AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del uso de metodología DevOps

The Institute of Internal Auditors

Instituto de Auditores Internos de España

El INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la Auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.

LA FÁBRICA DE PENSAMIENTO es el laboratorio de ideas del Instituto de Auditores Internos de España sobre gobierno corporativo, gestión de riesgos y Auditoría Interna, donde participan más de 150 socios y profesionales técnicos expertos.

AUDITORÍA INTERNA

OBSERVATORIO SECTORIAL

PRÁCTICAS DE BUEN GOBIERNO

BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS

El laboratorio trabaja con un enfoque práctico en la producción de documentos de buenas prácticas que contribuyan a la mejora del buen gobierno y de los sistemas de gestión de riesgos en organizaciones de habla hispana. Además de desarrollar contenido, fomenta el intercambio de conocimientos entre los socios.

ENCUENTRA TODOS LOS DOCUMENTOS DE LA FÁBRICA EN www.auditoresinternos.es

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna del uso de metodología DevOps

Diciembre 2025

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Ángela de la Cruz Oñate, CISA, PMP. MAPFRE.

José María Acha Fernández. TELEFÓNICA.

Juan Diego Fallas Alvarado, SCRUM, COBIT. BANCO NACIONAL DE COSTA RICA.

Jesús García Benítez. SEAT.

Jonathan Laguna Ciudad, CISM, CISSP. EY.

José Martínez Vicaria, CISA, ISO 27001 - ISO 22301 Lead Auditor. REPSOL.

Marcos Pico Martínez, COSO Control Interno, CCSP. INDITEX.

Eneko Rodríguez Achalandabaso, CISA. IBERDROLA.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

La metodología DevOps surge con el propósito de acelerar el ciclo de vida del desarrollo del software, frente a las estructuras tradicionales en las que la diferenciación entre los equipos de desarrollo y operación de sistemas resultaba en un *time to market* más lento y con mayores costes. DevOps propone una metodología que busca la integración y colaboración de ambos equipos para automatizar procesos y acelerar la entrega de aplicaciones, propiciando ciclos de desarrollo más rápidos e implementaciones más fiables, a través de una mejora en la comunicación, frecuencia, calidad y escalabilidad del software.

La implementación exitosa de DevOps requiere cambios culturales significativos, tales como la adopción de una cultura ágil y enfocada al usuario o un proceso continuo de colaboración que sustituya el trabajo por etapas aisladas, avanzando en la integración continua en la que los desarrolladores integran código en un repositorio compartido y el despliegue continuo automatizando la puesta en marcha de aplicaciones al superar las pruebas requeridas.

En este entorno de mayor velocidad y automatización, el papel de Auditoría Interna es fundamental para la revisión de aspectos como la seguridad, el cumplimiento regulatorio o el aseguramiento de los procesos, ayudando a equilibrar la innovación con un adecuado gobierno y la incorporación de estructuras de control para hacer frente a los riesgos del uso de la metodología DevOps. Para ello, el documento incorpora una propuesta de programa de trabajo para revisar los principales aspectos de gobierno, gestión de riesgos y control interno en entornos DevOps, considerando lo previsto en referentes como el marco NIST o la norma ISO 27001.

INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Índice

Introducción

DevOps pretende lograr ciclos de desarrollo más rápidos, implementaciones más fiables y una mayor eficiencia en la gestión del software.

DevOps se define como una metodología que busca la integración de los equipos de desarrollo de software y operaciones de IT para aumentar la colaboración, automatizar procesos y acelerar la entrega de aplicaciones. Su utilización pretende lograr ciclos de desarrollo más rápidos, implementaciones más fiables y una mayor eficiencia en la gestión del software, asegurando que el código se construya, pruebe y despliegue de forma continua y sin interrupciones. No obstante, una implementación exitosa bajo entornos DevOps requiere cambios culturales significativos, incluyendo la adopción de una cultura ágil y enfocada en el usuario y el diseño de un proceso continuo de colaboración que abandone la mentalidad de trabajar por etapas aisladas.

Aunque los beneficios de adoptar DevOps son variados y pueden ser significativos para el negocio, ante ese entorno de alta velocidad y automatización, el papel de la función de Auditoría Interna resulta fundamental para la revisión de aspectos como la seguridad, el cumplimiento y, en general, todo lo relacionado con la gestión de riesgos y controles sobre el desarrollo y operación del software, ayudando así a equilibrar la velocidad e innovación con un adecuado proceso de gobierno, como base para establecer un entorno de control efectivo.

Este documento, además de abordar las implicaciones generales del uso de las metodologías DevOps, presenta una propuesta de programa de trabajo como referencia para la revisión por parte de Auditoría Interna de los principales aspectos relacionados con el gobierno, gestión de riesgos y control interno en entornos DevOps, considerando lo establecido en los principales marcos o estándares internacionales de referencia en este ámbito.

Contexto y nacimiento de DevOps

La metodología de desarrollo DevOps surge entre los años 2007 y 2008, principalmente para resolver posibles situaciones de conflicto de intereses entre los equipos de desarrollo y operaciones tecnológicas y acelerar el ciclo de vida del desarrollo del software.

Antes del origen de la metodología DevOps, las organizaciones del mundo de las Tecnologías de la Información (IT) se basaban en una estructura tradicional, donde desarrolladores y operadores se veían los unos a otros como adversarios, debido a que sus objetivos a alcanzar parecían ser contrarios entre sí.

Por un lado, el equipo de desarrollo debe responder a los cambios del mercado, llevando nuevas funcionalidades a producción de la manera más rápida posible. Mientras que el área de operaciones debe encargarse de ofrecer servicios estables, fiables y seguros para el cliente, lo cual supone evitar que pasen a producción cambios que pongan en peligro el entorno de control del desarrollo realizado.

El conflicto aparece cuando los equipos implementan medidas para cumplir sus propios objetivos, sin tener en cuenta la repercusión que esto puede causar en los demás. Así, las empresas IT que no utilizaban la metodología DevOps se veían incapaces de hacer cambios en producción en poco tiempo, tardando semanas e incluso meses; además, al no ser una rutina, los cambios solían resultar en caídas del sistema y otras complicaciones.

Este conflicto de intereses e incapacidad de realizar cambios constantes se traduce en un *time to market*[1] lento, una calidad de producto cuestionable, un coste humano y económico no deseado y un aumento de la deuda técnica; siendo estas algunas de las dificultades que se presentaban antes del origen de la metodología DevOps.

La necesidad de una mejor dinámica de trabajo llevó a profesionales e investigadores de la ingeniería del software como Patrick Dubois, Gene Kim y John Willis a iniciar un movimiento que promovía la colaboración estrecha entre desarrollo y operaciones, lo que más tarde se conocería como DevOps. Lo que comenzó en foros y encuentros locales se convirtió en una metodología clave para mejorar la entrega continua, la calidad del software y la satisfacción del cliente.

DevOps aporta ventajas como la reducción del "time to market" de las aplicaciones.

BENEFICIOS DEL USO DE DEVOPS

A continuación, se enumeran algunos de los beneficios más destacados del uso de la metodología DevOps:

- **Aumento de la rentabilidad:** disminuye el *time-to-market* y permite abarcar una mayor cuota de mercado.
- **Mejora en la comunicación:** la cooperación y entendimiento entre departamentos son clave en el sistema DevOps. Muchas herramientas utilizadas en este proceso fomentan el intercambio de información bidireccional sobre el flujo de trabajo, lo que genera dinámicas constantes de comunicación y retroalimentación.
- **Más publicaciones y con mayor frecuencia:** mediante la integración continua, los desarrolladores pueden compilar y ejecutar pruebas de forma recurrente en las primeras etapas y los equipos de operaciones pueden entregar versiones de calidad en menor tiempo. Como resultado, el usuario final recibe mejor producto y en menor plazo.
- **Software de mejor calidad:** desde las etapas más tempranas de la creación de la aplicación, hasta el despliegue del software, se verifica continuamente, a través de las pruebas ya mencionadas, que no exis-

1. Se entiende por *Time to market* el intervalo temporal que transcurre entre el inicio formal del desarrollo de un producto, servicio o funcionalidad y su disponibilidad efectiva para el cliente o usuario final.

La metodología DevOps favorece la escalabilidad del software, aportando mayor flexibilidad.

tan posibles defectos que perjudiquen el desarrollo del código, ni dificulten el uso del software.

El usuario final recibe desde el primer momento un producto estable, además de un soporte continuo y eficaz, generando una mejor experiencia de usuario.

- **Escalabilidad:** el sistema DevOps aporta flexibilidad para añadir nuevo código. Esto permite adaptarse a circunstancias cambiantes, que requieran la ampliación del software en cualquier sentido, sin arriesgar toda la producción.

- **Mayor seguridad:** gracias a la automatización de los procesos de control de código, se reduce la participación humana que no aporta valor añadido, minimizando la posibilidad de error.

  A través de enfoques como "Security by Design"[2], el control de amenazas y vulnerabilidades ya no queda relegado a las fases de despliegue del código, ahora los departamentos especialistas en ciberseguridad se integran en el proceso desde que se obtienen los requisitos, es decir, al inicio del ciclo de vida del software. Esto es lo que se conoce como DevSecOps, desarrollado más adelante en este documento.

- **Seguimiento continuado de la aplicación:** el objetivo ya no es entregar un producto cerrado al usuario o cliente y desentenderse del mismo. Las aplicaciones no tienen un final de ciclo de vida definido, por lo que las acciones de monitoreo y registro son continuas.

  Se da cobertura eficaz a las posibles incidencias a la vez que se pueden seguir desarrollando nuevas versiones según lo estipulado.

- **Crecimiento de la productividad:** el sistema DevOps está basado en el rendimiento y en la colaboración, evitando obstáculos burocráticos y la rigidez de las jerarquías.

  Los usuarios empiezan a tener conciencia de cómo afecta su labor al conjunto del trabajo, entendiendo mejor cuál debe ser su aportación, por lo que comienzan a sentirse más valorados. Esto hace que se involucren más en el proceso de desarrollo.

- **Mejora de la metodología DevOps:** DevOps no es un sistema cerrado, permite asimilar nuevas herramientas que mejoren la comunicación y la eficacia. Los continuos avances tecnológicos exigen una permanente innovación que permita mantener el estándar de agilidad.

- **Reducción de costes:** el resultado directo del aumento de la eficacia de los trabajadores, de la productividad, el menor tiempo requerido para la entrega de un producto digital y la agilidad del proceso en general es la reducción de gastos.

2. *Security by design* es una metodología de desarrollo de sistemas en la que los requisitos de seguridad se incorporan como criterios fundamentales de diseño, de forma que las arquitecturas, procesos y mecanismos implementados reduzcan riesgos y vulnerabilidades desde la raíz, antes de la implementación y el despliegue.

Fundamentos y Metodología DevOps

CULTURA Y RESPONSABILIDADES COMPARTIDAS

La implementación de la metodología DevOps requiere cambios culturales significativos con respecto al funcionamiento que comúnmente tienen los departamentos de TI, algunos de los cuales son los siguientes:

- **Adopción de la cultura ágil enfocada en el usuario, para toda la organización;** que permita acelerar el desarrollo de productos y que garantice la innovación.
  Esto demanda una gestión del cambio y una involucración desde la alta dirección hasta la participación de los niveles operativos.

- La integración de áreas de desarrollo y operaciones corresponde a un **cambio radical con los modelos de trabajo tradicionalmente divididos.**
  Esto implica que las organizaciones deben diseñar un proceso continuo de colaboración entre los equipos de trabajo, desde la atención de una idea hasta su puesta en producción. Esta situación requiere abandonar la mentalidad de solo alcanzar o superar etapas por parte de un equipo, para luego trasladar su resultado al siguiente durante la construcción del software.

- Las funciones de control también se ven afectadas cuando se adopta esta práctica, debido a la **necesidad de considerar el aseguramiento de primera y segunda línea para integrarse en el flujo de trabajo.**
  Esta situación requiere adaptarse al concepto de agilidad, garantizando al mismo tiempo calidad, seguridad y cumplimiento. Auditoría Interna, como tercera línea, también se ve afectada dado su propósito de proporcionar al Consejo de Administración y a la Alta Dirección aseguramiento, asesoramiento, prospectivas y previsiones de manera independiente, objetiva y basada en riesgos[3].

Por otro lado, la adopción de estas metodologías y cambios culturales en contextos OT (organización industrial) puede representar un reto aún mayor, ya que la disponibilidad de los sistemas juega un papel fundamental, con tiempos de parada mínimos y con unos requisitos de seguridad si caben más estrictos debido a las infraestructuras críticas que pueden estar involucradas.

Por ello, si bien algunas organizaciones están comenzando a ver los beneficios de poder configurar y reprogramar los elementos como PLCs o SCADA de forma más ágil y continua, su adopción es más paulatina que en entornos IT.

La adopción de la metodología DevOps conlleva retos como un cambio cultural y en los modelos de trabajo tradicionales.

3. Declaración del propósito de la función de Auditoría Interna según lo establecido en las *Normas Globales de Auditoría Interna*™

INTEGRACIÓN Y DESPLIEGUE CONTINUOS (CI/CD)

La integración y despliegue continuos son elementos esenciales para la eficiencia y calidad del desarrollo de software.

Como se ha mencionado en los puntos anteriores, las organizaciones se están enfrentando a cambios culturales significativos y a una mayor exigencia en el cumplimiento normativo y regulatorio en el marco del desarrollo de software. Estos cambios y exigencias están derivando en la búsqueda de conseguir una mayor eficiencia y calidad en los procesos de desarrollo del software.

La integración continua (CI) y el despliegue continuo (CD) son elementos esenciales o fundamentales para lograr los objetivos de eficiencia y calidad.

La **integración continua** es una práctica de desarrollo de software donde los desarrolladores integran su código en un repositorio compartido varias veces al día. Cada integración es verificada por una construcción automatizada y mediante pruebas para detectar errores lo antes posible.

Prácticas y principios básicos de la integración continua

- Repositorios de origen.
- Control de versiones.
- Pruebas automatizadas.
- Cambios publicados.
- Compilaciones automáticas.
- Ambientes homogéneos.

El **despliegue continuo** se puede entender como una extensión de la integración continua que automatiza el despliegue de una aplicación en un entorno productivo, después de haberse sometido a todas las pruebas.

Principios básicos en el despliegue continuo

- Automatización del despliegue.
- Integración continua.
- Revisión de código.
- Monitorización y *Feedback*.

Elementos clave en la automatización y herramientas disponibles para la integración y el despliegue continuos

- Reducción de errores humanos.
- Entrega continua.
- Mayor seguridad.
- Optimización de recursos.
- Aumento de los requerimientos y exigencias de negocio.

Plantear una estrategia de CI/CD en las organizaciones debería ir acompañada de herramientas que logren cubrir el objetivo de automatización deseado. El mundo tecnológico avanza a un ritmo mayor que el ritmo marcado por las propias organizaciones y se enfrenta a constantes cambios y evoluciones.

A continuación, se plantean una serie de herramientas que son base para el desarrollo de CI/CD. Estos son ejemplos, ya que cada organización tiene sus propios flujos de trabajo y herramientas.

- **Jenkins.** Compilación, prueba y despliegue de aplicaciones.
- **Docker.** Empaquetado de aplicaciones en contenedores "ligeros".
- **Kubernetes.** Plataforma que automatiza la gestión de contenedores.

- **Ansible.** Automatización de servidores y gestión de infraestructura mediante código.
- **Terraform.** Gestión de infraestructuras en la nube (AWS, Azure, Google Cloud).
- **GitHub Actions.** Automatización de flujos de trabajo directamente sobre los repositorios de código.

FIGURA1. FLUJO DE TRABAJO DE INTEGRACIÓN Y DESPLIEGUE CONTINUO (CI/CD)

SEGURIDAD EN LOS PROCESOS: DevSecOps

Las organizaciones están afrontando un aumento en las amenazas de ciberseguridad, así como en la exigencia de marcos de cumplimiento cada vez más rigurosos, lo que está llevando a la necesidad de integrar la seguridad en el desarrollo de software. La aproximación *DevSecOps*[4] propone una solución a esta problemática al combinar los principios de DevOps con prácticas de seguridad.

La principal diferencia entre DevSecOps y DevOps radica en la integración de la seguridad en cada etapa del ciclo de vida del producto; por un lado, DevOps está centrado en la colaboración entre desarrollo y operaciones para garantizar la entrega continua de software, mientras que DevSecOps añade una capa de seguridad desde la planificación y el diseño hasta la operación y el mantenimiento. Esto implica que las consideraciones de seguridad y cumplimiento, desde una perspectiva ágil, son incorporadas en cada sprint, en lugar de ser atendidas por separado o al final del proceso de desarrollo; permitiendo a los equipos abordar problemas de seguridad y confiabilidad en los productos digitales de manera rápida y efectiva.

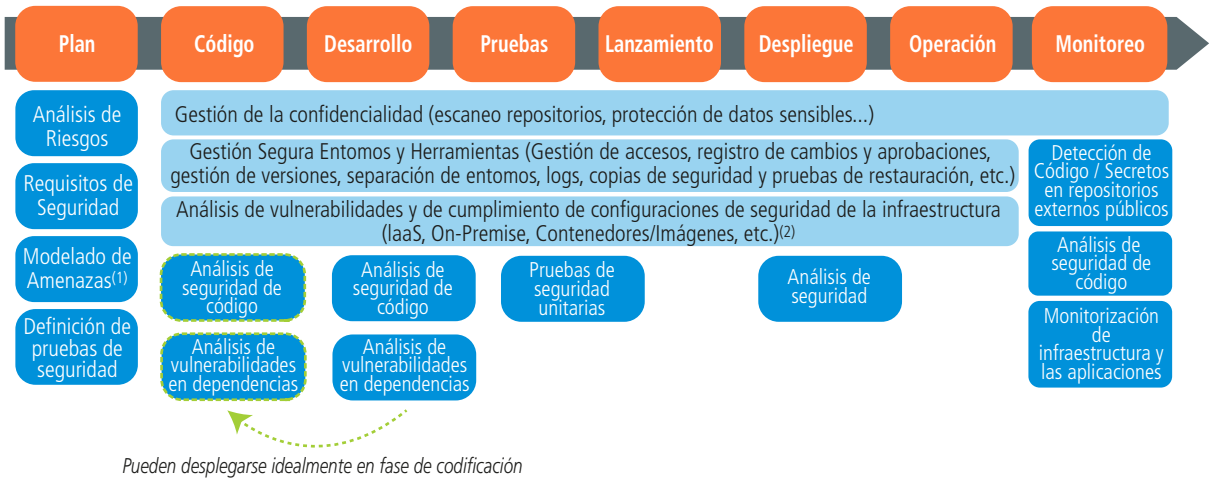
DevSecOps posee características clave que permiten a las organizaciones cumplir altos estándares de seguridad. Primero, facilita incrementar la frecuencia de las liberaciones de

4. Enfoque integrado de ingeniería de software que extiende la filosofía DevOps incorporando la Seguridad (Sec) como un componente transversal y automatizado en todo el ciclo de vida de desarrollo, de modo que los principios, prácticas y controles de ciberseguridad se aplican desde las fases iniciales de diseño hasta la operación en producción.

software sin comprometer la postura de riesgo. Además, contribuye a implementar tareas para mejorar el tiempo promedio en la atención de vulnerabilidades; eliminando retrasos, sobrecostos, defectos de productos y posibles vulnerabilidades.

Sin embargo, para obtener todos los beneficios de este modelo es necesario aplicar cambios en la gestión tecnológica; que incluye la creación de un modelo operativo integrado con equipos multifuncionales y expertos áreas como seguridad y cumplimiento, automatizaciones de tareas, así como desarrollo de productos digitales seguros desde el diseño y considerando la experiencia de Auditoría Interna en la supervisión del control interno.

FIGURA 2. FLUJO DE TRABAJO DE PARA UN ENTORNO DEVSECOPS



(1) El modelado de amenazas trabaja para identificar, comunicar y comprender las amenazas y mitigaciones dentro del contexto de proteger las aplicaciones.
Fuente: https://devguide.owasp.org/es/04-design/01-threat-modeling/01-threat-modeling/

(2) El análisis consiste en determinar la probabilidad de una amenaza y compararlo contra la evaluación de riesgos que tenga el servicio o la aplicación.
Fuente: https://ciberseguridad.com/guias/desarrollo-seguro/owasp/

Indicadores o métricas relevantes DevOps

En el contexto de DevOps es esencial evaluar el rendimiento de la operativa para garantizar la entrega, desarrollo continuo y de calidad. Algunas empresas tecnológicas detallan los siguientes indicadores mínimos a tener en cuenta:

- *Lead Time for Changes*: similar al plazo para modificaciones, este indicador mide el tiempo desde que se inicia el desarrollo de una nueva característica hasta que está disponible en producción.

- *Change Failure Rate:* este indicador mide el porcentaje de implementaciones que resultan en fallos en producción y requieren intervención inmediata; este aspecto es clave para la implementación de actividades de mejora continua.
- *Deployment Frequency:* frecuencia con la que se despliega código en producción, similar a la frecuencia de implementación.
- *Mean Time to Recovery:* mide el tiempo promedio para restaurar el servicio después de una interrupción, similar al tiempo medio de recuperación.

Marcos de referencia

DevOps va más allá de ser un conjunto de herramientas o una metodología de trabajo, hace referencia a una cultura o forma de pensar de cara a obtener la máxima eficiencia durante las fases de Desarrollo y Operación dentro de los sistemas de una organización. Para entender esta filosofía existen distintos marcos que tratan de explicar el enfoque DevOps.

DevOps va más allá de una metodología, supone un cambio cultural en los sistemas de la organización.

THE THREE WAYS (DE "THE PHOENIX PROJECT" Y "THE DEVOPS HANDBOOK")

Este marco describe los tres principios que sustentan el flujo de trabajo de DevOps:

- La primera vía: Flujo
  Optimizar el flujo de trabajo desde el desarrollo hasta la operación, identificando y eliminando cuellos de botella.
- La segunda vía: Retroalimentación
  Establecer bucles de retroalimentación rápidos y constantes en todas las etapas del ciclo de vida para aprender y mejorar continuamente.
- La tercera vía: Experimentación y Aprendizaje Continuo
  Fomentar una cultura de experimentación segura, donde los equipos puedan probar nuevas ideas, aprender de los errores y mejorar sus procesos.

CALMS (CULTURE, AUTOMATION, LEAN, MEASUREMENT, SHARING)

No es un proceso prescriptivo, sino más bien una filosofía a seguir que se basa principalmente en 5 pilares:

- Cultura: fomentar la colaboración, la confianza y la comunicación entre los equipos de desarrollo y operaciones.
- Automatización: automatizar tareas repetitivas y procesos clave para aumentar la eficiencia, la velocidad y la confiabilidad.
- Lean: aplicar principios de pensamiento Lean para eliminar innecesarios, optimizar el flujo de valor y mejorar continuamente.

- **Medición:** establecer métricas clave para monitorear el rendimiento, identificar cuellos de botella y tomar decisiones basadas en datos.
- **Compartir:** promover la transparencia, el intercambio de conocimientos y el aprendizaje continuo entre los equipos, además de compartir las responsabilidades y los logros entre los equipos.

Para dar soporte a esta cultura o forma de trabajo existen marcos y herramientas que ayudan a implementar estos principios.

CALM	SOPORTE	DESCRIPCIÓN
Cultura	Scrum	Promueve la colaboración y la comunicación continua a través de sprints y reuniones diarias.
	Kanban	Fomenta la transparencia y la mejora continua mediante la visualización del flujo de trabajo.
	SAFe	Facilita la alineación organizacional y la colaboración en equipos grandes.
	ITIL	Alinea los servicios de IT con las necesidades del negocio, promoviendo una cultura de servicio.
	XP (Extreme Programming)	Enfocado en la calidad del software y la colaboración continua con el cliente.
Automatización	CI/CD Pipelines	Prácticas que automatizan la integración y entrega continua de software, mejorando la eficiencia y reduciendo errores.
Lean	Kanban	Optimiza el flujo de trabajo y minimiza el desperdicio mediante la gestión visual de tareas.
	Lean Six Sigma	Metodología que combina Lean y Six Sigma para mejorar la eficiencia y la calidad.
	ITIL	Mejora la eficiencia en la entrega de servicios mediante la gestión de procesos de TI.
Medición	ITIL	Proporciona métricas y reportes para la gestión de servicios de TI.
	Kanban	Permite la visualización del progreso y la identificación de cuellos de botella a través de métricas de flujo.
	Dora Metrics	Conjunto de métricas diseñadas para medir el rendimiento de los equipos de DevOps: frecuencia de despliegue, tiempo de entrega de cambios, tiempo de recuperación de incidentes, tasa de fallos en cambios.
Compartir	Inner Source	Aplicar las mejores prácticas de código abierto (Open Source) dentro de la propia organización. Esto significa que los equipos comparten su código, sus herramientas y sus conocimientos con otros equipos internos, fomentando la colaboración y la reutilización.
	Blameless Post-Mortems (Análisis Post-Mortem sin Culpa)	Cuando ocurre un incidente, se realiza un análisis exhaustivo para entender qué pasó, por qué pasó y qué se puede hacer para evitar que vuelva a ocurrir. Lo crucial es que no se busca culpar a individuos, sino aprender del evento. Los resultados se comparten ampliamente para que todos aprendan y mejoren los sistemas y procesos.
	Uso de herramientas colaborativas	Uso de distintas herramientas que fomenten la compartición de trabajo y responsabilidades: documentales, gestión de proyectos y tareas, repositorios de código, plataformas CI/CD, monitorización y observabilidad.

Indicadores o métricas relevantes DevOps

LA AUDITORÍA INTERNA EN PROCESOS DEVOPS

La función de Auditoría Interna juega un papel clave en el proceso DevOps al aportar la revisión de aspectos de seguridad, cumplimiento y la gestión de riesgos y controles en el desarrollo y la operación de software. En un entorno donde la velocidad y la automatización son esenciales, la actividad de Auditoría Interna ayuda a equilibrar la innovación con la gobernanza, apoyando a establecer un entorno de control efectivo, siempre en el ámbito de sus responsabilidades.

Funciones principales con enfoque en marcos de control

- **Identificación y evaluación de riesgos:** debido al expertise de Auditoría Interna, su contribución es especialmente valiosa para identificar y mitigar riesgos relacionados con la seguridad en general, la privacidad de los datos y el cumplimiento normativo de cada jurisdicción. Para ello, es importante identificar aquellos aspectos que pueden afectar al cumplimiento de los principales objetivos estratégicos.
- **Monitoreo de cumplimiento:** verifica que las prácticas DevOps cumplan con regulaciones y estándares de la industria y los criterios de servicios de confianza.
- **Control de accesos y seguridad con automatización:** a través de la evaluación de los controles de acceso automatizados a sistemas y datos críticos, incluyendo la revisión de controles preventivos, detectivos y correctivos integrados en los desarrollos. Esto abarca aspectos como la evaluación de la segregación de funciones automatizada y los controles de autorización basados en roles.
- **Revisión de procesos automatizados:** incluye la auditoría de las herramientas de integración y entrega continua, para garantizar su correcta configuración y funcionamiento.
- **Gestión de registros y trazabilidad:** mediante el aseguramiento de la existencia de un registro adecuado de cambios en el código, configuraciones y despliegues.
- **Gestión y operación de la seguridad:** analizando las políticas de seguridad definidas alrededor de los procesos y herramientas DevOps así como su cumplimiento a lo largo de todo el ciclo de vida.
- **Calidad:** asegurar que los conjuntos de pruebas ejecutadas durante los procesos son completos suficientes para garantizar el menor impacto posible en los entornos productivos de la Compañía.
- **Cultura de control y comunicación:** fomenta la mentalidad de seguridad y cumplimiento dentro de los equipos DevOps sin frenar la innovación, estableciendo canales efectivos de comunicación e información para aplicar adecuadamente los procesos y metodologías DevOps.

Auditoría Interna ayuda a equilibrar innovación y gobernanza, apoyando al establecimiento de un control efectivo.

La clave está en contribuir desde la función de Auditoría Interna a la mejora del gobierno, gestión de riesgos y control en los procesos DevOps de manera ágil y sinérgica, añadiendo valor con su conocimiento en materia de identificación y evaluación de riesgos, así como de diseño y funcionamiento de estructuras de control interno efectivas.

Auditoría Interna debe adaptar su enfoque al revisar procesos bajo entornos DevOps.

Otros aspectos clave a tener en cuenta por Auditoría Interna respecto de la supervisión del control interno:

- Revisar la estrategia DevOps de la organización y su alineación con el apetito de riesgo definido, conforme a lo previsto en el marco ERM de COSO[5].
- Profundizar en la gestión de cambios, automatizada, especialmente en entornos ágiles donde los desarrolladores pueden tener acceso directo a producción, evaluando los controles de gestión de cambios.
- Revisar periódicamente las herramientas DevOps para asegurar su integridad y correcto funcionamiento, y el cumplimiento con los criterios de disponibilidad e integridad del procesamiento.
- Asesorar en la implementación de capacidades de monitorización continua que permitan la evaluación en tiempo real de controles y el monitoreo de indicadores de riesgo clave.

Evolución del enfoque de Auditoría Interna

Aunque la función de Auditoría Interna no cambia, sí debe adaptar su enfoque a la hora de realizar revisiones en entornos DevOps. Es importante revisar cómo se gestionan los permisos, cómo se registran los cambios y cómo se controlan los riesgos en procesos automáticos.

Auditoría Interna se configura como una función que aporta valor, en primera instancia, a través de actividades de asesoramiento sobre los procesos de identificación y evaluación de riesgos, tanto en los aspectos estratégicos del proyecto, como en la incorporación de estructuras de control interno efectivas y, en segunda instancia puede plantear la realización de auditorías de manera integrada con el proyecto, sobre el diseño de las estructuras de control interno, con la emisión de conclusiones de auditoría a la finalización del proyecto. Esta auditoría deberá estar planificada y ejecutada cumpliendo con los estándares establecidos por las *Normas Globales de Auditoría Interna™*.

En este sentido, además de evaluar específicamente las estructuras de control interno desarrolladas, se podrá evaluar la gobernanza y gestión de riesgos de las prácticas en la aplicación de los procesos y metodologías de DevOps.

PROPUESTA DE PROGRAMA DE TRABAJO PARA UNA AUDITORÍA INTERNA

La adopción de prácticas DevOps, si bien impulsa la agilidad y eficiencia en el ciclo de vida del software, también introduce una serie de riesgos relacionados con la seguridad, la trazabilidad y el cumplimiento normativo. En este apartado se propone un programa de

5. *Enterprise Risk Management, Integrating with Strategy and Performance,* publicado por el *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) en 2017.

trabajo que sirva como referencia a los equipos de Auditoría Interna para la revisión de los principales aspectos de gobierno, gestión de riesgos y control interno del entorno DevOps, identificando una serie de riesgos, objetivos de control y pruebas de auditoría sobre los mismos. Este programa de trabajo contiene controles que habitualmente podrían encontrarse en contextos de ciclo de vida tradicional, si bien se han adaptado para su aplicación en entornos DevOps, y se han complementado con controles específicos para estos entornos.

Estos riesgos y controles se encuentran enmarcados en estándares reconocidos como la norma ISO 27001 y el marco NIST[6], los cuales proporcionan directrices para la gestión de la seguridad de la información y la evaluación de riesgos tecnológicos.

Por último, es importante remarcar que queda a juicio del auditor adaptar la siguiente propuesta de programa de trabajo en función del contexto auditado, omitiendo o incluyendo controles adicionales, y agregando a cada control algún tipo de criterio de valoración (cuantitativo o cualitativo) que sirva como pilar para poder medir y comparar el grado de cumplimiento, identificar deficiencias y oportunidades de mejora, ya que se considera que estos criterios son intrínsecos a cada organización.

El documento aporta una propuesta de programa de trabajo para realizar una auditoría interna en entornos DevOps.

Conclusiones: implicaciones y actividades de auditoría interna en entornos DevOps

Tal y como se ha descrito a lo largo del documento, el uso de metodologías DevOps plantea algunas ventajas e impactos significativos en las áreas de desarrollo de software y operación de sistemas de información de las organizaciones, las cuales requieren ser consideradas por la función de Auditoría Interna, de cara a planificar y desarrollar actividades dentro de este ámbito.

Para ello, el documento plantea una propuesta de programa de trabajo orientada a abordar los principales aspectos de gobierno, gestión de riesgos y controles, tales como los relacionados con la seguridad, privacidad, el cumplimiento normativo, la revisión de procesos automatizados o la evaluación de los controles de acceso a los sistemas o datos en entornos DevOps, considerando lo establecido en estándares reconocidos como la norma ISO 27001 o el marco NIST.

6. *National Institute of Standards and Technology* (https://www.nist.gov/). Este marco de ciberseguridad del NIST proporciona una guía completa y las mejores prácticas que las organizaciones del sector privado pueden seguir para mejorar la seguridad de la información y la gestión de riesgos de ciberseguridad.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: GOBIERNO	Cumplimiento	**Incumplimiento** con la legislación o regulación vigente aplicable.	Comprobar que se realiza una monitorización continua de la legislación existente para poder valorar su cumplimiento.	Comprobar que el área que sustenta el Gobierno sobre los procesos DevOps, cuenta con canales correctos y suficientes donde mantenerse informado de las legislaciones que puedan impactar en cada momento.	ISO 27001 -> Anexo A 5.31 – Requisitos legales, reglamentarios y contractuales. NIST -> SSDF, SP 800-53, DevSecOps – Integración de cumplimiento legal en procesos DevOps.
			Comprobar que la monitorización realizada sobre la legislación es completa y suficiente.	Asegurar que los canales anteriores cubren toda la geografía donde se utilizan o se implementan estos procesos.	ISO 27001 -> Anexo A.5.31 y A.18.1.1 – Legislación aplicable por ubicación. NIST -> SP 800-53 (PL-1, RA-3), SSDF – Cumplimiento normativo distribuido.
			Realizar un análisis preliminar sobre la posible legislación aplicable a la temática auditada y comprobar que toda ha sido considerada por la monitorización anterior.	Realizar una prospección de las regulaciones que puedan afectar al sector y geografías en las que se está presente, y comprobar que están cubiertas por la monitorización anterior.	ISO 27001 Cláusulas 4.1, 4.2 y A.5.31 – Análisis del contexto y requisitos legales. NIST SP 800-53 (RA-3, PM-5), SSDF – Evaluación de riesgos regulatorios.
			Comprobar el nivel de cumplimiento con la legislación aplicable existente.	En caso de que existiera alguna legislación aplicable, comprobar que se han llevado a cabo las acciones necesarias para garantizar su cumplimiento, siendo la primera y mínimamente exigible, un GAP Análisis para comprobar punto de partida.	ISO 27001 Cláusulas 6.1.3, 9.2, A.5.31 – Evaluación de cumplimiento y controles. NIST CA-2, RA-3 – Evaluación de seguridad y cumplimiento normativo.
	Modelo de gobierno	**Eficiencia y alineación con objetivos de negocio**	Existe una metodología alineada con los objetivos de la organización, que alcance a todos los stakeholders	Debería existir una metodología con roles definidos, que, si bien puede disponer de cierta flexibilidad, debe aclarar los roles de todos los participantes y ser una guía en la resolución de conflicto. Como *Nice-to-have* se puede valorar que haya indicadores o monitorización de la propia metodología.	ISO 27001 Anexo A.5.1 – Políticas para la seguridad de la información. Anexo A.6.1 – Examen en línea. NIST SP 800-53 Rev. 5 PM-1 (Information Security Program Plan), PS-2 (Position Risk Designation), CP-2 (Contingency Planning Roles).
		Un inadecuado seguimiento de la estrategia puede conllevar una **percepción errónea sobre el grado de consecución** y aporte de valor de la misma.	Revisión de la definición y monitorización de métricas y KPIs de gobierno.	Existen métricas y KPIs que permiten realizar un seguimiento del nivel de despliegue de la estrategia Devops en la compañía, así como su grado de madurez. A modo de ejemplo: - % de proyectos con DevOps formalizado: Proyectos que aplican procesos DevOps	ISO 27001 Cláusula 9.1 – Seguimiento y medición del desempeño del SGSI. NIST SP 800-53 (PM-6, CA-7, MA-6) – Métricas de desempeño, auditorías y validación.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: GOBIERNO	Modelo de gobierno			definidos vs. total de proyectos. - % de pipelines con validación automatizada: Pipelines con pruebas, escaneos, políticas de seguridad activas. - % de herramientas DevOps inventariadas y aprobadas: Herramientas que han sido registradas, evaluadas por IT y/o seguridad. - % de auditorías internas realizadas sobre pipelines críticos: Ejecución de auditorías anuales o semestrales sobre componentes críticos. - Grado de cumplimiento de políticas de cambio Cambios con documentación, pruebas y autorizaciones adecuadas.	
	Normas, políticas y procedimientos	Una normativa desactualizada puede derivar en **incumplimiento legal o desalineación con políticas internas** si no se incorporan en tiempo y forma.	Revisión del marco documental (normas, políticas y procedimientos) de aplicación al ámbito Devops y su nivel de revisión y actualización.	Marco documental revisado y actualizado al menos una vez al año.	ISO 27001 Cláusula 7.5 – Control de la información documentada; A.5.1 – Políticas de seguridad. NIST SP 800-53 (PL-1, PL-2, SI-12) – Gestión y revisión de políticas y procedimientos.
	Objetivos y estrategia	Una estrategia desactualizada puede **omitir avances tecnológicos o cambios relevantes en la Compañía.**	La estrategia, objetivos y alcance de la misma está definida formalmente y revisada periódicamente.	Se establecen y actualizan periódicamente una estrategia y unos objetivos formales relacionados con Devops en línea con los objetivos de negocio de la compañía y los cambios tecnológicos.	ISO 27001 Cláusula 6.2 – Objetivos de seguridad de la información; Cláusula 5.1 – Liderazgo y alineación con objetivos estratégicos NIST SP 800-53 (PM-1, PM-8) – Planificación estratégica y alineación con objetivos de misión.
	Roles y responsabilidades	**Funciones no asignadas o de roles que acumulen funciones incompatibles entre sí.**	Verificar si están definidos los roles clave (desarrollador, Operaciones, Release Manager, Product Owner, DevSecOps, Scrum Master, Security Champion, entre otros) y sus funciones asignadas.	Matriz definida según el modelo de gestión de responsabilidades (RACI, RASCI, DACI, RAPID, etc.) con roles formalmente definidos y sin solapamientos entre ellos.	ISO 27001 Anexo A.5.2, Cláusula 5.3 – Roles y responsabilidades definidos. NIST CSF, PM-1, CA-1 – Asignación de funciones y responsabilidades.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: GOBIERNO	Roles y responsabilidades	**Funciones no realizadas o acumulación de funciones** en la misma persona o rol que resulten incompatibles.	Verificar que operativamente se está siguiendo el modelo de roles y responsabilidades definido, mediante la comprobación de que las actividades asociadas a cada función están realizadas por las personas / grupos asignados a ese rol.	Existe una correspondencia entre actividades operativas y roles que las ejecutan. Ejemplos: los cambios a producción de código se realizan por roles de operaciones, existen aprobaciones por el Product Owner de los requisitos funcionales en cada sprint, etc.	ISO 27001 Anexo A.5.2 – Roles y responsabilidades de seguridad de la información. NIST SP 800-53 (AC-5, AC-6), CSF – Separación de funciones y asignación de tareas.
	Gestión de Proveedores	**Calidad y seguridad del servicio no percibida.** Una falta de monitorización y correcta gestión de los proveedores puede conllevar un servicio de calidad inferior a la contratada, incluidos riesgos de seguridad en el desarrollo.	Procesos de gobierno de terceros.	Existen procesos que permiten para los terceros participantes en los diferentes procesos Devops, una adecuada alineación tecnológica y metodológica, visibilidad y control de sus actividades, SLAs técnicos propios de metodologías DevOps y una continuidad operativa y gestión del conocimiento. - Evaluación de criterios técnicos utilizados para la selección de terceros - Análisis de contratos y SLA en relación con prácticas CI/CD, IaC y seguridad - Evidencia de seguimiento y evaluación periódica del desempeño técnico de los terceros.	ISO 27001 Anexo A.15.1.1 – Política de Seguridad de la Información para las Relaciones con Proveedores.
ÁREA: RIESGOS	Definición de perfil de riesgo	**Falta de integración entre perfiles de riesgo con pipelines CI/CD implementados.** El comportamiento de los flujos de despliegue no responden a los puntos críticos identificados en las valoraciones riesgo.	Las aplicaciones se clasifican en función de su relevancia para el negocio.	Existe una clasificación de aplicaciones acorde con el riesgo de negocio basado en un set de preguntas simples y predefinidas.	ISO 27001 A.5.12 – Clasificación de la información; A.5.8 – Evaluación de riesgos de seguridad de la información. NIST SP 800-53 (RA-2, RA-3) – Evaluación de riesgos y categorización de sistemas.
	Evaluación de perfil de riesgo	**Debilidades en la definición del perfil de riesgos.** Los perfiles de riesgos se deben adaptar a la velocidad de las implementaciones, para generar valor y facilitar la habilitación de acciones de mitigación.	Las evaluaciones se realizan de manera centralizada.	Se utilizan aplicaciones centralizadas y cuantificadas de perfiles de riesgo para evaluar el riesgo de negocio.	ISO 27001 Cláusula 6.1.2 – Evaluación de riesgos de seguridad de la información; A.5.8 – Evaluación de riesgos. NIST SP 800-53 (RA-3, RA-5) – Evaluación y respuesta al riesgo con herramientas centralizadas.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: RIESGOS	Evaluación de perfil de riesgo	**Falta de automatización para la verificación o evaluación del riesgo.** Es necesario mantener un perfil de riesgo que refleje la realidad operativa y que esté alimentado con datos. Por ejemplo, de las actividades ejecutadas el flujo de despliegue.	Las evaluaciones se realizan de manera centralizada y con la periodicidad suficiente teniendo en cuenta los cambios en el entorno.	Se realizan regularmente actualizaciones y revisiones del perfil de riesgo de las aplicaciones.	ISO 27001 Cláusula 6.1.2 – Evaluación continua de riesgos; A.8.8 – Revisión periódica de riesgos. NIST SP 800-53 (RA-3, RA-6) – Reevaluación periódica del riesgo y ajustes en controles.
ÁREA: CONTROL INTERNO	Operación	**Falta de observabilidad.** La ausencia de monitoreo o la sobre generación de alertas puede retrasar la detección de incidentes y aumentar el tiempo de recuperación.	Detección de incidentes por medio del análisis de datos de eventos.	Se realizan análisis de los data logs de incidentes de seguridad periódicamente.	ISO 27001 A.5.24 – Monitorización de seguridad; A.8.16 – Revisión de logs. NIST SP 800-53 (AU-6, IR-5) – Análisis de registros de auditoría e incidentes.
			Documentación y aplicación de un flujo aprobado para la detección de incidentes.	Se documenta y sigue un proceso de detección de incidentes.	ISO 27001 A.5.26 – Gestión de incidentes de seguridad de la información. NIST SP 800-53 (IR-4, IR-5) – Respuesta y análisis de incidentes.
		Falta de calibración de las tareas de detección. Las alertas deben estar ligadas a un impacto con el negocio para determinar su prioridad. Además, los eventos deben ser correlacionados entre las diferentes herramientas de monitoreo para garantizar cobertura y una detección oportuna.	Revisión y actualización continua del flujo de atención de incidentes.	Se realiza y actualiza el proceso de detección de incidentes de forma regular. El control puede considerar como insumo lecciones aprendidas, nuevas amenazas, cambios estratégicos y tecnológicos.	ISO 27001 A.5.26 – Gestión de incidentes de seguridad de la información (incluye revisión y mejora continua). NIST SP 800-53 (IR-4, IR-8) – Detección, revisión y mejora continua del proceso de respuesta a incidentes.
		Falta de oportunidad en la respuesta del incidente. Los retrasos pueden aumentar el impacto a las operaciones o al negocio, para esto es posible automatizar la respuesta a ciertos tipos de eventos ya conocidos o identificados.	Implementación de tareas para respuesta a los incidentes cuando estos ocurren.	Se responde a los incidentes de manera oportuna.	ISO 27001 A.5.26 – Gestión de incidentes de seguridad de la información. NIST SP 800-53 (IR-4, IR-5, IR-6) – Respuesta a incidentes, análisis y corrección.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Operación	**Inadecuada trazabilidad y respuesta.** La documentación estándar permite evaluar las condiciones y respuesta de los equipos y aplicar planes de mejora para futuros eventos.	Definición de un flujo de actividades que tenga un resultado estandarizado en el momento de atender un evento adverso.	Se dispone de un proceso estandarizado para responder a los incidentes.	ISO 27001 A.5.26 – Gestión de incidentes de seguridad de la información. NIST SP 800-53 (IR-1, IR-4) – Políticas y procedimientos estandarizados de respuesta a incidentes.
		Falta de experiencia en la respuesta. Esto puede conllevar a prologar o incrementar el impacto del incidente, además, para los casos de seguridad es necesario equipos con habilidades que garanticen la mitigación de las amenazas.	Asignación de un equipo especializado que contribuya a minimizar el impacto al negocio ante un incidente.	Se dispone de un equipo especializado dedicado a la respuesta de incidentes.	ISO 27001 A.5.26 – Gestión de incidentes de seguridad de la información (incluye roles y responsabilidades). NIST SP 800-53 (IR-1, IR-4, IR-7) – Establecimiento de un equipo de respuesta a incidentes (CSIRT).
		Exposición a amenazas. La falta de integración de actividades para escanear vulnerabilidades en el pipeline CI/CD, puede conllevar a la exposición de ataques y esto a fallos en el ambiente productivo, paralización del negocio o incluso brechas de datos.	Análisis y atención de vulnerabilidades para cierre de brechas de seguridad.	Las vulnerabilidades identificadas son parcheadas o solucionadas en tiempo y forma.	ISO 27001 A.8.8 – Gestión de vulnerabilidades. NIST SP 800-53 (SI-2, SI-5) – Gestión de parches y corrección de vulnerabilidades.
		Inadecuada gestión de actualizaciones. Aplicar constantemente actualizaciones fuera del modelo de pipeline CI/CD. Por ejemplo, de manera manual, puede conllevar a problemas de gestión de versiones, errores en el ambiente productivo o afectara el objetivo de implementación continua.	Parcheo y actualizaciones sobre componentes y aplicaciones.	Se dispone de un proceso estandarizado y se sigue para actualizar componentes y aplicaciones.	ISO 27001 A.8.8 – Gestión de vulnerabilidades; A.8.26 Requisitos de seguridad de la aplicación. NIST SP 800-53 (SI-2, SI-5) – Gestión de parches y corrección de vulnerabilidades.
		Falta de cobertura o retrasos en las evaluaciones. Es necesario integrar las evaluaciones como parte del flujo, con tareas automatizadas, que conlleve a mejorar la visibilidad de toda la infraestructura e incrementar la rapidez al aplicar las evaluaciones.	Validación de parcheo y actualizaciones.	Se realizan evaluaciones regulares de los componentes y se revisa el estatus del nivel de parcheo.	ISO 27001 A.8.8 – Gestión de vulnerabilidades; A.8.16 – Revisión técnica de aplicaciones y sistemas. NIST SP 800-53 (SI-2, RA-5) – Evaluación continua de componentes y gestión de parches.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Operación	**Incidencias en el pipeline de DEVOPS.** La inadecuada gestión y control de las incidencias en el pipeline de DEVOPS puede terminar afectando al proceso de entrega e integración continua.	Se dispone de medidas adecuadas para la gestión de incidencias en el pipeline de DEVOPS, tanto a nivel operativo como tecnológico.	Es necesario asegurar la existencia de procedimientos de gestión de incidencias correctamente implementados, que describan las medidas de detección, respuesta, contingencia y recuperación existentes, la tecnología asociada, y los pasos a seguir en caso de indisponibilidad o fallos en el pipeline de DEVOPS, con el fin de minimizar la afectación las prácticas de CI/CD.	ISO 27001 Anexo A.5.25 – Evaluación y Decisión sobre Eventos de Seguridad de la Información. A.8.27 – Principios de ingeniería y arquitectura de sistemas seguros. NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide – Detección, análisis, contención, erradicación y recuperación.
		Desarrollos no controlados que afecten a la continuidad y seguridad de los sistemas.	Los entornos no productivos cuentan con medidas de seguridad adecuadas a su nivel de riesgo. Esto incluye protección de datos confidenciales y recuperación ante desastres.	Los entornos no productivos deben ser lo más homologables a los entornos finales, no ya sólo por un testing más fiable, sino que por ser un activo en sí mismo, que hay que proteger. También es necesario conocer y proteger la información sensible almacenada en entornos no productivos. La propia actividad de desarrollo debería contar con medidas de continuidad de negocio y recuperación ante desastres (backups de código fuente, recuperación de entornos de desarrollo, entornos de respaldo, pruebas de recuperación periódicas, etc.)	ISO 27001 Anexo A.8.13– Copias de seguridad. Anexo A.8.31 Separación de entornos de desarrollo, prueba y producción. Anexo A.8.25 – Ciclo de vida en desarrollo seguro. NIST SP 800-53 Rev. 5 CP-9 (Backup), CP-10 (Recovery), SA-11 (Developer Testing), SC-28 (Protection of Information at Rest).
			Existe CMDB e información clara sobre infraestructura, incluyendo una gestión formal del cambio.	Existe un inventario de configuración que se mantiene actualizado, para todos los entornos del proceso.	ISO 27001 Anexo A.5.9 – Inventario de otros activos. NIST SP 800-53 Rev. 5 CM-2 (Baseline Configuration), CM-8 (System Component Inventory), CM-9 (Configuration Management Plan).
	Herramientas	**Obsolescencia de los sistemas.** Posibilidad de que los sistemas tecnológicos, software o hardware queden desactualizados o incompatibles con las necesidades operativas, normativas o de seguridad, afectando la eficiencia, soporte y continuidad del negocio.	Existe una revisión continua de las versiones de las herramientas.	Asegurar que las herramientas utilizadas están siempre actualizadas con las últimas versiones o por lo menos contar con versiones del software que aún tengan soporte. Además, definir una periodicidad y procedimiento en el que se revisen y actualicen esas versiones.	ISO 27001 8.26 Requisitos de seguridad de la aplicación; A.8.9 – Gestión de la configuración. NIST SP 800-53 (SI-2, CM-6) – Aplicación de actualizaciones y mantenimiento de versiones soportadas.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Herramientas	**Ineficiencia en el proceso.** Eventualidad de que las actividades operativas no se ejecuten de manera óptima, generando desperdicio de recursos, retrasos o resultados de baja calidad que afectan el desempeño organizacional.	Se desarrolla un programa de formación a los usuarios de las herramientas involucradas en el proceso DevOps.	En algunos casos, hay herramientas concretas, que puede ser necesario evidenciar que el personal que las utiliza es capaz de usarlas y mantenerlas mediante algún tipo de capacitación que demuestre estos conocimientos.	ISO 27001 A.6.1 – Recursos, examen en línea; A.6.2 – Competencia. NIST SP 800-53 (AT-2, AT-3) – Formación técnica y validación de competencias.
		Integridad, confidencialidad y disponibilidad de los sistemas. Posibilidad de que los sistemas y datos sean alterados, expuestos o inaccesibles, comprometiendo la seguridad y continuidad operativa de la organización.	Se aplican mecanismos en las herramientas que aseguran la integridad de los datos guardados en ellas.	Asegurar que los datos almacenados en las herramientas no pueden ser corrompidos. Se pueden usar varios mecanismos como registros de log, integridad referenciada, validaciones automáticas en los formularios... todos ellos con el objetivo de garantizar la integridad.	ISO 27001 A.8.12 – Prevención de fuga de datos; A.5.25 – Evaluación y Decisión sobre Eventos de Seguridad de la Información; A.8.11 – Protección contra alteración de datos. NIST SP 800-53 (SI-7, AU-9) – Protección de la integridad de la información y registros de auditoría.
			Realizar algún tipo de actuación para la búsqueda de posibles fugas o vulnerabilidades en las herramientas.	Implementación de procesos y herramientas que permiten identificar, evaluar y priorizar debilidades de seguridad en sistemas o aplicaciones. Por ejemplo, mediante Pentesting, revisión de librerías, revisión de configuraciones inseguras.	ISO 27001 A.5.9 – Inventario de información y otros activos asociados; A.8.8 Gestión de Vulnerabilidades Técnicas; A.8.16 – Revisión técnica de aplicaciones. NIST SP 800-53 (RA-5, SI-2, CA-8) – Identificación y análisis de vulnerabilidades, pruebas de seguridad.
			Existen pruebas periódicas que evalúan el rendimiento de las herramientas.	Realizar algún tipo de análisis periódico que confirme que la disponibilidad de los sistemas utilizados cumple con lo esperado para que no haya un impacto en la continuidad del negocio.	ISO 27001 A.5.29 – Resiliencia de la información; A.8.16 NIST SP 800-53 (CP-2, CP-4, AU-6) – Planes de continuidad, monitoreo de disponibilidad y análisis de logs.
		Eficiencia y alineamiento con objetivos de negocio.	Existen herramientas de gestión de cambio de software, releases, incidencias, configuración (JIRA, Kanbanize...)	Si bien el precepto de DevOps es la agilidad y la eficiencia, una herramienta (o un set de varias) de gestión, es algo que debería recomendarse. Es importante revisar que no haya actividad relevante fuera de estas herramientas.	ISO 27001 Anexo A.5.12 – Clasificación de la información. Anexo A.5.13 – Protección de registros. Anexo A.8.18 – Uso de programas de utilidad privilegiados. NIST SP 800-53 Rev. 5 AU-2 (Auditable Events), AU-6 (Audit Review, Analysis, and Reporting), CM-6 (Configuration Settings).

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Continuidad	**Incidencias en el pipeline de DEVOPS.** La inadecuada gestión y control de las incidencias en el pipeline de DEVOPS puede terminar afectando al proceso de entrega e integración continua.	Se ejecutan pruebas ante posibles escenarios de desastre que afecten al pipeline de DEVOPS, demostrando así la efectividad de las medidas implementadas.	Es necesario verificar la existencia de planes de pruebas ante potenciales escenarios de desastre que afecten al pipeline de DEVOPS. En los resultados de estas pruebas debe quedar demostrado que los valores de continuidad asignados por la organización a los sistemas involucrados se están satisfaciendo, tales como RTO y RPO. La tipología de pruebas puede ser desde aquellas más teóricas (Tabletop o Walkthrough), hasta aquellas más técnicas que supongan una interrupción del servicio de forma controlada.	ISO 27001 Anexo A.5.30 – Preparación de las TIC para la continuidad del negocio. Anexo A.5.29 – Seguridad de la información durante la disrupción. NIST SP 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems – Pruebas de recuperación, RTO/RPO, tabletop y técnicas.
		Medidas de rollback insuficientes dentro del entorno DEVOPS. La falta de medidas de rollback sobre el entorno DEVOPS puede afectar a la recuperación del mismo en caso de cambios/modificaciones erróneas.	Se dispone de procedimientos de rollback debidamente implementados que permitan restaurar los sistemas a un estado anterior funcional en caso de error.	Debe comprobarse que los procedimientos de rollback necesarios existen, están debidamente implementados y operativos, con el fin de garantizar la continuidad de las actividades DEVOPS en caso de cambios o desarrollos erróneos.	ISO 27001 Anexo A.8.32 – Gestión de cambios. Anexo A.5.30 – Preparación de las TIC para la continuidad del negocio. NIST SP 800-53 Rev. 5 CM-3 (Configuration Change Control), CP-2 (Contingency Plan), CP-10 (System Recovery and Reconstitution).
		Medidas de respaldo insuficientes dentro del entorno DEVOPS. La falta de medidas de respaldo sobre los activos que componen el entorno DEVOPS puede afectar a su recuperación en caso de incidente.	Se realizan pruebas periódicas sobre las copias de seguridad, asegurando su efectividad para recuperar los sistemas en tiempo y forma.	Es necesario verificar la existencia de pruebas específicas sobre las copias de seguridad que demuestre su integridad, su disponibilidad y su correcto funcionamiento, permitiendo satisfaces los valores de continuidad establecidos por la organización, tales como RPO y RTO.	ISO 27001 Anexo A.8.13 – Copias de seguridad (incluye verificación de restauración y pruebas de integridad). NIST SP 800-53 Rev. 5 CP-9 (Backup) y CP-10 (System Recovery and Reconstitution) – Requiere pruebas periódicas de restauración y validación de backups.
			Se realizan copias de seguridad en todo el entorno DEVOPS de manera periódica, de acuerdo con las necesidades de la organización.	Debe asegurarse la existencia de copias de seguridad ejecutadas con la periodicidad necesaria para todos los activos involucrados en el entorno DEVOPS. Estas copias de seguridad deben ser tanto a nivel de código como de sistema.	ISO 27001 Anexo A.8.13 – Copias de seguridad. NIST SP 800-53 Rev. 5 CP-9 (Backup) – Requiere copias de seguridad de información y sistemas críticos, incluyendo automatización y pruebas de restauración.

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Desarrollo y despliegue	**Desarrollos no controlados** que afecten a la continuidad y seguridad de los sistemas.	Existen normativas o procedimientos de desarrollo y operación seguros, que se aplican en todo el proceso: desde el desarrollo, testing en entornos de prueba hasta en operación.	Existen normativas a cumplir por los aplicativos, tanto en su etapa de desarrollo, como en su fase de operación. La propia actividad de desarrollo debería contar con medidas y controles de ciberseguridad (protección de repositorios de código, pentesting, revisión de versionado de código, etc.)	ISO 27001 Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.8.28 – Protección de código fuente y control de cambios. NIST SP 800-53 Rev. 5 SA-11 (Developer Testing and Evaluation), CM-5 (Access Restrictions for Change), RA-5 (Vulnerability Scanning).
			Existe una segregación de funciones que describa las responsabilidades de negocio, desarrollo, despliegue, modificación de infraestructura, capacidad de resolución de incidentes, etc. Se identifican las situaciones excepcionales de emergencia (usuarios tipo firefighter).	Si bien DevOps promueve la eficiencia mediante una alta coordinación de actividades de desarrollo y operación, en ocasiones esto puede suponer un conflicto de intereses, sobre todo a la hora de alinear desarrollo, transportes y correctivos. Una correcta segregación de funciones (SoD) con perfiles claros debería ser un producto disponible. Se deben analizar los flujos de aprobación definidos para los desarrollos y cambios en función de su criticidad que aseguren esa segregación de funciones, comprobando que existe segregación entre el desarrollador y el aprobador. Deberían identificarse, como mínimo, las siguientes actividades: - Desarrollar/customizar nuevas funcionalidades. - Modificar configuración de infraestructura. - Resolución de incidencias. Esto puede suponer un conflicto de intereses o un riesgo de seguridad (confidencialidad, integridad...) por lo que estos conflictos deben identificarse, así como controles mitigantes (por ejemplo: usuarios de resolución de incidencias desactivados salvo emergencia, control de cambios en CMDB, logs de acceso....).	ISO 27001 Anexo A.8.3 – Segregación de funciones: separación de tareas y responsabilidades para evitar conflictos de interés y errores. NIST SP 800-53 Rev. 5 AC-5 (Segregation of Duties), CM-3 (Configuration Change Control), PL-2 (System and Communications Protection Policy).

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Desarrollo y despliegue	**Desarrollos no controlados** que afecten a la continuidad y seguridad de los sistemas.	Existen pruebas automáticas de calidad de código.	Existen diversas herramientas orientadas a garantizar una buena codificación, que deberían emplearse, sobre todo en entornos de equipos cambiantes y/o alta complejidad de código. Los workflows de desarrollo deben garantizar que estas pruebas se ejecutan. Analizar los informes disponibles sobre las pruebas realizadas y el flujo de reporte de estos resultados a los equipos involucrados.	ISO 27001 Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.8.26 – Revisión técnica del código y validación de seguridad. NIST SP 800-53 Rev. 5 SA-11 (Developer Testing and Evaluation), SA-15 (Development Process, Standards, and Tools) – Uso de herramientas seguras y revisión automatizada de código.
			Existen pruebas integradas de caja negra y caja blanca.	Existen pruebas funcionales y técnicas completas, que incluyen tanto la funcionalidad, como el impacto de la implementación en el entorno: - Pruebas de caja negra: persiguen realizar muestras que validen que, ante unas entradas, el objeto probado produce resultados deseados, tanto en formato como funcionalidad. - Pruebas de caja blanca: persiguen controlar que la ejecución interna del objeto probado es la deseada, que todas las posibilidades de ejecución son tomadas en cuenta (gestión de excepciones), que el software se ejecuta de manera eficiente y que responde a los inputs funcionales deseados (evitar efecto 'Mago de Oz') Se han definido umbrales a partir de los cuales se bloquea el despliegue al considerarse no seguro, no apto para el entorno o sin la calidad funcional necesaria.	ISO 27001 Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.8.26 – Revisión técnica del código y validación de seguridad. NIST SP 800-53 Rev. 5 SA-11 (Developer Testing and Evaluation), RA-5 (Vulnerability Scanning), SI-2 (Flaw Remediation).
			Existen pruebas de requisitos no funcionales (rendimiento, disponibilidad, continuidad), o al menos, análisis de impacto.	Se evalúa si un cambio o desarrollo supone un impacto no funcional sobre el entorno, y se prueba en caso de ser necesario. Adicionalmente, se realizan pruebas no funcionales periódicas o a demanda sobre diversos requisitos no funcionales (tiempo de respuesta, prueba de carga, recuperación de backups...).	ISO 27001 Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.5.30 – Continuidad del negocio. NIST SP 800-53 Rev. 5 SA-11 (Developer Testing and Evaluation), CP-10 (System Recovery and Reconstitution), PE-20 (Asset Monitoring).

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Desarrollo y despliegue	**Desarrollos no controlados** que afecten a la continuidad y seguridad de los sistemas.		No todos los requisitos no funcionales pueden ser probados, o el nivel de oportunidad de su prueba puede ser bajo (por coste/beneficio). Debe tener como criterio la propia naturaleza del sistema, los requisitos funcionales a los que da respuesta y el propio apetito de riesgo de la organización. Los requisitos funcionales con mayor oportunidad suelen ser: pentests, UATs enfocados en probar la Segregación de funciones, performance del entorno (incluyendo pruebas de carga), elementos de monitorización del entorno (indicadores de disponibilidad, consumo de recursos, alertas de performance o seguridad, etc.), backups, etc. En aquellos sistemas con requisitos de continuidad altos se debe valorar realizar test en los entornos de recuperación homólogos a los realizados en el entorno principal.	
			El entorno último de pruebas es homologable al de producción.	Los entornos no productivos deben ser lo más homologables a los entornos finales, minimizando las incidencias relacionadas con configuración. Se debe valorar si debe copiarse el entorno de producción en un entorno no productivo de manera periódica, analizando la necesidad de enmascaramiento de datos en base a su sensibilidad y/o confidencialidad. El nivel de control debe estar alineado al riesgo de estos entornos. Ejemplos: -En sistemas con time-to-market muy reducidos se debe valorar el performance de estos entornos. -En entornos con datos sensibles, pero que por funcionalidad el enmascaramiento supone un riesgo funcional (ejemplos: sistemas de nóminas, o sistemas con datos de facturación de clientes, que necesitan ser validados con datos reales), se debería disponer de controles adicionales de confidencialidad y control de permisos y segregación de funciones dedicados.	ISO 27001 Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.5.30 – Continuidad del negocio. Anexo A.8.32 – Gestión de cambios. NIST SP 800-53 Rev. 5 SA-10 (Developer Configuration Management), CM-2 (Baseline Configuration), CP-10 (System Recovery and Reconstitution).

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Desarrollo y despliegue	**Incidencias en el pipeline de DEV-OPS,** que afecte a la entrega e integración continua	El desarrollo y el soporte (incidencias) deben, en la medida de lo posible, evitar impactarse mutuamente.	Si bien puede resultar un nice-to-have en muchas organizaciones, cabe analizar la dedicación de recursos a la gestión de incidencias de manera que impacten lo menos posible en el desarrollo de las release de historias de usuario, especialmente de aquellas de alta criticidad. En caso de que el soporte a incidencias y el desarrollo de nuevas funcionalidades (o mantenimiento de las existentes) compartan el mismo pool de recursos, se sugiere que se haga una monitorización del nivel de dedicación de los equipos a ambas actividades, así como de su performance. Por último, es una buena práctica monitorizar una correcta catalogación del nivel de oportunidad de todas las tareas (urgencia e impacto), que permita una correcta priorización a la hora de conseguir los objetivos de la organización (es habitual que un entorno con alto nivel de incidencias tenga desalineamiento con los objetivos de negocio y priorice la solución de dichas incidencias).	ISO 27001 Anexo A.8.21 – Gestión de incidentes de ciberseguridad. Anexo A.5.30 – Continuidad del negocio. NIST SP 800-53 Rev. 5 IR-4 (Incident Handling), CP-2 (Contingency Planning), IR-8 (Incident Response Plan Testing) – Minimización del impacto operativo de incidentes.
		Desarrollos no controlados que afecten a la continuidad y seguridad de los sistemas.	Debe existir una metodología de transportes, formal o informal, que incluya al menos: - validación de las pruebas - transportar todos los elementos impactados, incluyendo código, ficheros de configuración y otros cambios.	Los transportes deben validarse (salvo situaciones de emergencia), y deben incluir toda la información necesaria (código, configuración, datos). Asimismo, se debe valorar la potencial segregación de funciones con actividades de desarrollo y resolución de incidentes, poniendo especial énfasis en situaciones en las cuales un desarrollador tenga la capacidad de transportar sus propios cambios. Se debe comprobar que los cambios están documentados y versionados y pueden ser trazados. Por último, se debe valorar el impacto de los transportes (con o sin parada de servicio, periódicos o a demanda) dentro del apetito de riesgo de la organización.	ISO 27001 Anexo A.8.32 – Gestión de cambios. Anexo A.8.3 – Segregación de funciones. Anexo A.8.28 – Protección del código fuente y control de cambios. NIST SP 800-53 Rev. 5 CM-3 (Configuration Change Control), AC-5 (Segregation of Duties), AU-2 (Auditable Events), SA-10 (Developer Configuration Management).
		Incidencias en el pipeline de DEV-OPS, que afecte a la entrega e integración continua.	Se monitoriza el proceso de desarrollo, según aplicabilidad, de los aspectos relevantes de desarrollo y operación. Las métricas se emplean como input en la gestión de riesgos y en la gestión de problemas.	Se deben valorar todos los aspectos relevantes a monitorizar, de acuerdo con las necesidades de la organización. Según el riesgo inherente, se deben mitigar mediante monitorización aquellos aspectos más probables o de mayor impacto. Algunos potenciales aspectos de seguimiento pueden ser: - Time-to-market (tiempo entre backlog y puesta a producción). - Capacidad y recursos de desarrollo (workforce). En base a puntos de historia/tareas. - Tiempo en cada estado (Backlog, On-Going, Testing...). - Testing y calidad de código. - Incidencias y correctivos. - Valor de negocio (cambios funcionales vs cambios puramente técnicos).	ISO 27001 Anexo A.8.32 – Gestión de cambios. Anexo A.8.3 – Segregación de funciones. Anexo A.8.28 – Protección del código fuente y control de cambios. NIST SP 800-53 Rev. 5 CM-3 (Configuration Change Control), AC-5 (Segregation of Duties), AU-2 (Auditable Events), SA-10 (Developer Configuration Management).

	SUBÁREA	RIESGO	OBJETIVO DE CONTROL	PRUEBA DE AUDITORÍA	GUÍA NORMATIVA
ÁREA: CONTROL INTERNO	Desarrollo y despliegue	**Incidencias en el pipeline de DEV-OPS,** que afecte a la entrega e integración continua	Existen controles de aplicación automáticos (con alertas de distinta naturaleza: ciber, errores, métricas de performance, etc).	En aquellos casos donde es posible y rentable, se puede valorar incluir controles de aplicación (ITACs) automáticos. Esto sobre todo es especialmente interesante en entornos sujetos a regulación y/o auditoría financiera. Algunos ejemplos de ITACs: - Log de acciones de usuarios administradores (con posible alerta de actividad) - Log de bajas y altas del sistema con cambio/ticket asociado - Log de aprobaciones de transporte - Recertificaciones de usuarios - Aprobaciones de workflows. Etc.	ISO 27001 Anexo A.8.32 – Gestión de cambios. Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.8.16 – Registro de actividades del sistema. NIST SP 800-53 Rev. 5 AU-2 (Auditable Events), AU-6 (Audit Review), SA-11 (Developer Testing and Evaluation), AC-3 (Access Enforcement).
		Despliegues ineficientes que provocan pérdida de disponibilidad y sobre trabajo de los equipos de desarrollo.	Existe monitorización y controles de la calidad de los despliegues.	Existen controles post-Despliegue que garanticen el correcto funcionamiento del despliegue en términos de disponibilidad, rendimiento y operatividad. Para ello se pueden usar métricas del estilo: 1. (Número de Rolbacks + Número de Fix Releases) /Número total de despliegues. 2. Tiempo de indisponibilidad Post Despliegue.	ISO 27001 Anexo A.8.32 – Gestión de cambios. Anexo A.8.25 – Seguridad en procesos de desarrollo. Anexo A.8.15 – Registro de actividades del sistema. Anexo A.5.11 - Disponibilidad de la información. NIST SP 800-53 Rev. 5 CM-3(Configuration Change Control), IR-4 (Incident handling), SA-11 (Developer Testing and Evaluation), CA-7 (Continuous Monitoring).

Bibliografía

ARTÍCULOS Y/O PUBLICACIONES WEB

- *Acerca de la implementación continua con Acciones de GitHub.* Github.com, 5 de octubre de 2021. https://docs.github.com/es/actions/concepts/overview/about-continuous-deployment-with-github-actions
- **Améndola, Mauricio.** *DevOps.* Openwebinars.net, 19 de agosto de 2022. https://openwebinars.net/blog/top-herramientas-devops-integracion-y-despliegue-continuo/.
- *Implementación DevOps en entornos OT (industriales): Cómo DevOps facilita la automatización escalable en los sistemas industriales modernos* | *Controles 6G y Does DevOps have a place in OT/ICS Development?* | Nexus.
- *CI/CD: Tu guía para la integración continua y la entrega continua*. Getguru.com, 19 de junio de 2025. https://www.getguru.com/es/reference/cicd.
- **Comella-Dorda, Santiago, et al.** *Agile, Reliable, Secure, Compliant IT: Fulfilling the Promise of DevSecOps.* Mckinsey.com, McKinsey & Company, 21 de mayo de 2020. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/agile-reliable-secure-compliant-it-fulfilling-the-promise-of-devsecops.
- *La automatización: qué es y sus ventajas.* Redhat.com, 20 de septiembre de 2023. https://www.redhat.com/es/topics/automation.
- *Automatización en DevOps.* Nivelics.com, 18 de febrero de 2025. https://www.nivelics.com/blog/automatizacion-devops-herramientas.
- **Pfeiffer, Mike.** *12 KPI de DevOps que debe seguir para medir las mejoras.* ComputerWeekly.es, TechTarget, 26 de noviembre de 2019. https://www.computerweekly.com/es/consejo/12-KPI-de-DevOps-que-debe-seguir-para-medir-las-mejoras.
- *¿Qué es el despliegue continuo?* Ibm.com, 13 de julio de 2023. https://www.ibm.com/es-es/topics/continuous-deployment.
- **ShiftLeft.** *How to Achieve DevSecOps Maturity* | *Shannon Lietz @ Secure Software Summit 2022.* Youtube.com https://www.youtube.com/watch?v=2kO3xldZ3Sg.
- **Taylor, David.** *Las 15 mejores herramientas de CI/CD (2025).* Guru99.com, 2 de mayo de 2025. https://www.guru99.com/es/top-20-continuous-integration-tools.html.
- **Vaghela, Ena.** *Top 12 DevOps Metrics & Key Performance Indicators (KPIs) to Track.* DEV Community, 5 de septiembre de 2024. https://dev.to/enna/top-12-devops-metrics-key-performance-indicators-kpis-to-track-p10.
- **Hall, Tom.** *4 métricas clave de DevOps.* Atlassian.com, 16 de diciembre 2020. https://www.atlassian.com/es/devops/frameworks/devops-metrics.
- **Rehkopf, Max.** *Herramientas de integración continua.* Atlassian.com, 4 de mayo de 2021. https://www.atlassian.com/es/continuous-delivery/continuous-integration/tools.
- *OWASP - Seguridad en la web.* Ciberseguridad.com, 24 de enero de 2020. https://ciberseguridad.com/guias/desarrollo-seguro/owasp/.
- *Threat Modeling in Practice.* Owasp.org, 5 de agosto de 2023. https://devguide.owasp.org/en/04-design/01-threat-modeling/01-threat-modeling/.

NORMATIVAS Y/O ESTÁNDARES

- **Organización Internacional de Normalización:** *ISO27001:2022 Information security, cybersecurity and privacy protection.*
- **National Institute of Standard and Technology:** *NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.*
- **Normas Globales de Auditoría Interna™,** publicadas por el Instituto de Auditores Internos.

Instituto de Auditores Internos de España

Santa Cruz de Marcenado, 33 · 28015 Madrid · Tel.: 91 593 23 45 · Fax: 91 593 29 32 · www.auditoresinternos.es

ISBN: 979-13-991286-1-1

Maquetación: desdecero, estudio gráfico

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

AUDITORÍA INTERNA DE LA INTELIGENCIA ARTIFICIAL APLICADA A PROCESOS DE NEGOCIO (ACTUALIZACIÓN 2024)

El documento aborda múltiples aspectos relacionados con el uso de Inteligencia Artificial (IA) por las empresas en sus procesos de negocio. Desde la regulación, a principales modelos y tipologías, el marco de control interno y procedimientos para llevar a cabo una auditoría interna. Esta nueva versión incluye como novedad la incorporación de la perspectiva de la Inteligencia Artificial generativa.

AUDITORÍA INTERNA Y GESTIÓN OPERATIVA DEL CLOUD

Los servicios en la nube ofrecen ventajas, pero también implica la evaluación y mitigación de los riesgos asociados a esta tecnología. A través de este documento de la Fábrica del Pensamiento, se facilita una guía útil y práctica para la realización de revisiones de los entornos Cloud por parte de Auditoría Interna, ayudando a afrontar los retos que supone la revisión de esta tecnología, como parte del proceso de transformación digital de las organizaciones.

AUDITORÍA INTERNA DEL RIESGO REPUTACIONAL

Este documento resalta el papel clave de la función de Auditoría Interna en la empresa familiar para asegurar su continuidad y el buen gobierno. Aborda la cultura organizativa, el marco normativo y los principales retos, ofreciendo herramientas como un autodiagnóstico y un modelo de madurez. Subraya la independencia y adaptación metodológica de Auditoría Interna y recomienda su posicionamiento como aliado estratégico en la consolidación del legado familiar y en la profesionalización de las compañías.

AUDITORÍA INTERNA EN LA EMPRESA FAMILIAR

Auditoría Interna juega un papel clave para asegurar la continuidad y el buen gobierno en la empresa familiar. Este documento aborda la cultura organizativa, el marco normativo y los principales retos, ofreciendo herramientas como un autodiagnóstico y un modelo de madurez. Subraya la independencia y adaptación metodológica de Auditoría Interna y recomienda su posicionamiento como aliado estratégico en la consolidación del legado familiar y en la profesionalización de las compañías.

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Este documento describe el contexto y beneficios del uso de la metodología DevOps y el papel de Auditoría Interna de cara a la supervisión de los procesos de gobierno, gestión de riesgos y control en este ámbito, conforme a lo previsto en los principales marcos de referencia.

Instituto de Auditores Internos de España

The Institute of Internal Auditors