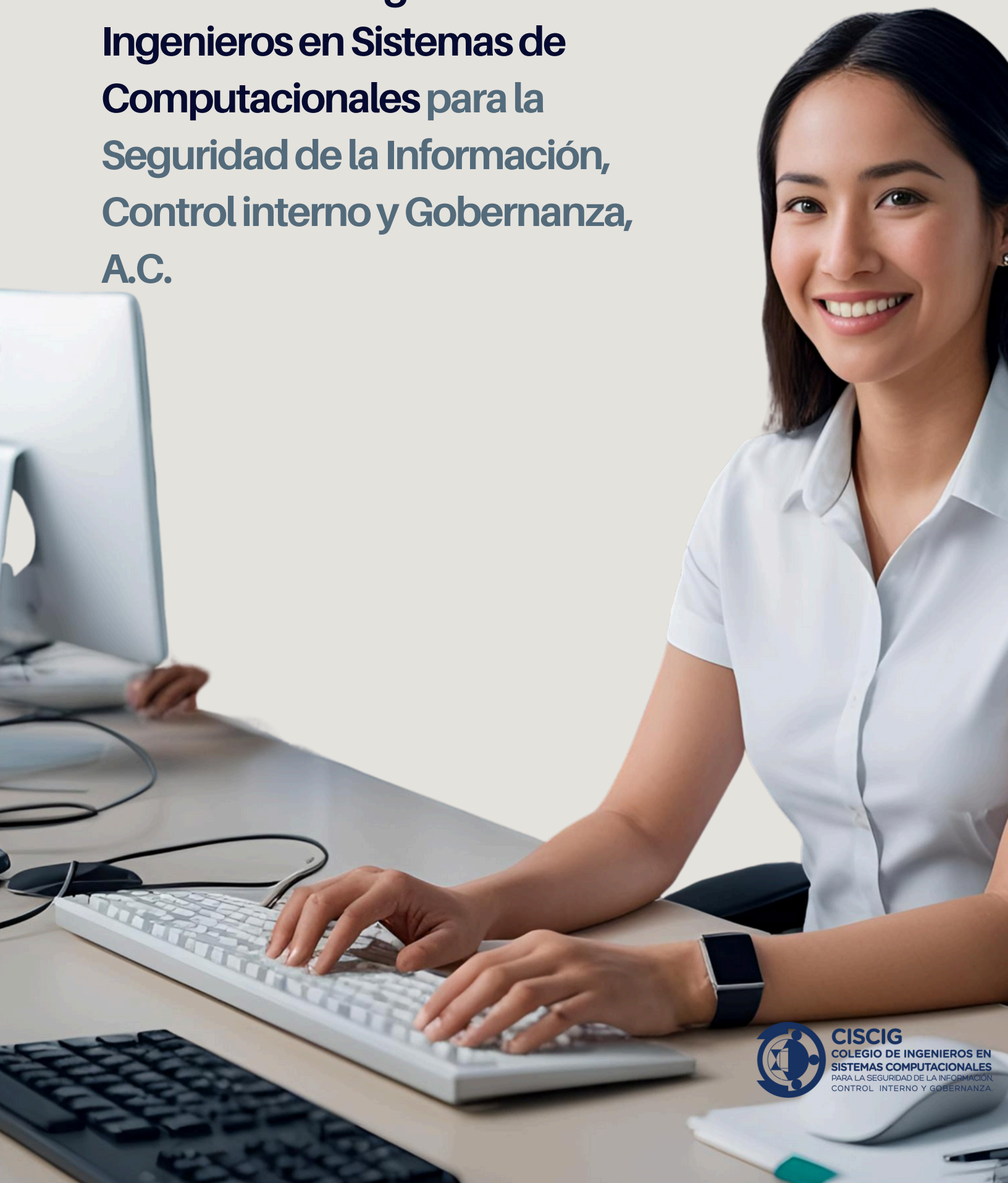
Diciembre 2024

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

CONTENIDO

WhatsApp:

+52 55 6736 9071

+ 52 55 3516 7586

+52 55 6502 1522

servicios@ciscig.mx

www.ciscig.mx

Número ISSN: 2992-7250- Año II, volumen VII, Diciembre 2024

REVISTA DEL COLEGIO DE INGENIEROS EN SISTEMAS DE COMPUTACIONALES PARA LA SEGURIDAD DE LA INFORMACIÓN , CONTROL INTERNO Y GOBERNANZA, A.C, año 2, No. 7, diciembre 2024, es una publicación trimestral editada por el Colegio de Ingenieros en Sistemas de Computacionales para la Seguridad de la Información Control Interno y Gobernanza, A.C. (CISCIG), Calle Parral # 6, Colonia Condesa, Alcaldía Cuauhtémoc, C.P. 06140, Ciudad de México, Tel (55) 3516 7586, www.ciscig.mx, jorge.garcia@marcg.com.mx Editor y responsable de la última actualización de este Número Armando Avalos Pérez, Calle Parral # 6, Colonia Condesa , Alcaldía Cuauhtémoc , C.P. 06140 , Ciudad de México armando.avalos@marcg.com.mx Reserva de Derechos al Uso Exclusivo No. 04-2023- 033115290800-102, ISBN: 2992-7250, ambos otorgados por el Instituto Nacional de Derecho de Autor, fecha de última actualización, 31 de diciembre de 2024.

CONOCE NUESTRA REVISTA

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.

Por Joaquín Ortiz

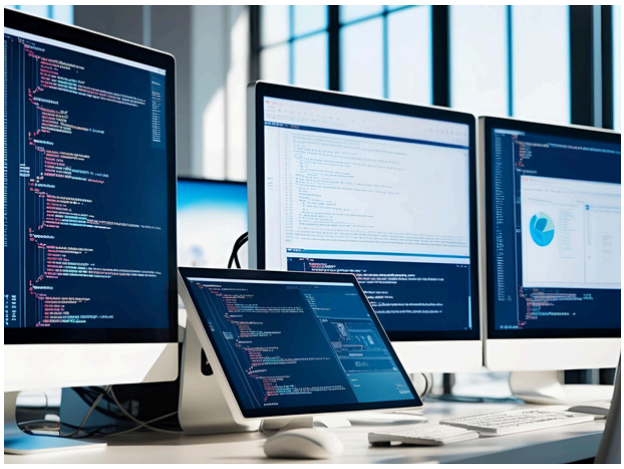
Riesgos y Controles de TI

INTRODUCCIÓN

En el entorno actual, donde la tecnología es un pilar fundamental para el éxito de las organizaciones, la gestión de riesgos de TI se ha convertido en un aspecto crítico para garantizar la seguridad, la continuidad del negocio y el cumplimiento normativo. Los riesgos de TI no solo se refieren a amenazas cibernéticas, sino también a fallos en sistemas, errores humanos, deficiencias en la infraestructura y problemas relacionados con la gestión de datos. Para mitigar estos riesgos, las organizaciones deben implementar controles de TI que aseguren la protección de los activos tecnológicos y la integridad de la información. Los auditores de TI desempeñan un papel clave en la evaluación de estos controles, identificando debilidades y recomendando mejoras.

IMPORTANCIA EN LA AUDITORÍA DE TI

- Comprender los riesgos y controles relacionados con TI es esencial para cualquier auditor, ya que permite:
- Evaluar la Eficacia de los Controles: Identificar si los controles existentes son adecuados para mitigar los riesgos identificados.
- Adoptar un Enfoque Basado en Riesgos: Priorizar los esfuerzos de auditoría en aquellas áreas que presentan mayor exposición al riesgo.
- Asegurar el Cumplimiento Normativo: Verificar que la organización cumple con regulaciones como SOX, PCI-DSS, ISO 27001, entre otras.
- Proteger Activos Críticos: Garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas de la organización.



El Instituto de Auditores Internos (IIA) y ISACA promueven el enfoque basado en riesgos como una práctica fundamental para la auditoría de TI, lo que implica comprender no solo los riesgos inherentes de la tecnología, sino también cómo se gestionan a través de controles eficaces.

ARQUITECTURA DE RIESGOS Y CONTROLES DE TI

La gestión de riesgos de TI se basa en identificar, evaluar y mitigar los riesgos que podrían afectar la capacidad de la organización para alcanzar sus objetivos. Para ello, se implementan controles que actúan como salvaguardas frente a estos riesgos.

PRINCIPALES CATEGORÍAS DE RIESGOS DE TI

Categoría de Riesgo	Descripción	Ejemplos Comunes
Riesgos de Seguridad de la Información	Amenazas a la confidencialidad, integridad y disponibilidad de la información.	Ciberataques, malware, fugas de datos.
Riesgos Operacionales	Fallos en procesos, sistemas o infraestructura tecnológica.	Caídas de servidores, errores en la configuración, fallos en la red.
Riesgos de Cumplimiento	Incumplimiento de leyes, regulaciones o políticas internas.	Violaciones de GDPR, PCIDSS o SOX.
Riesgos de Disponibilidad	Interrupciones que afectan la continuidad de los servicios de TI.	Fallos en la recuperación ante desastres, ataques DDoS.
Riesgos de Terceros (Proveedor/TI Externa)	Dependencia de proveedores de servicios externos que pueden afectar la operación de TI.	Fallos en servicios en la nube, vulnerabilidades en proveedores críticos.
Riesgos de Desarrollo de Software	Deficiencias en el ciclo de vida del desarrollo de aplicaciones.	Código vulnerable, falta de pruebas de seguridad.

TIPOS DE CONTROLES DE TI

Los controles de TI se diseñan para mitigar riesgos específicos y garantizar el funcionamiento seguro de los sistemas. Se clasifican en varias categorías, según su naturaleza y propósito:

Tipo de Control	Propósito	Ejemplos
Controles Preventivos	Evitar que ocurran incidentes o fallos	Firewalls, autenticación multifactor (MFA), políticas de seguridad.
Controles Detectivos	Identificar incidentes o anomalías después de que ocurren.	Sistemas de detección de intrusiones (IDS), monitoreo de logs, alertas de seguridad.
Controles Correctivos	Corregir problemas detectados y restaurar operaciones normales.	Planes de recuperación ante desastres (DRP), parches de seguridad, procedimientos de respuesta a incidentes.
Controles Físicos	Proteger el acceso físico a los Control de acceso a centros de datos, activos de TI.	Control de acceso a centros de datos, cámaras de vigilancia, cerraduras electrónicas
Controles Lógicos o Técnicos	Proteger los sistemas y la información mediante soluciones tecnológicas.	Criptografía, sistemas de gestión de identidades (IAM), configuraciones seguras de red.
Controles Administrativos	Definir políticas, procedimientos y normas para gestionar la seguridad de TI.	Programas de concientización en seguridad, segregación de funciones, auditorías internas.

Estos controles se complementan entre sí para proporcionar un enfoque integral de seguridad y gestión de riesgos.

EVALUACIÓN DE RIESGOS Y CONTROLES EN LA AUDITORÍA DE TI

El proceso de auditoría de TI basado en riesgos implica varias etapas que permiten identificar, analizar y evaluar los controles implementados por la organización.

Proceso de Evaluación de Riesgos de TI

1. Identificación de Riesgos:
   - Analizar los activos de TI críticos (sistemas, aplicaciones, infraestructura, datos).
   - Identificar amenazas internas y externas, vulnerabilidades y posibles escenarios de riesgo.

2. Evaluación de Riesgos:
   - Determinar la probabilidad de que ocurra un evento de riesgo y su impacto potencial en la organización.
   - Utilizar metodologías de análisis de riesgos como ISO 31000 o NIST Risk Management Framework (RMF).

3. Priorización de Riesgos:
   - Clasificar los riesgos en función de su severidad para enfocar los recursos de auditoría en las áreas de mayor impacto.

4. Análisis de Controles Existentes:
   - Evaluar si los controles implementados son eficaces para mitigar los riesgos identificados.
   - Realizar pruebas de controles para verificar su diseño y efectividad operativa.

5. Informe de Resultados:
   - Documentar los hallazgos, incluyendo deficiencias en controles, vulnerabilidades críticas y recomendaciones para la mejora continua

BUENAS PRÁCTICAS EN LA GESTIÓN DE RIESGOS Y CONTROLES DE TI

Implementar buenas prácticas en la gestión de riesgos y controles de TI contribuye a fortalecer la postura de seguridad de la organización y a mejorar su resiliencia frente a amenazas.

- Enfoque Basado en Riesgos (Risk-Based Approach):

Priorizar la gestión de riesgos críticos que podrían afectar la continuidad del negocio o la seguridad de la información.

- Segregación de Funciones (SoD):

Evitar conflictos de interés y reducir el riesgo de fraudes mediante la separación de funciones clave en los procesos de TI.

- Revisión y Actualización Periódica de Controles:

Los controles deben revisarse y actualizarse regularmente para adaptarse a nuevos riesgos, cambios en la tecnología y en el entorno regulatorio.

- Cultura de Seguridad:

Fomentar la concienciación en seguridad entre los empleados a través de programas de capacitación y simulaciones de ciberseguridad.

- Pruebas de Controles y Auditorías Internas Regulares: Realizar auditorías continuas y pruebas de penetración para evaluar la efectividad de los controles de seguridad.

- Gestión de Incidentes y Respuesta Rápida: Establecer procedimientos claros para la detección, análisis, contención y recuperación de incidentes de seguridad.

MATRIZ DE RIESGOS DE TI Y CONTROLES DE MITIGACIÓN

A continuación se presenta una matriz que asocia los riesgos comunes en TI con los controles recomendados para su mitigación:

Riesgo de TI	Impacto Potencial	Controles de Mitigación
Acceso no autorizado a sistemas críticos	Pérdida de datos sensibles, fraude	Control de acceso basado en roles (RBAC), autenticación multifactor (MFA)
Ataques de malware o ransomware	Pérdida de datos, interrupción de servicios	Antivirus actualizado, filtrado de contenido, capacitación en ciberseguridad
Fallo en la infraestructura de TI	Interrupción del negocio	Redundancia de sistemas, monitoreo continuo, planes de continuidad (BCP)
Errores en la gestión de cambios	Fallos en sistemas en producción	Procedimientos formales de gestión de cambios, revisiones de seguridad
Incumplimiento normativo (SOX, GDPR, etc.)	Sanciones legales, daños reputacionales	Programas de cumplimiento, auditorías regulares, gestión de riesgos de TI
Fugas de información confidencial	Daño reputacional, impacto financiero	Cifrado de datos, DLP (Data Loss Prevention), monitoreo de tráfico de red
Vulnerabilidades en aplicaciones web	Exposición a ciberataques	Pruebas de seguridad en el ciclo de desarrollo (DevSecOps), análisis de código estático

CASO PRÁCTICO: EVALUACIÓN DE RIESGOS Y CONTROLES EN UNA EMPRESA DE COMERCIO ELECTRÓNICO

Escenario:
Una empresa de comercio electrónico ha experimentado intentos de acceso no autorizado a su plataforma, así como incidentes de disponibilidad durante campañas de alto tráfico. Se solicita una auditoría para evaluar los riesgos de TI y la eficacia de los controles existentes.

MATRIZ DE EVALUACIÓN DE LA AUDITORÍA

Área Evaluada	Riesgo Identificado	Hallazgos Clave	Recomendaciones
Gestión de Accesos	Acceso no autorizado a cuentas de usuarios	Uso limitado de autenticación multifactor (MFA)	Implementar MFA en todas las cuentas críticas
Disponibilidad del servicio	Caídas del sitio durante picos de tráfico	Falta de pruebas de estrés en la infraestructura	Realizar pruebas decarga y escalar recursos en la nube según demanda
Seguridad de la Información	Exposición de datos sensibles debido a vulnerabilidades web	Falta de pruebas regulares de seguridad en aplicaciones web	Integrar pruebas de seguridad en el ciclo de vida del software (DevSecOps)
Gestión de Incidentes	Tiempos de respuesta lentos ante incidentes críticos	Ausencia de un plan formal de respuesta a incidentes de seguridad	Desarrollar y probar un plan de respuesta a incidentes de ciberseguridad

IMPACTO DE LA AUDITORÍA:

- Mejora significativa en la seguridad de las cuentas de usuario. Mayor resiliencia del sitio web ante picos de demanda.
- Reducción en los tiempos de respuesta ante incidentes críticos.

CONCLUSIÓN

La gestión de riesgos y controles relacionados con TI es un pilar fundamental para la seguridad, la continuidad del negocio y el cumplimiento normativo. Los auditores de TI deben comprender no solo los riesgos inherentes a la tecnología, sino también cómo evaluarlos y verificar la eficacia de los controles implementados. Aplicar un enfoque basado en riesgos, junto con buenas prácticas y marcos de referencia internacionales como COBIT, ISO 27001 e ITIL, permite fortalecer la resiliencia tecnológica y proteger los activos críticos de la organización.

Cuando la realidad supera la ficción.

Por Jedidia Ortiz

La fragilidad global ante la potencia del internet, la dependencia más inminente que no todos vimos venir, o que tal vez no quisimos.

El pasado 2023, en una plataforma de streaming bastante conocida, cerramos el año con la película “Dejando el mundo atrás” un thriller psicológico de tinte apocalíptico que, a diferencia de otros fines del mundo que el cine nos ha regalado, este describe uno más incómodo puesto que se trata de algo muy tangible para todos, hablamos del colapso del internet o las redes tecnológicas.

La película se basa en obras de los novelistas estadounidenses Don DeLillio y Rumaan Alam llamadas “El silencio” y “Dejar el mundo atrás”, sin embargo, un año antes llegó “Error 404: ¿Preparados para un mundo sin internet? una obra escrita por Esther Paniagua, una reconocida periodista española especializada en ciencia y tecnología y directora de la revista OpenMind... El libro plantea una exploración intrigante sobre la posibilidad de enfrentarnos a un mundo en el que la conexión a la internet ya no esté disponible, desatando el caos y el pánico a nivel mundial. De acuerdo con ella “ni los gobiernos ni los Estados están preparados para enfrentar el escenario apocalíptico que podría seguir a tal eventualidad” (Didyme, A, Rolling Stone).

Dicho filme remarca la confusión y caos de un par de familias que luchan por comprender la falta de comunicación y señal mientras presencian un avión caer, un barco que no se detiene, animales salvajes cambiar de ambiente, dispositivos electrónicos sin funcionar, rumores de conspiraciones y guerras entre naciones y un silencio por parte de los gobiernos que resulta ensordecedor, todo, mientras nos espejean una sociedad absurda abarrotada en intereses propios que ya no sabe hacer mucho si al botón tecnológico lo ponen en pausa o, lo lidera alguien que no conocemos.

La ficción que relata es interesante, algunos solo hablaron de las actuaciones y, si bien fue popular una temporada, nadie creyó que la realidad nos diera una probada de lo que solo parecía ser una película más.

El pasado 19 de julio, el mundo tuvo unas horas de colapso ante la caída informática de Microsoft, empresas, bancos, aeropuertos, hoteles, escuelas, administraciones públicas, medios de comunicación y servicios de emergencia se vieron terriblemente afectados ante lo que algunos llaman “el mayor apagón informático que la historia ha visto”, lo anterior, al parecer fue resultado de fallos en la nube, una inoportuna actualización de software para sistemas operativos Microsoft Windows por la empresa de ciberseguridad CrowdStrike; y por “picos repentinos de incidencias en múltiples sitios web que utilizan aplicaciones de Microsoft desde la noche anterior” (Maturana, J, 2024, Euronews).

El daño requirió trabajos manuales urgentes, no obstante, se estimó que las secuelas perduren un tiempo antes de retomar su curso normal, aunque la toma de responsabilidades y temas jurídicos son un punto y aparte muy pendientes a esclarecer todavía.

Un apagón que encendió el terror del mundo, caos a escala, cancelaciones y retrasos, instituciones y servicios detenidos, la seguridad nacional amenazada por ciberdelincuencia, y una horda de pantallas azules que sólo dice error… eso supera cualquier escena de ficción.

En conclusión, considero que comprobamos tres cuestiones.

1. Nuestro sustento en el ámbito informático puede ser también nuestra debilidad.
2. No estamos preparados para reaccionar a una realidad sin internet o tecnología en nuestros tiempos.
3. La ficción cada vez, es más nuestra realidad.

Tal vez este no sea nuestro fin del mundo preferido.

Fuentes:
Didyme, A. (s.f.). Crítica: Dejar el mundo atrás. RollingStone.https://es.rollingstone.com/critica-dejar-el-mundo-atras/

Maturana, J. (2019). Caos informático mundial por la caída de los servicios de Microsoft que incluso ha provocado la cancelación de vuelos. Euronews. https://es.euronews.com/next/2024/07/19/caos-informatico-mundial-por-la-caida-de-los-servicios-de-microsoft-que-incluso-ha-provoca

Por Omar D. Alonzo Rodríguez

REDES 6G (Innovación tecnológica)

Desde el surgimiento de la tecnología 5G, el mundo de las comunicaciones ha cambiado de manera significativa, especialmente por el aumento de velocidad que esta tecnología celular inalámbrica pudo proporcionar. Sin embargo, a pesar de ser una conectividad aún no expandida en la mayor parte del mundo, ya se habla de la próxima conexión 6G, especialmente en China donde se iniciará un proyecto piloto en 2026.

Cabe destacar que, tras un aumento global del 76% en la adopción de 5G entre 2021 y 2022, alcanzando a 1.05 mil millones de personas según datos de Omnia y 5G Américas, se proyecta que la cifra llegue a 5.9 mil millones para 2027. Así, la conectividad 6G se posiciona ya como una realidad inminente. Para 2030, se espera que la 6G conecte más de 500.000 millones de dispositivos en todo el mundo, según Ericsson.

Aunque la adopción generalizada de la tecnología 6G aún se encuentra a varios años de distancia, los esfuerzos realizados en 2025 establecerán las bases para un futuro más interconectado e innovador.

¿QUÉ ES LA TECNOLOGÍA 6G?

El 6G se refiere a la sexta generación de tecnología inalámbrica y comunicaciones móviles. Aunque todavía se encuentra en etapas tempranas de desarrollo, se espera que proporcione avances importantes en términos de velocidad, capacidad, latencia y confiabilidad en comparación con el 4G y 5G.

El 6G traerá consigo ventajas en diferentes sectores de la industria y la economía, como la medicina y la automoción. Hay varios campos que serán potenciados claramente con esta nueva generación de redes: la realidad extendida y las comunicaciones holográficas; la inteligencia artificial, automatizada e interconectada; y la eficiencia energética, que se situará en niveles de consumo ultra bajos.

Las empresas deben actuar de forma proactiva, aprovechando herramientas como el procesamiento inteligente de documentos para agilizar los flujos de trabajo y adoptando tecnologías sostenibles para alinearse con los objetivos medioambientales globales. Mientras que la IA y la conectividad sigan evolucionando, las posibilidades de innovación serán ilimitadas.

Se prevé que el crecimiento de las redes 6G abra paso al perfeccionamiento de las aplicaciones y tecnologías que tenemos ahora mismo.

Gracias al poder de descarga de hasta 100 Gb/s, la visualización de contenido 8K será rutinario, y la experiencia de la realidad aumentada será cada vez más accesible.

Por otro lado, gracias a latencias inexistentes, los avances médicos como la cirugía remota y el control preciso de maquinaria permitirán avances nunca antes vistos.

Además, la capacidad de conectar millones de dispositivos por kilómetro cuadrado, impulsará el crecimiento del Internet de las Cosas, facilitando el surgimiento de hogares inteligentes, vehículos autónomos y sistemas de monitoreo en tiempo real.

Esto abre camino a unas innovaciones tecnologías sin límites, fomentando la creación y adopción de aplicaciones que aún no conocemos.

Sectores como la sanidad están comenzando a aprovechar las posibilidades que ofrece el 6G para realizar cirugías a distancia, lo que permitirá a los médicos operar a pacientes en tiempo real, sin importar su ubicación física. A continuación, se detallan algunas de las innovaciones que podemos anticipar:

- Experiencias digitales inmersivas: Gracias al 6G, se mejorarán los entornos de realidad aumentada y realidad virtual, ofreciendo simulaciones más realistas para juegos, capacitación y educación.

- Ciudades inteligentes: La conectividad avanzada permitirá una gestión más eficiente del tráfico en tiempo real, optimizando el uso de la energía y apoyando iniciativas de seguridad pública.

- Exploración espacial: La tecnología 6G podría abrir la puerta a sistemas de comunicación más sofisticados para misiones espaciales, incluyendo la exploración de Marte.

Recursos y tecnologías de las redes 6G

Aunque es complicado ofrecer una lista completa, a continuación, se presentan algunas de las tecnologías y recursos anticipados para la conectividad 6G:

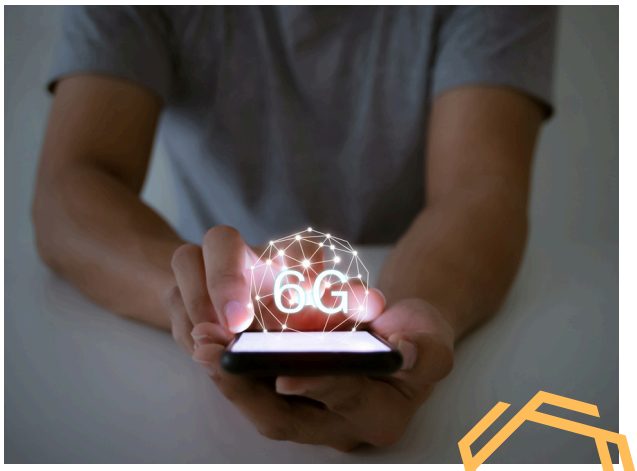
- Redes neuronales y aprendizaje automático: La integración de redes neuronales y algoritmos de aprendizaje automático permitirá gestionar la red de forma más eficiente e inteligente, adaptándose dinámicamente a diversas condiciones de uso.

- Frecuencias y mayor ancho de banda: Se prevé que 6G opere en frecuencias superiores a las de 5G, lo que permitirá alcanzar velocidades de datos más rápidas y mejorar las capacidades de transmisión.

- Terahercios (THz) y ondas milimétricas: La utilización de frecuencias en la banda de los terahercios proporcionará un ancho de banda excepcionalmente amplio y capacidades de transmisión sobresalientes.

- Comunicación de terabit: Se espera que 6G contemple comunicaciones a nivel de terabit, llevando la velocidad y la capacidad de datos a nuevos límites.

- Comunicación máquina a máquina avanzada: La conectividad 6G se enfocará en optimizar la comunicación entre dispositivos y sistemas, permitiendo aplicaciones más complejas dentro de la Internet de las Cosas y la automatización industrial.



- Computación cuántica: La computación cuántica tiene el potencial de mejorar significativamente la capacidad de procesamiento y análisis de datos, facilitando el desarrollo de aplicaciones más avanzadas en la red 6G.

- Holografía y realidad extendida: Se anticipa un notable avance en las capacidades de holografía y realidad extendida, lo que brindará experiencias más realistas e inmersivas en áreas como videoconferencias y entretenimiento.

- Integración de redes satelitales y terrestres: Las redes 6G podrían fusionar las comunicaciones terrestres con las satelitales, garantizando una cobertura global y una conectividad más fiable en áreas remotas.

DEDICADOS A CERTIFICAR AL SECTOR, PROMOVER LAS MEJORES PRÁCTICAS EN LA INDUSTRIA, EMITIR DICTÁMENES Y DEFENDER LOS INTERESES DE NUESTROS COLEGIADOS.

OBTEN CON NOSOTROS:

- Acompañamiento
- Capacitación
- Programas de calidad
- Constante actualización
- Networking

LO BUENO Y LO MALO DE LA TECNOLOGÍA

Todo me es lícito, pero no todo conviene; todo me es lícito, pero no todo edifica.
Pablo.

Por Mtro. Joaquín Ortiz Urióstegui

Con la cita de Pablo expongo que podría ser que, en mi vida académica, cotidiana, escolar, necesito realizar un análisis sobre todo lo que reciben mis sentidos, emociones, sentimientos, sobre todo en esta época estamos bajo un contexto de avances tecnológico de manera acelerada.

A través de la historia podemos observar cómo la influencia de la tecnología ha tenido muchos beneficios en todas las esferas de la humanidad para el bienestar, agilizar y mejorar comodidades de la vida diaria, laboral, médica, educativa, entre otras áreas.

La narrativa de la humanidad ha presentado todo tipo de avances con la finalidad de ser más prácticos para comunicarnos, el producir bienes y servicios, transformar nuestro entorno natural, y la meta es hacer de la vida de la humanidad más fácil, placentera y feliz.

Por medio del registro de la historia humana, todo avance técnico tiene la óptica de satisfacer las necesidades básicas de los seres humanos.

El hombre tuvo que crear sus propias herramientas en la época de la prehistoria como las piedras de corte para obtener y la preparación de sus alimentos para la subsistencia que se necesitaba en ese periodo, así como el descubrimiento del fuego, elemento sustantivo en su momento, y hoy en día de total importancia de su utilidad.

Con la llegada de la Revolución Industrial en Inglaterra se presenta un cambio, avance en el marco de la tecnología, recordemos que para que sea una Revolución, bajo este contexto debe alcanzar varios escenario que impacte para ser llamada como lo cité anteriormente: el ahorro del tiempo , la economía, el bien común y social, así como el no regresar al pasado[1]. Provocando ese impacto en los diferentes sectores, así como subrayando en el ámbito agrícola, sobresaliendo el uso de maquinaria para la fabricación industrial, todo eso era muy bueno como primer impacto europeo, así como posteriormente los países anglosajones.

[1] Boletín de la Academia Malagueña de Ciencias.

Con este tópico, los avances en las cuestiones domésticas sería un gran avance, básicamente para las amas de casa y familia. La electricidad sería otro elemento sustantivo para el desarrollo humano.

Los griegos como toda tradición de conocimiento, aportaron ideas en todas las esferas de las ciencias, tecnología, artes y más, pero en sus avances también ponen en cuestión qué tan provechoso puede ser las aportaciones para el beneficio del hombre , puede verse en los diálogos de Platón en específico El Fedro, así como dice el filósofo griego … no sólo podía afectar las capacidades cognitivas del ser humano, en especial la memoria[1].

[1] Munoz Iturrieta,Pablo.(2023). Apaga el Celular y Enciende tu Cerebro, p.21.

Para cerrar el presente escrito diremos que todo exceso en la vida trae complicaciones, todo abuso por muy sano que sea, puede acarrear adversidades, no obstante, en la historia de la tecnología, vemos todas las bondades para el desarrollo de la humanidad, los beneficios en las diferentes áreas nos permiten facilitar nuestra vida y relaciones personales e interpersonales.

.

La propuesta de este artículo es tener cuidado de mis redes sociales, su contenido y evitar toda manipulación y control de tus decisiones este ámbito tecnológico.

Por Ana Karen Ingalls

Las 8 ciber amenazas más letales

Los delincuentes tienden a ver a las PYMES como objetivos atractivos, ya que a menudo tienen menos recursos para invertir en medidas de seguridad y, en muchos casos, carecen de la experiencia necesaria para gestionar riesgos de seguridad adecuadamente. Esto puede incluir desde fraudes y robos hasta ciberataques.

¿Sabías que un solo ciberataque puede ser tan letal que puede llegar incluso a destruir una pyme en cuestión de días o incluso horas? Da miedo, ¿verdad? Pero lo cierto es que un ciberataque puede detener toda la operación de una pyme en aproximadamente 10 minutos y dejarla sin ingresos y golpear para siempre su reputación.

Ransomware

El ransomware es un tipo de malware peligroso que infecta los sistemas de una empresa, encriptando sus datos y haciéndolos inaccesibles para los usuarios. Para restablecer el acceso, los delincuentes suelen exigir el pago de un rescate, lo que puede representar una amenaza significativa para las pequeñas y medianas empresas (PYMES), que pueden no estar preparadas para afrontar la pérdida de datos ni el costo del rescate.

Según el informe Sophos Threats 2024, el ransomware se ha convertido en la principal preocupación para las PYMES, constituyendo hasta el 50% de todos los incidentes de malware reportados en 2023. Esta cifra resalta la prevalencia de este tipo de ataque y la urgencia con la que las empresas deben abordar la ciberseguridad. Las PYMES, al ser a menudo más vulnerables a ataques debido a la falta de recursos y sistemas de seguridad robustos, deben implementar medidas proactivas de protección, como copias de seguridad regulares, formación en ciberseguridad para empleados y software de seguridad actualizado. La concienciación sobre estas amenazas es clave para minimizar el riesgo de ser víctima de ransomware.

Software vulnerability exploits.

Se trata de ciber atacantes que se aprovechan de bugs en el software sin actualizar u obsoletos que no tiene corregidos los fallos identificados para así infiltrarse en un software o equipo profesional.

Malware

Los programas informáticos infectan el sistema de hardware de la pyme o roban sus datos e información. Informes recientes afirman que las infecciones por malware en pymes por troyanos disfrazados de archivos de Excel aumentaron un 5% en el primer trimestre del año.

Ataque de denegación de servicio o DDoS.

Un ataque de denegación de servicio (DoS) o ataque de denegación de servicio distribuido (DDoS) es una forma de ataque cibernético en la que múltiples dispositivos comprometidos inundan los servidores de una empresa o su sitio web con tráfico excesivo. Esta saturación provoca que los servidores se vuelvan inoperativos, interrumpiendo el funcionamiento normal de los servicios y haciendo que los usuarios legítimos no puedan acceder a ellos.

Los ataques DDoS son particularmente dañinos porque pueden paralizar las operaciones de una empresa, causando pérdidas financieras, daño a la reputación y frustración entre los usuarios. Estos ataques pueden ser perpetrados por diversos motivos, desde la extorsión hasta la competencia desleal o incluso como una forma de protestar.

Software Software vulnerability exploits.y exploits.

Se trata de ciber atacantes que se aprovechan de bugs en el software sin actualizar u obsoletos que no tiene corregidos los fallos identificados para así infiltrarse en un software o equipo profesional.

Remote Desktop Protocol Attacks.

Los ataques a través del Protocolo de Escritorio Remoto (RDP) son una técnica utilizada por ciber atacantes para obtener acceso no autorizado a los sistemas de una empresa de manera remota. Estos ataques se dirigen especialmente a organizaciones que no cuentan con medidas de seguridad adecuadas o que tienen configuraciones débiles en sus sistemas RDP, lo que facilita la vulnerabilidad.

Dispositivos robados.

La pérdida o el robo de dispositivos portátiles, teléfonos y otros dispositivos que contienen información crítica compromete la seguridad empresarial. Por ello, si éstos se pierden o roban se debe actuar con rapidez para controlar el acceso a la información que hay en su interior.

Ataques internos.

Empleados descontentos o no capacitados, pueden ser tan perjudiciales para una empresa que un ciberataque. Los sabotajes internos pueden llegar a ser devastadores entonces ¿controlas en tu empresa qué trabajadores pueden acceder a dispositivos, programas y softwares? Es imprescindible seguir el rastro de cada empleado.

Impacto de los ciberataques en las pymes

Los costes de un ciberataque son astronómicos para las pymes. De hecho, la media en España gira en torno a los 35.000 euros.

Educación en la Era de la Inteligencia Artificial y Automatización

Por Andrea Ramírez

La inteligencia artificial (IA) y la automatización están transformando rápidamente el mercado laboral, dando lugar a la creación de nuevas oportunidades, pero también a la desaparición de muchos trabajos tradicionales. Este cambio plantea retos significativos para el sistema educativo, que debe adaptarse para preparar a los estudiantes para trabajos y habilidades que aún no existen. La educación, en este contexto, no solo debe enfocarse en los conocimientos técnicos específicos de las industrias actuales, sino también en desarrollar habilidades transferibles que permitan a los estudiantes prosperar en un entorno laboral en constante evolución. Este artículo reflexiona sobre cómo la IA y la automatización están redefiniendo el mercado laboral y cómo las instituciones educativas deben ajustarse a estos cambios para garantizar que los estudiantes estén preparados para el futuro.

IMPACTO DE LA INTELIGENCIA ARTIFICIAL Y LA AUTOMATIZACIÓN EN EL MERCADO LABORAL

La inteligencia artificial y la automatización están reformulando el mercado laboral de diversas maneras. En muchos sectores, las máquinas y los algoritmos están reemplazando tareas rutinarias y repetitivas, como la fabricación, la recopilación de datos y el análisis de grandes volúmenes de información. De acuerdo con un informe de McKinsey (2017), se espera que la automatización pueda reemplazar hasta el 30% de los trabajos en los próximos 15 a 20 años, especialmente aquellos que involucren tareas mecánicas y administrativas.

Sin embargo, la automatización no solo está desplazando empleos; también está creando nuevas oportunidades. La necesidad de diseñar, gestionar y mantener sistemas automatizados y de IA está dando lugar a una demanda creciente de trabajos especializados en áreas como la programación, el análisis de datos y la ciberseguridad. Además, la IA está permitiendo la creación de trabajos que antes no existían, especialmente en campos como la tecnología, la biomedicina y la inteligencia artificial aplicada.

El gran desafío radica en la velocidad con que estos cambios se están produciendo y en cómo las instituciones educativas pueden anticiparse a las habilidades y capacidades que los estudiantes necesitarán en este entorno laboral en constante cambio.

LA ADAPTACIÓN DEL SISTEMA EDUCATIVO: ENFOQUE EN HABILIDADES TRANSFERIBLES

En lugar de centrarse exclusivamente en la adquisición de conocimientos técnicos específicos de un sector, el sistema educativo debe centrarse en el desarrollo de habilidades transferibles que preparen a los estudiantes para la adaptabilidad y la resolución de problemas complejos.Estas habilidades incluyen el pensamiento crítico, la creatividad, la capacidad de trabajar en equipo, la comunicación efectiva y la alfabetización digital.

La educación debe fomentar la capacidad de los estudiantes para aprender de forma continua y autónoma, ya que el ritmo acelerado de los avances tecnológicos exigirá que los trabajadores del futuro se adapten constantemente a nuevas herramientas y métodos.

La "educación para la resiliencia" será esencial en este nuevo panorama. Los estudiantes deben estar preparados para enfrentarse a desafíos y a la incertidumbre en un mercado laboral que sigue cambiando, aprendiendo a tomar decisiones informadas en situaciones de ambigüedad y aprendiendo de sus errores. Las instituciones educativas deberán integrar estos aspectos en su currículo y ofrecer programas que fomenten una mentalidad de crecimiento y flexibilidad.

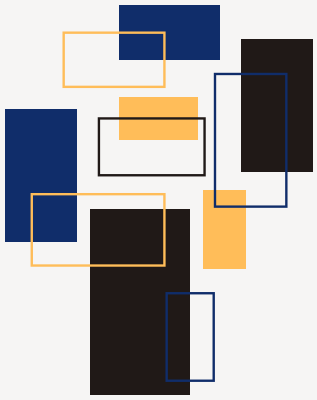
EL ROL DE LAS TECNOLOGÍAS EDUCATIVAS EN LA FORMACIÓN DEL FUTURO

Las tecnologías educativas juegan un papel fundamental en la preparación de los estudiantes para la era de la IA y la automatización. Las plataformas de aprendizaje en línea, la inteligencia artificial aplicada a la enseñanza y la realidad aumentada son herramientas que pueden enriquecer el proceso educativo y ofrecer a los estudiantes experiencias más interactivas y personalizadas. Las herramientas de IA pueden ayudar a los estudiantes a desarrollar habilidades de manera individualizada, proporcionando recursos adaptativos y retroalimentación instantánea que les permita avanzar a su propio ritmo.

Además, la incorporación de simulaciones, juegos educativos y entornos virtuales de aprendizaje (entornos inmersivos) permitirá a los estudiantes experimentar en escenarios que reflejan los cambios rápidos y las demandas tecnológicas del mundo laboral.

REVISIÓN DEL ROL DE LOS DOCENTES EN LA ERA DIGITAL

El papel de los docentes está cambiando a medida que las tecnologías avanzan. Si bien la IA puede desempeñar un papel crucial en la personalización del aprendizaje, los educadores seguirán siendo esenciales en la enseñanza de habilidades socioemocionales, valores éticos y la capacidad de adaptación. Los docentes deben adoptar un enfoque más como mentores y facilitadores del aprendizaje, apoyando a los estudiantes en su desarrollo de competencias y habilidades cognitivas que les permitan navegar en un entorno digital y automatizado.



PREPARACIÓN PARA LOS TRABAJOS DEL FUTURO: DE LA ESPECIALIZACIÓN A LA FLEXIBILIDAD

En el futuro, los trabajos no serán estáticos. En lugar de preparar a los estudiantes para trabajos concretos y especializados, las instituciones educativas deben fomentar una mentalidad de "aprendizaje continuo" y equipar a los estudiantes con las herramientas necesarias para que puedan adquirir nuevas habilidades a lo largo de su vida. El concepto de "trabajos del futuro" es dinámico y debe entenderse como un entorno flexible, donde los individuos puedan adaptarse a nuevas tecnologías y roles a medida que emergen.

Las habilidades que los estudiantes necesitarán incluirán conocimientos profundos sobre IA y automatización, así como una comprensión sólida de cómo interactuar con estas tecnologías de manera ética y responsable. Además, las habilidades creativas, como la innovación y la resolución de problemas complejos, seguirán siendo esenciales en roles que no pueden ser fácilmente automatizados.

CONCLUSIÓN

La inteligencia artificial y la automatización están remodelando el panorama laboral, lo que exige una transformación en el sistema educativo. Preparar a los estudiantes para trabajos que aún no existen implica un enfoque en el desarrollo de habilidades transferibles, la adaptabilidad y el pensamiento crítico. Las instituciones educativas deben evolucionar para incorporar tecnologías que mejoren el aprendizaje y ayudar a los estudiantes a desarrollar una mentalidad de crecimiento continuo. A medida que el mercado laboral se transforma, las escuelas y universidades tienen un papel crucial en la formación de individuos preparados para un futuro dinámico y lleno de oportunidades impulsadas por la tecnología.

***B**ibliografía*

Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company

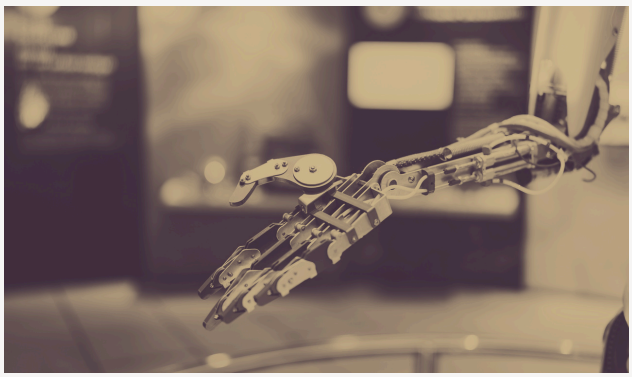
Chui, M., Manyika, J., & Miremadi, M. (2017). Where machines could replace humans—and where they can't (yet). McKinsey Quarterly. https://www.mckinsey.com

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerization? Technological Forecasting and Social Change, 114, 254-280. https://doi.org/10.1016/j.techfore.2016.08.019

Levy, F., & Murnane, R. J. (2013). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. W. W. Norton & Company.

Schwab, K. (2016). The Fourth Industrial Revolution. Crown Business.

World Economic Forum. (2020). The future of jobs report 2020. https://www.weforum.org/reports/the-future-of-jobs-report-2020



Propósito y Aplicación de los Marcos de Control de TI

Por Joaquín Ortiz

INTRODUCCIÓN

En la actualidad, las organizaciones dependen cada vez más de la tecnología para alcanzar sus objetivos estratégicos. Sin embargo, esta dependencia también conlleva riesgos relacionados con la seguridad, la disponibilidad y la integridad de los sistemas de TI. Para gestionar estos riesgos de manera efectiva y garantizar una operación segura y eficiente, las empresas implementan marcos de control de TI.

Estos marcos proporcionan estructuras organizadas que permiten establecer, evaluar y mejorar los controles de TI, asegurando que los sistemas y procesos tecnológicos sean confiables y cumplan con las regulaciones aplicables.

IMPORTANCIA EN LA AUDITORÍA DE TI

Desde la perspectiva de la auditoría de TI, los marcos de control son esenciales para:

- Estandarizar los Controles: Proporcionan un enfoque estructurado para diseñar y evaluar controles de TI.
- Identificar y Mitigar Riesgos: Ayudan a las organizaciones a identificar riesgos tecnológicos y establecer mecanismos para mitigarlos.
- Garantizar el Cumplimiento Normativo: Facilitan la alineación con regulaciones como SOX, PCI-DSS, ISO 27001 y GDPR. Optimizar la Gobernanza de TI: Aseguran que la tecnología se administre de manera eficiente y alineada con los objetivos del negocio.
- Facilitar la Auditoría: Proporcionan referencias claras para evaluar la efectividad de los controles implementados.

Los marcos de control de TI son fundamentales para establecer buenas prácticas en la gestión de riesgos y seguridad, permitiendo a las organizaciones operar en entornos digitales de manera confiable.

PROPÓSITO DE LOS MARCOS DE CONTROL DE TI

Los marcos de control de TI tienen como propósito proporcionar una estructura sistemática para la gestión de la tecnología dentro de las organizaciones. Sus principales objetivos incluyen:

1. Definir un Modelo de Gobernanza de TI: 1Asegurar que la toma de decisiones tecnológicas esté alineada con los objetivos estratégicos del negocio.
2. Mejorar la Seguridad de la Información: Implementar controles efectivos para proteger la confidencialidad, integridad y disponibilidad de los datos.
3. Asegurar el Cumplimiento Normativo: Facilitar la adherencia a regulaciones y estándares internacionales de seguridad y control interno.

4. Optimizar la Gestión de Riesgos: Identificar amenazas potenciales y definir estrategias para mitigarlas de manera proactiva.

5. Estandarizar Procesos de TI: Establecer procedimientos claros para la administración de la infraestructura, servicios y operaciones tecnológicas.

6. Incrementar la Eficiencia Operativa: Mejorar la administración de recursos tecnológicos y reducir la probabilidad de incidentes.

7. Facilitar Auditorías y Evaluaciones de Control: Proveer una base estructurada para evaluar la efectividad de los controles implementados.

Los marcos de control de TI permiten establecer un entorno tecnológico seguro, confiable y auditable, reduciendo la incertidumbre en la gestión de TI y fortaleciendo la resiliencia organizacional.

APLICACIONES DE LOS MARCOS DE CONTROL DE TI EN LAS ORGANIZACIONES

Los marcos de control de TI no son solo guías teóricas, sino herramientas prácticas que se aplican en diversas áreas de la gestión tecnológica. Algunas de sus aplicaciones más comunes incluyen:

CUMPLIMIENTO REGULATORIO Y NORMATIVO

- Las organizaciones utilizan marcos de control de TI para cumplir con regulaciones como: SOX (Sarbanes-Oxley Act): Requiere controles de TI robustos para garantizar la confiabilidad de los informes financieros.
- GDPR (Reglamento General de Protección de Datos): Exige la protección adecuada de datos personales en empresas que operan en la Unión Europea.
- ISO 27001: Establece un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger activos digitales.
- PCI-DSS (Payment Card Industry Data Security Standard): Define requisitos de seguridad para la protección de datos de tarjetas de pago.

GESTIÓN DE RIESGOS DE TI Y SEGURIDAD CIBERNÉTICA

Los marcos de control permiten identificar y mitigar riesgos tecnológicos mediante la implementación de controles de seguridad, como:

- Gestión de Identidades y Accesos (IAM).
- Monitoreo de eventos y respuesta a incidentes de seguridad.
- Análisis de vulnerabilidades y pruebas de penetración.

MEJORA DE LA GESTIÓN DE SERVICIOS DE TI

- Implementación de ITIL o ISO 20000 para mejorar la entrega y soporte de servicios tecnológicos.
- Gestión de incidentes, problemas y cambios para garantizar la estabilidad operativa. Optimización de la infraestructura de TI para reducir costos y mejorar la eficiencia.

Conclusión

Los marcos de control de TI son esenciales para garantizar una gestión eficiente y segura de los sistemas tecnológicos en cualquier organización. Su aplicación permite mitigar riesgos, fortalecer la seguridad de la información y cumplir con normativas internacionales. Además, la implementación de controles básicos de TI es fundamental para proteger los activos digitales y asegurar la continuidad del negocio en un mundo cada vez más digitalizado.

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