadas (CF-Benchmarks, KubeBench).

Pruebas y auditoría

Finalmente, validar y auditar los controles. Realice pentestsregulares, escaneos de vulnerabilidades (Nessus, OpenVAS) y revisiones de cumplimiento (por ejemplo, SCAP, Tenable Compliance). Implemente monitoreo continuo con métricas (por ejemplo, % parches aplicados, N° de cuentas con exceso de privilegios). Documente las políticas y entrenamientos. Métricas de éxito generales: reducción de incidentes, cobertura de controles (evaluada por auditorías internas/externas) y cumplimiento de estándares.

Checklist operativo y plantilla de políticas
Inventario y evaluación de riesgos:

Mantener actualizado inventario de servidores, OS, aplicaciones. Evaluar amenazas y clasificar activos.
Parches y actualizaciones: Parcheo automático o gestionado con SLAs. Pruebas previas de parches críticos.
Configuración base: Aplicar CIS Benchmarks o Group Policies para durizar sistemas (reforzar sshd_config, registro de auditoría, políticas de contraseña, etc.).
Servicios y puertos: Deshabilitar servicios innecesarios (servicios de Windows, demonios Linux) y cerrar puertos no usados.
Cuentas y privilegios: Deshabilitar/renombrar cuentas por defecto (Guest, Admin), asignar mínimo privilegio, auditar elevaciones (sudo, grupos).
Autenticación: Habilitar MFA para administradores y accesos remotos.
Cifrado: Encriptar discos (BitLocker/LUKS) y datos sensibles. Forzar TLS en comunicaciones (SSL/TLS 1.2+).
Logging/monitoreo: Canalizar logs a servidor central o SIEM. Monitorear actividad anómala (login fallidos, cambios de configuración).
Detección de intrusos: Implementar IDS/IPS o EDR con actualizaciones de firmas.
Backup: Respaldos diarios/semanales con retención acorde a políticas de negocio. Pruebas regulares de restauración.
Red: Segmentar redes (DMZ, VLANs, subredes internas). Configurar Firewalls/NSGs para restringir tráfico intersegmentos.
Aplicaciones/Contenedores: Usar imágenes seguras (CIS Docker Benchmarks), actualizar aplicaciones, remover plugins no usados.
Virtualización: Parches al hypervisor, restringir accesos a consolas de virtualización. En nube, habilitar cloud-native firewalls, cifrado y logs de auditoría (CloudTrail/Azure Monitor).
Auditoría: Revisar periódicamente cumplimiento (auditorías internas, pentests, certificaciones ISO/NIST).

(auditorías internas, pentests, certificaciones ISO/NIST).

Política/Tema	Descripción resumida	Responsable
Gestión de parches y actualizaciones	Definir frecuencia de parches (mensual/bimensual); canales de distribución (WSUS, repositorios internos); pruebas previas; aprobar cambios mediante CMDB.	Equipo de Infraestructura / TI
Configuración segura	Aplicar guías de endurecimiento (CIS Benchmarks, GPO, secpol); blindaje de SSH/WinRM; políticas de contraseña MFA.	Seguridad TI / Administradores de Sistema
Control de servicios y puertos	Lista blanca de servicios imprescindibles; desactivar/desinstalar servicios innecesarios; políticas de firewall con puertos mínimos abiertos.	Administradores de Red
Gestión de cuentas/privilegios	Revisión periódica de usuarios y grupos; habilitar bloqueo de cuentas; registro de alta/baja de empleados; principio de mínimo privilegio.	Seguridad / RRHH
Cifrado de datos	Política de cifrado en reposo para servidores críticos; uso obligatorio de TLS/SSL para comunicaciones; manejo seguro de claves (cofre de claves/HSM).	Arquitectura de TI / Seguridad
Logging y monitoreo	Definir qué logs se recolectan (sistema, aplicación, red); establecer retención de logs; alertas ante eventos críticos; analizar SIEM diariamente.	Operaciones / SOC
Backups y DRP	Políticas de frecuencia (full/diferencial/incremental); almacenamiento seguro y georeplicado; pruebas de recuperación semestrales; responsabilidades claras.	Operaciones TI
Seguridad de red y perimetral	Segmentación de red por zona (producción, DMZ, admin); diseño de firewall perimetral y interno; VPN segura para accesos remotos; monitoreo de tráfico anómalo.	Arquitectura de Red
Seguridad de aplicaciones/cont.	Revisión de código/actualizaciones periódicas; imágenes de contenedores actualizadas; aislamiento de contenedores (user namespace, seccomp); WAF/IDS para apps.	Desarrollo / Seguridad
Gestión de incidentes	Definir proceso de respuesta (IRP); pruebas de simulacros; comunicación con stakeholders; informes post-incidente; enseñanza de lecciones aprendidas.	CISO / Equipo de Respuesta

Recomendaciones prácticas y hoja de ruta

A continuación se resumen pasos recomendados con prioridad estimada, para desplegar un programa de hardening de manera lógica:

Alta prioridad (rápida ejecución): Inventariar sistemas; aplicar parches pendientes; deshabilitar cuentas predeterminadas (Guest, Admin); establecer contraseñas fuertes/MFA; habilitar firewall local (deny-by-default) y cerrar puertos no esenciales; configurar logging mínimo (al menos eventos de login)[24][13].

Media prioridad: Implementar políticas de auditoría (auditd, eventos Windows); segregar redes internas (VLANs, DMZ) y restringir administración remota (por IP, VPN); desplegar SIEM o servicio EDR; eliminar servicios y características inactivos; cifrado de discos y TLS/SSL.

Baja prioridad: Afinar configuraciones avanzadas: revisiones periódicas de vulnerabilidades (pentest, escaneo), segmentación granular basada en aplicaciones, uso de contenedores hardening (CIS Docker Benchmarks), actualizar y entrenar al personal, formalizar SGSI (ISO 27001) o controles formales (NIST 800-53).

Los esfuerzos varían según la complejidad del entorno; los controles de base suelen requerir bajo esfuerzo técnico (configuración de políticas, comandos simples) mientras que las mejoras organizativas (gestión documental, certificación ISO) implican mayor esfuerzo. La curva inicial se concentra en asegurar configuraciones y parches, seguido por monitoreo y segmentación.

Ejemplos de comandos y configuraciones

Linux (systemd, iptables/nft, sshd, sudo, auditd)

systemd: Para detener y deshabilitar servicios no requeridos:

sudo systemctl stop cron.service && sudo systemctl disable cron.service

iptables/nft: Ejemplo de reglas básicas (nftables):

sudo nft add table inet filter

sudo nft add chain inet filter input { type filter hook input priority 0 \; }

sudo nft add rule inet filter input ct state { established,related } accept

sudo nft add rule inet filter input iif "lo" accept

sudo nft add rule inet filter input tcp dport 22 accept # SSH

sudo nft add rule inet filter input counter drop

sshd: En /etc/ssh/sshd_config, reforzar:

PermitRootLogin no

PasswordAuthentication no

AllowUsers adminuser

Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs hmac-sha2-256,hmac-sha2-512

Luego sudo systemctl restart sshd.

sudo: Editando con visudo, por ejemplo:

%admin ALL=(ALL) ALL

Defaults timestamp_timeout=0 # obliga a reautenticar siempre[16]

Defaults requiretty

Asegurar permisos: sudo chown root:root /etc/sudoers && sudo chmod 440 /etc/sudoers.

auditd: Instalación y regla de ejemplo:

sudo apt install auditd

sudo systemctl enable auditd && sudo systemctl start auditd

Registrar todas las llamadas exec

sudo auditctl -a exit,always -F arch=b64 -S execve -k cmd_exec

Los registros en /var/log/audit/audit.log guardarán cada comando ejecutado (pueden buscarse con ausearch -k cmd_exec).

Ejemplos de logs y alertas

Linux (sshd):

Jun 25 14:23:12 server1 sshd[2345]: Failed password for invalid user admin from 192.168.1.100 port 51324 ssh2

Jun 25 14:23:12 server1 sshd[2345]: Failed password for invalid user admin from 192.168.1.100 port 51324 ssh2

Jun 25 14:23:14 server1 sshd[2347]: Accepted publickey for john from 192.168.1.101 port 54231 ssh2: RSA SHA256:XXXXX

Un SIEM debe generar alerta ante múltiples líneas “Failed password” seguidas.

Windows (Event Viewer):

WinEvt ID 4625 (fallo de inicio de sesión):

An account failed to log on.

Subject: … Logon Type: 3 (Network) … Account For Which Logon Failed: Administrator

Source Network Address: 10.0.0.50 … Status: 0xC000006A

WinEvt ID 4768 (ticket Kerberos):

A Kerberos authentication ticket (TGT) was requested for account: DESARROLLO\usuario

Alertas típicas: múltiples 4625 de un mismo host, TGT inesperado, etc.

Diagramas de flujo

```
flowchart LR
  A[Inicio: Planificación del hardening] --> B[Inventario de sistemas y riesgos]
  B --> C[Aplicación de parches y actualizaciones]
  C --> D[Configuración segura del SO]
  D --> E[Desactivación de servicios innecesarios]
  E --> F[Configuración de firewall y segmentación]
  F --> G[Gestión de cuentas y MFA]
  G --> H[Cifrado en tránsito/reposo]
  H --> I[Logging, monitoreo y alertas]
  I --> J[Pruebas de vulnerabilidades y auditoría]
  J --> K[Mantenimiento continuo y revisión periódica]
```

```
flowchart LR
  subgraph Infraestructura
    FW[Firewall Perimetral] --> DMZ[Zona DMZ]
    DMZ --> Web[Servidor Web]
    Core[Red Interna] --> DB[Servidor BD]
    Core --> File[Servidor de Archivos]
    NTP[NTP Server] --> File
    Core --> SIEM[Servidor SIEM]
        Seg[Segmentaci\u00f3n de Red] --> |VLANs, Subredes| Core
  end
  subgraph Usuarios y Servicios
    User[Usuarios/Clientes] --> VPN[VPN/MFA]
    VPN --> Core
    Admin[Administradores] --> MFA[MFA/SSO]
    MFA --> Core
      Apps[Aplicaciones/Cotenedores] --> |Docker/K8s| Web
    Apps --> DB
  end
  SIEM --> IR[Equipo de Respuesta a Incidentes]
```

Las figuras ilustran un flujo de proceso de hardeningprogresivo y la relación entre componentes (redes segmentadas, servidores, usuarios y monitoreo). En síntesis, se planifica, se aplica un endurecimiento en capas (sistema, red, aplicaciones) y se mantiene con monitoreo continuo.

Fuentes: Las recomendaciones anteriores se apoyan en estándares de la industria y guías oficiales (por ejemplo, NIST SP 800-123[5], CIS Benchmarks[8][9], guías de Red Hat[7] y Microsoft[6], entre otras). Estos marcos y publicaciones son referenciados para fundamentar cada control descrito.

[1] [4] [5] NIST SP 800-123, Guide to General Server Security
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

[2] What is System Hardening? Essential Checklists from OS to Applications | Ubuntu
https://ubuntu.com/blog/what-is-system-hardening-definition-and-best-practices

[3] Manejo de paquetes en Linux | LabEx
https://labex.io/es/tutorials/linux-linux-package-handling-271225

[6] [23] Mantenerse al día en el software de Microsoft | Microsoft Learn
https://learn.microsoft.com/es-es/security/zero-trust/prioritizing-defense/stay-current-microsoft-software

[7] [18] 10.3. Configuración de auditd para un entorno seguro | Endurecimiento de la seguridad | Red Hat Enterprise Linux | 8 | Red Hat Documentation
https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/8/html/security_hardening/configuring-auditd-for-a-secure-environment_auditing-the-system

[8] CIS Benchmarks®
https://www.cisecurity.org/cis-benchmarks

[9] CIS Critical Security Controls
https://www.cisecurity.org/controls

[10] SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[11] Norma ISO 27001: qué es y por qué es importante
https://isotools.org/normas/riesgos-y-seguridad/iso-27001/

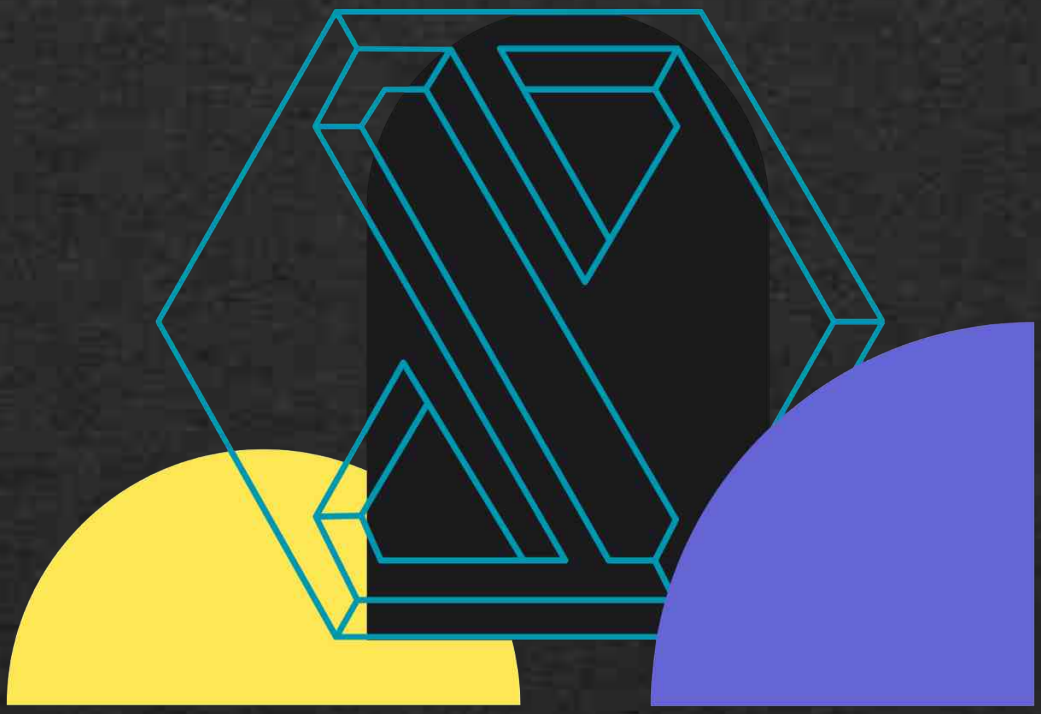
[12] [20] ¿Qué es la lista OWASP Top 10 de ciberamenazas en aplicaciones web? | Azion
https://www.azion.com/es/learning/websec/que-es-la-lista-owasp-top-10-de-ciberamenazas-en-aplicaciones-web/

[13] [14] [15] [17] [19] [24] [25] La lista de verificación completa para el endurecimiento de Windows Server | Netwrix
https://netwrix.com/es/resources/guides/windows-server-hardening-checklist/

[16] Cómo configurar correctamente el archivo sudoers | LabEx
https://labex.io/es/tutorials/nmap-how-to-configure-sudoers-file-correctly-419582

[21] [22] CIS Benchmark | Docker Docs
https://docs.docker.com/dhi/core-concepts/cis/

AFÍLIATE Y SÉ PARTE



CISCIG

ÚNETE A ESTE ESFUERZO COLECTIVO, DONDE PODRÁS COLABORAR CON OTROS PROFESIONALES PARA FORTALECER NUESTRA INDUSTRIA Y ASEGURAR QUE LAS PRÁCTICAS Y PRINCIPIOS ÉTICOS QUE SUSTENTAN NUESTRA PROFESIÓN SE MANTENGAN VIGENTES.

COELLO PÉREZ
ASESORES EN SEGUROS

40 Años Experiencia

MINIMIZA
RIESGOS,
MAXIMIZA
TRANQUILIDAD

ASESORÍA QUE ENTIENDE,
SEGUROS QUE PROTEGEN

961 171 6429
segyfia@hotmail.com

HDI sura AXA ZURICH

El control interno ha evolucionado de manera significativa en las últimas décadas, pasando de ser un mecanismo centrado en la protección de activos a constituirse como un sistema integral orientado al logro de objetivos organizacionales.

HACIA UNA CULTURA EN MATERIA DE DESEMPEÑO Y ADMINISTRACIÓN DE RIESGOS EN EL MARCO DE CONTROL DE LA ADMINISTRACIÓN PÚBLICA FEDERAL

JORGE GARCÍA ALONSO
ESPECIALISTA EN RIESGOS Y CONTROL INTERNO

1. Introducción

El control interno ha evolucionado de manera significativa en las últimas décadas, pasando de ser un mecanismo centrado en la protección de activos a constituirse como un sistema integral orientado al logro de objetivos organizacionales. En el sector público, esta evolución ha estado estrechamente vinculada a los esfuerzos por mejorar la transparencia, la rendición de cuentas y la eficiencia en el uso de los recursos públicos.

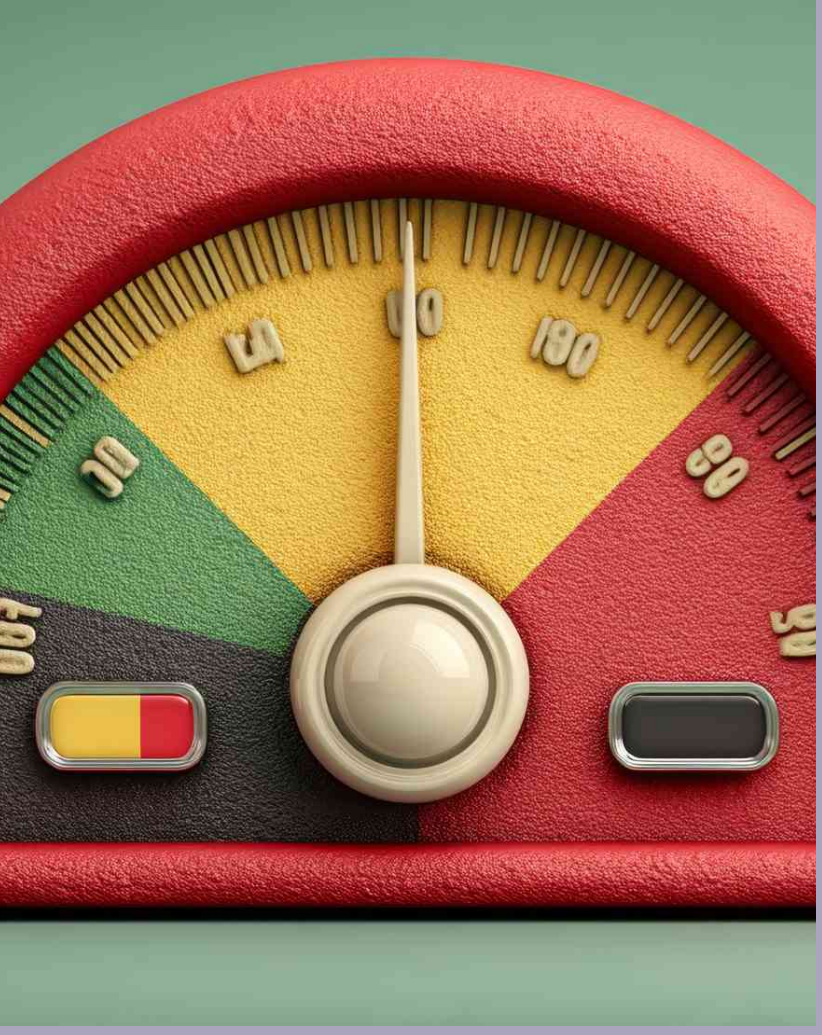
En México, las Disposiciones en Materia de Control Interno emitidas por la entonces Secretaría de la Función Pública (SFP) representan el principal marco normativo para la implementación de sistemas de control en las dependencias y entidades de la Administración Pública Federal. Estas disposiciones se basan en el modelo COSO tradicional, particularmente en su versión actualizada de 2013, la cual estructura el control interno en cinco componentes interrelacionados.

No obstante, la creciente complejidad del entorno institucional y la necesidad de orientar la gestión pública hacia resultados han puesto en evidencia las limitaciones de un enfoque centrado exclusivamente en el cumplimiento normativo. En este contexto, el marco COSO ERM 2017 introduce un cambio paradigmático al integrar la gestión de riesgos con la estrategia y el desempeño organizacional.

La transición hacia un modelo de control interno alineado con COSO 2017 plantea desafíos importantes, tanto a nivel normativo como organizacional. Entre ellos destacan la resistencia al cambio, la necesidad de capacitación y la disponibilidad de recursos.

No obstante, los beneficios potenciales son significativos), la modernización de la gestión pública requiere no solo cambios estructurales, sino también transformaciones en la forma en que se conciben y gestionan los riesgos.

En este sentido, la adopción de un enfoque integrado podría contribuir a mejorar la eficiencia, la transparencia y la capacidad de respuesta de las instituciones públicas.



La alineación a una mejor práctica internacional.

Las disposiciones emitidas por la SFP establecen un marco estructurado en torno a cinco componentes: ambiente de control, administración de riesgos, actividades de control, información y comunicación, y supervisión. Este modelo refleja una adopción directa del enfoque COSO, lo que ha permitido estandarizar prácticas y fortalecer la rendición de cuentas en la administración pública.

Sin embargo, diversos estudios han señalado que la implementación de estos sistemas en el sector público tiende a privilegiar el cumplimiento formal sobre la efectividad sustantiva, argumentando que la lógica burocrática en las organizaciones públicas puede generar incentivos para cumplir con requisitos documentales sin necesariamente mejorar el desempeño institucional.

En la práctica, la administración de riesgos suele materializarse en la elaboración de matrices que identifican riesgos y controles, pero que no siempre se vinculan con la toma de decisiones estratégicas. Esta situación limita la capacidad del control interno para influir en la asignación de recursos y en la priorización de acciones.

Asimismo, la ausencia de un marco explícito para definir el apetito de riesgo dificulta la evaluación de qué riesgos son aceptables y cuáles requieren intervención, lo que puede derivar en una gestión reactiva y poco eficiente.

Marco teórico: control interno, riesgo y desempeño

El concepto de control interno ha sido ampliamente desarrollado en la literatura académica y en los estándares internacionales. De acuerdo con COSO (2013), el control interno es un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una organización, diseñado para proporcionar una seguridad razonable en el logro de objetivos relacionados con operaciones, información y cumplimiento.

Por su parte, la gestión de riesgos empresariales (ERM, por sus siglas en inglés) amplía esta visión al incorporar la identificación, evaluación y respuesta a riesgos como parte integral de la gestión organizacional. Según COSO (2017), el ERM no es un proceso aislado, sino un conjunto de prácticas integradas que apoyan la formulación de estrategias y la mejora del desempeño.

Diversos autores han señalado que la gestión de riesgos debe diferenciar entre riesgos evitables, estratégicos y externos, y que su adecuada administración requiere mecanismos específicos que permitan su integración en la toma de decisiones. Asimismo, advierte que una gestión de riesgos excesivamente burocratizada puede perder efectividad si no se vincula con la realidad operativa de las organizaciones.

En el ámbito del sector público, organismos como la INTOSAI han enfatizado la importancia de adoptar enfoques de control interno que no solo garanticen el cumplimiento normativo, sino que también contribuyan al logro de resultados y al fortalecimiento de la gobernanza.

COSO ERM 2017: integración del riesgo con la estrategia y el desempeño

El marco COSO ERM 2017 representa una evolución significativa al proponer un enfoque basado en la integración del riesgo con la estrategia y el desempeño. Este modelo se estructura en cinco componentes: gobierno y cultura, estrategia y establecimiento de objetivos, desempeño, revisión y monitoreo, e información, comunicación y reporte (COSO, 2017).

Uno de los aportes más relevantes de este enfoque es la incorporación del concepto de apetito de riesgo, entendido como el nivel de riesgo que una organización está dispuesta a aceptar en la consecución de sus objetivos. Este concepto permite alinear las decisiones estratégicas con la tolerancia al riesgo, facilitando una gestión más coherente y eficiente.

Además, COSO 2017 enfatiza la importancia de considerar el riesgo en todas las etapas del ciclo de gestión, desde la formulación de objetivos hasta la evaluación del desempeño. Esto implica que los indicadores de desempeño deben reflejar no solo los resultados obtenidos, sino también los riesgos asumidos para alcanzarlos.

La literatura reciente ha destacado que esta integración permite a las organizaciones mejorar su resiliencia y adaptarse con mayor rapidez a cambios en el entorno.

Brechas entre el modelo mexicano y COSO 2017

El análisis comparado permite identificar diversas brechas que limitan la alineación del modelo mexicano con el enfoque COSO 2017. En primer lugar, destaca la desvinculación entre la gestión de riesgos y el desempeño institucional. Mientras que COSO propone una integración estrecha, en el modelo mexicano ambos procesos suelen desarrollarse de manera independiente.

En segundo lugar, la ausencia del concepto de apetito de riesgo impide establecer criterios claros para la toma de decisiones, lo que limita la capacidad de las organizaciones para gestionar la incertidumbre de manera estratégica.

En tercer lugar, el énfasis en el cumplimiento normativo reduce el potencial del control interno como herramienta para la generación de valor. Esta situación se ve reforzada por una cultura organizacional que tiende a percibir el riesgo como un elemento negativo, en lugar de una oportunidad para la mejora.

Finalmente, los mecanismos de monitoreo existentes suelen centrarse en la verificación de controles, sin evaluar su impacto en el logro de objetivos estratégicos.

Jorge García Alonso
Especialista en Riesgos y Control Interno

Propuestas de actualización normativa

Para cerrar estas brechas, es necesario impulsar una actualización del marco normativo que incorpore los principios del COSO 2017. En primer lugar, se requiere fortalecer la integración entre la gestión de riesgos y la planeación estratégica, de manera que el análisis de riesgos se convierta en un insumo fundamental para la toma de decisiones.

Asimismo, la incorporación del concepto de apetito de riesgo permitiría establecer límites claros para la asunción de riesgos, facilitando una gestión más eficiente y alineada con los objetivos institucionales.

Otra línea de acción consiste en reorientar el control interno hacia el desempeño, desarrollando indicadores que permitan evaluar el impacto de los riesgos en los resultados. Esto implicaría integrar la auditoría de desempeño con la gestión de riesgos, generando un enfoque más holístico.

Adicionalmente, es fundamental promover una cultura organizacional que valore la gestión de riesgos como una herramienta para la mejora continua. Esto requiere fortalecer las capacidades del personal, así como fomentar el liderazgo institucional.

Finalmente, la adopción de tecnologías de información podría facilitar el desarrollo de sistemas de monitoreo más dinámicos, capaces de proporcionar información oportuna para la toma de decisiones.

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

TITÚLATE

CON NOSOTROS

CUMPLE TUS METAS

¡TITÚLATE EN 12 MESES!

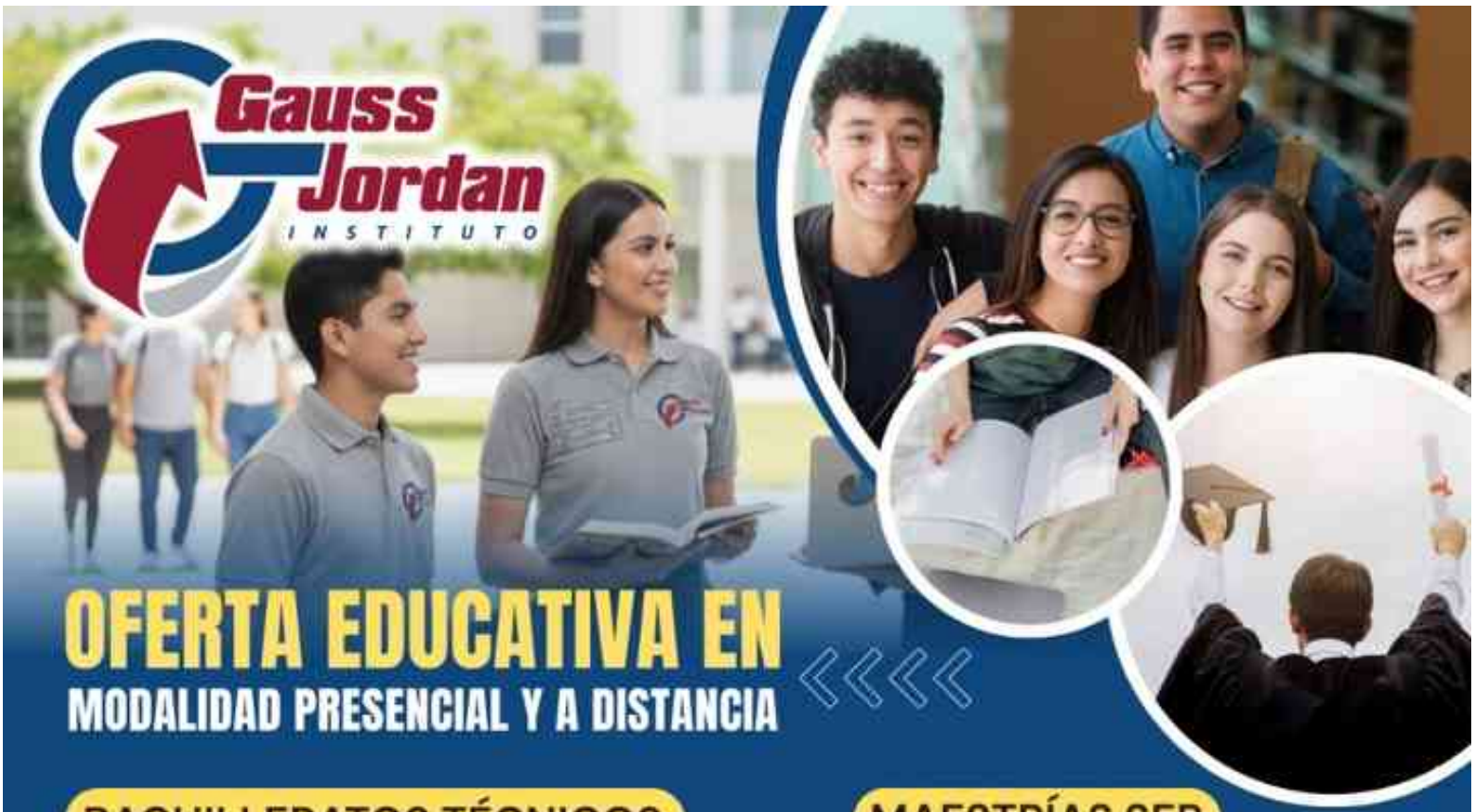
PREGUNTA POR NUESTRO PROGRAMA VIP Y TITÚLATE EN 6 MESES

RECONOCIMIENTO Y VALIDEZ OFICIAL SEP

55 3516 7586

ser vicios@ciscig.mx

www.ciscig.mx



Gauss Jordan
INSTITUTO

OFERTA EDUCATIVA EN
MODALIDAD PRESENCIAL Y A DISTANCIA

BACHILLERATOS TÉCNICOS

Turno: matutino y vespertino.

- Contaduría ((RVOE IPN NMS-0004/94)
- Informática (RVOE IPN NMS-005/94)
- Diseño Gráfico ((RVOE DGETI 2000264)
- Administración (RVOE DEGETI 2000265)

LICENCIATURAS IPN

Turno: matutino y vespertino.

- Contador Público (NS008/94)
- Ciencias de la Informática (NS014/94)

LICENCIATURAS SEP

Turno: matutino, vespertino y sabatino.

- Administración (RVOE 20254097)
- Ciencias de la Comunicación (RVOE 20081358)
- Ciencias de la Informática (RVOE 20252174)
- Contabilidad (RVOE 20252178)
- Derecho (RVOE 20241359)
- Diseño Gráico y Animación (RVOE 20241358)
- Inteligencia Artificial en la Administración
- (RVOE 20254098)
- Pedagogía (RVOE 20241360)
- Turismo (RVOE 20090884)

MAESTRÍAS SEP

Turno ejecutivo y sabatino

- Administración de las Tecnologías (RVOE 20254089)
- Derecho Procesal Civil (RVOE 20254088)
- Derecho Procesal y Juicios Orales (RVOE 20254087)
- Educación (RVOE 20252177)
- Finanzas Corporativas (RVOE 20252176)

TITULACIÓN POR ACUERDO 286 EN LAS SIGUIENTES LICENCIATURAS:

- Administración
- Ciencias de la Comunicación
- Contaduría *
- Derecho *
- Enseñanza del Inglés
- Gestión y Administración Pública
- Informática
- Ingeniería Computacional *
- Pedagogía

***Reguladas**

ADEMÁS, CONTAMOS CON:
CENTRO DE IDIOMAS, CURSOS Y DIPLOMADOS

www.gaussjordan.edu.mx
contacto@gaussjordan.edu.mx
Tels. 555537 4400 / 555537 2220
Whatsapp 55 3207 8759
Dvorak 59 Col. Vallejo
Alcaldía Gustavo A. Madero
a 2 cuadras del metrobús Robles Domínguez

LA ACTUALIZACIÓN DE LA ISO 37001

POR: CPC GUILLERMO WILLIAMS BAUTISTA, MCIE, CRMA, CFE
DR. EN CIENCIAS FORENSES

Qué es una norma ISO? Es una serie de medidas y recomendaciones que constituyen un estándar internacional sobre las mejores prácticas en torno al tratamiento de un asunto.

Una de las herramientas que considero indispensables para el conocimiento y la aplicación en materia anticorrupción -situación que atañe a el sector público y al sector privado- es precisamente el conocimiento de la norma ISO 37001 en su versión ahora actualizada 2025, dado que la misma incluye algunas directrices muy importante en cuanto al combate al fenómeno del soborno

Pero iniciemos por el principio, ¿Qué es una norma ISO?, bueno pues una norma ISO es una serie de medidas y recomendaciones que constituyen un estándar internacional sobre las mejores prácticas en torno al tratamiento de un asunto y que es desarrollado por la Organización Internacional de Normalización (ISO) que establece requisitos, directrices o especificaciones para productos, procesos o servicios.

En este sentido, en fechas recientes, la organización ISO emitió la actualización de la norma ISO 37001, la cual, en su primera versión fue la de 2016 para ahora dar lugar a la actualizada Segunda edición 2025-02, Sistemas de gestión antisoborno — Requisitos con orientación para su uso-.

Esta misma norma define el fenómeno del soborno como un fenómeno generalizado que plantea serias inquietudes sociales, morales, económicas y políticas, socava el buen gobierno, obstaculiza el desarrollo y distorsiona la competencia. Erosiona la justicia, socava los derechos humanos y es un obstáculo para el alivio de la pobreza. También aumenta el costo de hacer negocios, introduce incertidumbres en las transacciones comerciales, aumenta el costo de los bienes y servicios, disminuye la calidad de los productos y servicios, lo que puede conducir a la pérdida de vidas y bienes, destruye la confianza en las instituciones e interfiere con el funcionamiento justo y eficiente de los mercados.

Ahora bien, de conformidad con el concepto de soborno el cual indica que esto es la oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independiente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño de las obligaciones de esa persona.

Obviamente este concepto es como comentábamos antes general y la legislación del país en el que esté usted leyendo este artículo o el estado, entidad federativa o jurisdicción que resulten aplicables en ese lugar pueden tener una definición a este fenómeno que pudiera variar con la definición antes planteada, pero que sin lugar a dudas será congruente con la antes planteada.

Por su parte el Grupo de Acción Financiera Internacional afirma que, hay corrupción “Cuando una persona o un grupo de personas por acto u omisión directamente, o por influencia de alguna otra persona u organización, prometan, ofrezcan, reciban o concedan a funcionarios públicos, directivos, administradores, empleados o asesores de una sociedad, asociación o fundación pública o privada, una dadiva o cualquier beneficio (indebido) no justificado para que le favorezca a él o a un tercero, en perjuicio de aquélla.”

Por otro lado, la definición mas conocida de corrupción es la ccción y efecto de corromper o corromperse. putrefacción, descomposición, podredumbre, degeneración, fermentación.
Podríamos decir en este caso que el soborno es la acción comisiva y la corrupción es el efecto que causa (mediante el soborno realizó un acto de corrupción), y podemos también afirmar que todo acto de soborno es un acto de corrupción (el mas utilizado), pero un acto de corrupción podría ser algo que no necesariamente utilizaría el soborno para corromper, dependiendo de la cosa que se trate (corromper la mente de una persona, por ejemplo).
Por esto es tan importante que los expertos antifraude y anticorrupción estemos dotados de todas aquellas herramientas que nos auxilien en la prevención, en la detección y en la disuasión del soborno, como podría ser la ISO 37001:2025.
Volviendo entonces al tema de la actualización de la norma, se puede resaltar que en la misma, en esta nueva versión, se actualiza lo siguiente:

❖ Se añadieron apartados sobre el cambio climático
❖ Se destaca la importancia de la cultura del compliance;
❖ Se aborda de mejor manera los conflictos de interés;
❖ Se aclara el concepto de función antisoborno;
❖ Se armoniza la redacción con otras normas cuando resultó apropiado y razonable; y
❖ Se introdujo la última estructura armonizada.

En este sentido, a continuación, realizaremos algunos comentarios personales sobre estas actualización.

❖ Se añadieron apartados sobre el cambio climático

Y esto, resulta procedente y actualizado, ya que todos los actores económicos están volteando hacia una economía basada en principios de sostenibilidad, y el cambio climático es un factor trascendental en la fórmula que se impulsa a través de las organizaciones, como por ejemplo el Consejo Mexicano de Normas de Información Financiera (CINIF) quien emitió las Normas de Información de Sostenibilidad y que son obligatorias para todos aquellos que emiten estados financieros bajo las NIF, todo esto con origen y respaldo de las el Consejo de Normas Internacionales de Sostenibilidad (ISSB, por sus siglas en inglés) de la Fundación IFRS -Fundación de Estándares Internacionales de Reportes Financieros- pero además considerando que la Unión Europea viene impulsando de manera categórica una economía verde, sobre todo a partir de la emisión de bonos verdes; por su parte los gobiernos empiezan a exigir a través de tasas impositivas un saneamiento ecológico, incentivando aquellas empresas que contribuyen precisamente a un desarrollo sostenible.
Luego pues, hay que ir observando que toda esta economía no genere actos de corrupción y soborno sobre los factores que anteriormente hemos mencionado y que por supuesto debemos de entender que a la par se ha estado generando un fenómeno de “lavado de bonos verdes” por lo cual las prácticas anticorrupción y antisoborno deben de resultar adecuadas y fortalecidas, dando soporte y razón a la actualización de la norma y a la contemplación de un escenario de mejores prácticas antisoborno que incluya efectos como el cambio climático.

Con esto se busca garantizar que la cuestión de cambio climático sea considerada en el contexto de la organización e identificar si existe una parte interesada con requisitos vinculados al cambio climático.

❖ Se destaca la importancia de la cultura del compliance;

Al ser una mejor práctica mundial, la cultura del complianceinicia a su vez con un fortalecimiento de la cultura ética y de valores adecuadamente comunicados, difundidos y presentes en las prácticas de la organización y dando especial énfasis al cumplimiento legal y normativo de todas las actividades, resulta un entorno necesario para la salud operacional, financiera, legal, fiscal, laboral y por supuesto medio ambiental de los sectores público, privado y de los diferentes entes sin fines de lucro.
Esto constituye la base de resultados firmes y fidedignos en cualquier actividad y por supuesto le resulta relativa a la gestión antisoborno para lograr sus objetivos.

❖ Se aborda de mejor manera los conflictos de interés;

Promoviendo la claridad en la toma de decisiones y la administración de recursos, evitando precisamente que intereses y factores no deseables se presenten en la contratación de cualquier necesidad de la organización siendo generada por intereses particulares.
Esto requiere que la propia entidad fomente un sistema donde los empleados tengan como parte de la cultura de cumplimiento, la habilidad y el respaldo para denunciar posibles conflictos de interés y sus posibles consecuencias, asimismo, establece criterios de tratamiento de los asuntos detectados, además de la revisión constante del proceso.

De esta forma la función antisoborno resulta fortificada en esta nueva versión, e inclusive varía de su denominación original para dar mas claridad precisamente de su función.

❖ Se armoniza la redacción con otras normas cuando resultó apropiado y razonable; y

Esto a fin de que las normas entraran en una transversabilidad correcta entre las mismas y sirvieran de mejor apoyo, suplencia y aporte en áreas de especialización.

Algunas normas que se relacionan con esta ISO 37001:2025, son: ISO 9000, Sistemas de gestión de la calidad, ISO 14001, Sistemas de gestión ambiental, ISO/IEC 17000, Evaluación de la conformidad, ISO 19011, Directrices para la auditoría de los sistemas de gestión, ISO 22000, Sistemas de gestión de la inocuidad de los alimentos, ISO 26000, Guía de responsabilidad social, ISO/IEC 27001, Informationsecurity, cybersecurity and privacy protection, ISO 31000, Gestión del riesgo, ISO 31022, Risk management, ISO 37000:2021, Gobernanza de las organizaciones,ISO 37002, Sistemas de gestión de la denuncia de irregularidades,ISO/TS 37008, Investigaciones internas de las organizaciones, ISO 37009:—, Conflict of interest in organizations,ISO 37301, Sistemas de gestión del compliance.

❖ Se introdujo la última estructura armonizada

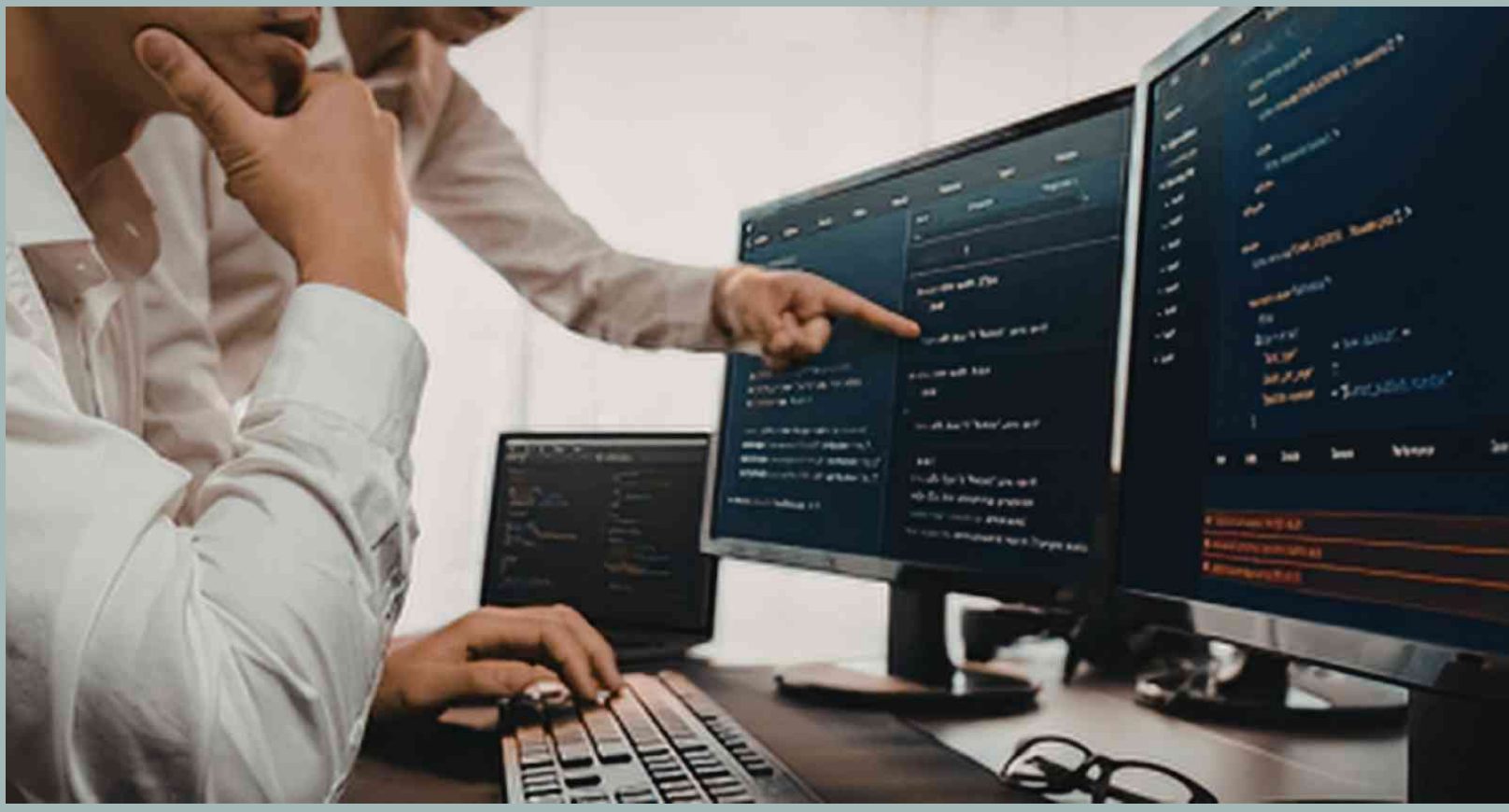
Esto busca armonizar la estructura de HLS con otros estándares. La cláusula persigue planificar los cambios que se presenten en la organización y que impacten en el SGSA.

En el contexto de la ISO, HLS significa High Level Structure (Estructura de Alto Nivel), un marco común creado por la Organización Internacional de Normalización para unificar la estructura, el texto y los términos de las normas de sistemas de gestión (como las normas ISO) y facilitar su integración en las organizaciones, utilizando un lenguaje y una estructura de 10 cláusulas similares para todos.

Y aunque este artículo en particular no busca sino establecer una alerta para los especialistas en el tema (por supuesto todos los dedicados a temas anticorrupción) sobre la necesidad de actualización de conocimientos y la valía de la emisión de esta norma, es importante señalar que esta resulta aplicable para situaciones tan complicadas, pero que pueden ser sujetas a un sistema de gestión como:

a) soborno en los sectores público, privado y sin fines de lucro;

b) soborno por parte de la organización;



c) soborno por parte del personal de la organización que actúe en nombre de la organización o para su beneficio;
d) soborno de los socios de negocios de la organización que actúen en nombre de la organización o para su beneficio;
e) soborno a la organización;
f) soborno del personal de la organización en relación con las actividades de la organización;
g) soborno de los socios de negocios de la organización en relación con las actividades de la organización;
h) soborno directo e indirecto (por ejemplo, un soborno ofrecido o aceptado a través o por un tercero)
i) entre otros tipos de soborno.

El llamado entonces es para adentrarse en el conocimiento de la norma, la utilización y la consulta a personas especializadas, siendo lo mencionado en el presente documento solo comentarios de las adiciones y mejoras realizadas, siendo un documento extenso pero de gran utilidad y que aborda precisamente las mejores normas internacionales y una preciosa oportunidad de actualización y de aplicación de estos conocimientos.

Al respecto, los ingenieros en sistemas computacionales, para la seguridad de la información, control interno y en gobernanza, tienen una oportunidad maravillosa de aportar sus conocimientos en el desarrollo, la implementación, la asesoría y la consultoría a todas esas organizaciones que necesitan precisamente esto, un sistema de gestión antisoborno, aunque esta, es solo mi humilde opinión.

POR: CPC GUILLERMO WILLIAMS BAUTISTA, MCIE, CRMA, CFE
DR. EN CIENCIAS FORENSES

REVISTA CISCIG

ANÚNCIATE CON NOSOTROS

DIFUSIÓN A NIVEL NACIONAL

Nuestra revistaen recibidaporprofesionalesdetecnología en entidades públicas, iniciativa privada e instituciones educativas

55 3516 7586 servicios@ciscig.mx www.ciscig.mx

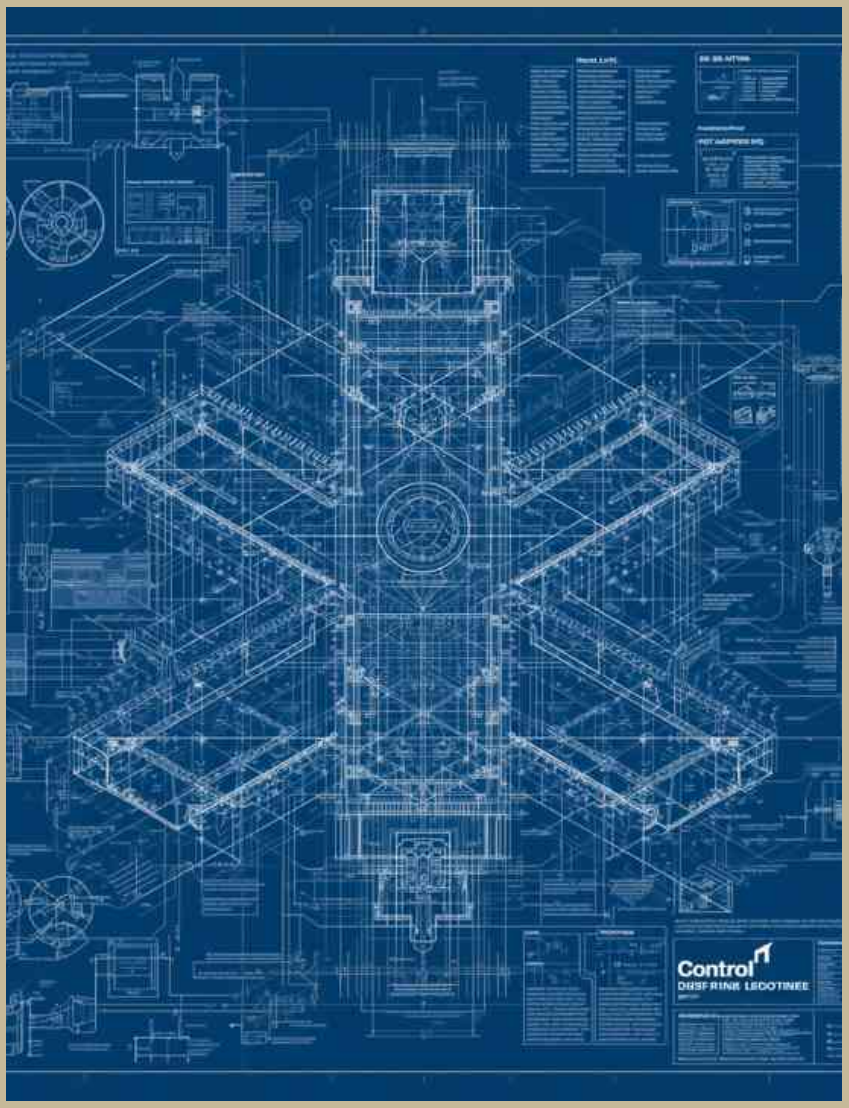
DE CONSTRUCTOR A VALIDADOR: EL ROL CRÍTICO DEL INGENIERO EN EL ASEGURAMIENTO Y GOBERNANZA DE SISTEMAS DE IA

La Inteligencia Artificial no reemplaza el juicio del profesional, lo pone a prueba. Un marco práctico para asegurar la confianza en la era algorítmica.

Introducción: La Paradoja de la IA en la Arquitectura de Control

Todos hablamos de la Inteligencia Artificial como una fuerza disruptiva, pero pocos nos detenemos a pensar qué pasa cuando el control se nos escapa de las manos, no ha llegado para hacernos el trabajo más fácil, sino para cuestionar cómo lo hemos hecho hasta ahora. En el ámbito de la auditoría y el control interno, la IA proporciona una capacidad de análisis masivo y casi en tiempo real (near-real-time), dependiendo de la escala y diseño del sistema, permitiendo detectar anomalías complejas que el muestreo manual pasaría por alto, pero aquí es donde surge la verdadera trampa: a mayor potencia, menor transparencia.

Esta misma tecnología introduce un riesgo arquitectónico profundo: el problema de la "caja negra". La falta de transparencia en algoritmos complejos dificulta la trazabilidad y la comprensión de sus resultados, minando la confianza. Frente a esto, la auditoría tradicional basada en muestreo manual resulta insuficiente. La disciplina debe evolucionar hacia una "Auditoría Algorítmica" o "Auditoría Continua", vía dashboards de monitoreo, donde el auditor tradicional adquiere capacidades de ciencia de datos para interrogar y probar al sistema en su propio idioma. La IA no sustituye el juicio humano, sino que lo aumenta.



Posicionamiento en la Arquitectura de Control

El Modelo de Tres Líneas y la Independencia del Validador

El Ingeniero Validador opera típicamente como una función de segunda línea de defensa (supervisión y riesgo), aunque en organizaciones ágiles puede integrarse como una función de calidad reforzada, siempre manteniendo independencia de decisión y veto respecto al paso a producción del modelo.

A diferencia de la auditoría interna (tercera línea, retrospectiva), el validador trabaja durante el ciclo de vida del modelo para una intervención temprana. Para ser efectiva, la independencia debe ser garantizada mediante:

• Independencia funcional: Reporte a un comité de riesgos o CRO, separado de la línea de desarrollo que construye los modelos.

• Separación de funciones: Quien valida el modelo no debe ser quien lo programó o entrenó.

• Revisión cruzada: En equipos pequeños, implementar revisiones por pares (peer reviews) obligatorias entre expertos técnicos, utilizando listas de verificación basadas en criterios objetivos (ej. NIST) para evitar sesgos de grupo.

Nota de Proporcionalidad: En organizaciones menores o startups donde segregar equipos es costoso, la falta de independencia estructural debe compensarse mediante validación externa periódica y puertas de control (gates) automatizadas antes de pasar a producción, evitando depender únicamente de la autoevaluación del desarrollador.

El Ecosistema Extendido: Auditoría Externa y Certificación

La confianza se completa con la validación por terceros, clave en sectores regulados. El rol del Ingeniero Validador es preparar a la organización para:

• Auditorías bajo ISO/IEC 42001: El estándar global para certificar el Sistema de Gestión de IA.

• Cumplimiento Regulatorio: Preparar la evidencia técnica necesaria para demostrar conformidad en sistemas de alto riesgo, alineándose con los marcos legales aplicables en cada jurisdicción (ej. EU AI Act).

Marco de Validación de IA: Tres Pilares de Aseguramiento

El aseguramiento de IA debe integrarse en el marco de control interno (COSO) y alinearse con guías técnicas como el NIST AI RMF o ISO 42001.

Pilar 1: Gobernanza Ética: Alineación, Responsabilidad y Propósito

• Alineación con el Negocio: Objetivos claros con métricas de éxito y tasas de error aceptables documentadas.

• Responsabilidad (Accountability): Se requiere una supervisión humana adecuada al nivel de riesgo: Human-in-the-Loop (autorización humana previa) para decisiones críticas como salud o crédito, o Human-on-the-loop (supervisión activa) para sistemas de alta velocidad, siempre con mecanismos de freno de emergencia y umbrales de confianza para escalar a revisión humana respetando siempre los requisitos regulatorios aplicables.

• Diseño Centrado en el Humano: Participación de usuarios no técnicos mediante Evaluaciones de Impacto Algorítmico (AIA) y pruebas de usabilidad para detectar daños no previstos por los ingenieros.

• Sostenibilidad: Medición y reporte de la huella de carbono del entrenamiento y la eficiencia energética en producción, cuando la organización cuente con capacidad de instrumentación para estas métricas.

Pilar 2: Integridad del Modelo: Calidad de Datos y Lógica Algorítmica

• Calidad y Sesgo de Datos: El validador debe auditar los datos de entrenamiento para detectar sesgos históricos o de representatividad antes de que el modelo los amplifique.

• Transparencia y Explicabilidad (XAI): Un marco robusto va más allá de herramientas básicas. Debe incluir técnicas de interpretabilidad intrínseca y, para la nueva ola de IA Generativa, controles de fidelidad y relevancia en modelos que consultan datos corporativos antes de responder (arquitectura RAG), verificando tanto la búsqueda de información correcta como la respuesta generada, para reducir las "alucinaciones" o invenciones del modelo, mejorando la comprensión de las decisiones, aunque en modelos complejos siempre se complementa con una trazabilidad detallada.

• Validez del Modelo: Evaluación estructurada para confirmar que el modelo realmente responde al problema de negocio y que su desempeño es consistente en el tiempo

.

Pilar 3: Seguridad Operacional: Resistencia y Trazabilidad

• Seguridad del Modelo y la Infraestructura:Implementar controles que protejan tanto el servidor como el propio algoritmo o "cerebro" de la IA (el modeloo), incluyendo evaluaciones de resistencia ante la manipulación de instrucciones (Prompt Injection), especialmente en asistentes virtuales y sistemas basados en texto, integrando estas pruebas en cada actualización del sistema.

• Resistencia a Ataques Adversariales: Garantizar que el sistema resista intentos de manipulación de datos (data poisoning) diseñados para engañarlo.

• Monitoreo Continuo: Detectar la degradación del modelo diferenciando claramente entre Data Drift(cambios en los datos de entrada) y Concept Drift(cambios en la relación de las variables con la realidad del entorno), priorizando alertas accionables dado que requieren soluciones distintas.

• Trazabilidad (Auditable): Mantener registros (logs) inmutables de las decisiones y documentación estandarizada del modelo (por ejemplo, Model Cards) que describan su propósito y limitaciones.

Casos Prácticos del Ingeniero Validador

El rol del Ingeniero Validador se manifiesta en la supervisión de controles técnicos avanzados:

Escenario 1: Seguridad – Robustez en Modelos de Fraude

En una entidad financiera, el validador verifica que el modelo no solo detecte fraudes conocidos, sino que sea robusto ante ataques nuevos. Coordina o verifica la ejecución de pruebas de estrés (Red Teaming) para confirmar su resistencia a intentos de evasión y asegura que existan reglas de respaldo cuando la incertidumbre del modelo es alta.

Beneficio: Evitar pérdidas millonarias y ataques sofisticados.

Escenario 2: Control Interno – Mitigación de Sesgo en Algoritmos de Crédito

Para evitar discriminación, el validador audita los datos históricos y el algoritmo antes de pasar a producción. Verifica la implementación de controles de equidad y supervisa que las tasas de aprobación sean justas entre diferentes grupos demográficos.

Beneficio: Garantizar decisiones justas y evitar sanciones regulatorias.

Escenario 3: Gobernanza – Explicabilidad ante Reguladores

Ante la opacidad de la "caja negra", el validador revisa que se utilicen técnicas de IA Explicable (XAI) para transformar decisiones matemáticas en documentación legible. Su rol es asegurar que, ante un cuestionamiento, la organización pueda rastrear y justificar por qué el modelo tomó una decisión específica.

Beneficio: Demostrar transparencia y evitar multas.

Conclusión: Liderazgo Ingenieril para la IA Confiable

En última instancia, la IA no es un destino inminente, sino un proceso que ya nos está rebasando, representa un cambio fundamental que introduce riesgos únicos. El rol del Ingeniero Validador es la respuesta crítica a esta disrupción. Al integrar el conocimiento técnico con los marcos de gobernanza, este profesional asegura que la IA sea funcional, justa y responsable, no podemos permitir que la eficiencia opaque la transparencia..

Hacemos un llamado a la acción. Hagamos estas preguntas:
¿Quién es responsable si nuestra IA comete un error crítico?
¿Podemos explicarle a un regulador cómo funciona nuestro modelo?
¿Estamos protegidos contra la manipulación de nuestros algoritmos?
Para responderlas, sugerimos esta hoja de ruta:
1. Inventariar ("Shadow AI"): Rastrear y listar todos los modelos que la organización ya está utilizando (cuando sea viable, análisis de logs de red para detectar uso no autorizado de APIs externas).
2. Clasificar (Matriz de Riesgo): Separar lo crítico de lo trivial. Identificar los modelos de Alto Riesgo (impacto en derechos, salud o dinero) que requieren validación profunda.
3. Asignar (Accountability): Definir un propietario técnico (mantenimiento) y un propietario de negocio (responsable del resultado) para cada algoritmo.
Nota: El tiempo de implementación variará según la madurez tecnológica de cada organización, desde semanas para un inventario básico hasta meses para una validación profunda.
Al asegurar la transparencia en el núcleo algorítmico, no solo auditaremos el futuro, sino que ayudaremos a construir uno en el que se pueda confiar.

Raul René Arévalo Villar/Especialista de Control Interno de TI

C I S C I G

Comprometidos con la excelencia, la innovación y la ética en nuestra profesión.

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

+52 55 6736 9071
+ 52 55 3516 7586
+52 55 6502 1522

servicios@ciscig.mx

www.ciscig.mx