

A U D I T O R Í A I N T E R N A



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Auditoría Interna de los procesos robotizados de negocio



The Institute of
Internal Auditors

Instituto de
Audidores 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



BUENAS PRÁCTICAS EN GESTIÓN DE RIESGOS



OBSERVATORIO SECTORIAL



PRÁCTICAS DE BUEN GOBIERNO

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 de los procesos robotizados de negocio

Noviembre 2022

MIEMBROS DE LA COMISIÓN TÉCNICA

COORDINACIÓN:

Iván Casacuberta Prat, CIA, CISA, CISM, CISSP, CCSP, CDPP. CAIXABANK.

Álvaro Arjona Canas, Doctor, EMBA, CIA, RPA Badge, Digital Acumen Badge. PWC.

David Eraso Giménez, COSO CI, COSO ERM. DELOITTE.

Javier Garate Arana, CISA. MAPFRE.

Antonio García González, CISA, COSO CI, CET-IA. REPSOL.

Eduardo Martínez Peña. IBERDROLA.

Raquel Pilares Gutiérrez, TEAI. AEDAS HOMES.

Jorge Puente Beltrán, CISA, CRISC, CDPSE. BBVA.

Daniel Rodríguez Jiménez. EY.

Carlos Romero Barrionuevo, CIA, CISA. TELEFÓNICA.



La reciente y creciente incorporación de tecnologías para la automatización de procesos de negocio ha supuesto la aparición de importantes ventajas y beneficios en diferentes campos dentro de las organizaciones: desde el incremento de la eficiencia de las operaciones, hasta una reducción significativa de ciertos costes, pasando por la disminución o eliminación de la manualidad de procesos clave para el negocio. Todo ello hace que cada vez sea más habitual la presencia de elementos robóticos, en sus diferentes versiones, en el día a día de nuestras compañías.

Al surgimiento de estas ventajas y beneficios se les une la aparición de amenazas y situaciones de riesgo que van ligadas a la adopción y uso de este tipo de tecnologías. ¿Qué papel debe jugar Auditoría Interna a lo largo del proceso de robotización de estos procesos de negocio? La respuesta dependerá, en gran medida, del nivel de madurez de la organización y del grado de adopción de estas tecnologías en su entorno.

Este documento aborda, entre otros aspectos, los tipos de robotización de procesos del negocio más frecuentes, así como los diferentes roles que puede asumir Auditoría Interna (aseguramiento y asesoramiento) frente a una tecnología que está cada vez más presente en las operativas corporativas.

Asimismo, los autores del documento tratan los diferentes trabajos que Auditoría Interna puede asumir para garantizar que los riesgos vinculados a estas tecnologías quedan cubiertos, de cara a proporcionar confort a los órganos de gobierno y alta dirección de nuestras organizaciones.

Todos estos elementos, a los que se suma una propuesta de cómo llevar a cabo la revisión de los principales riesgos presentes en los procesos con diferentes grados de robotización, hacen de este documento una referencia imprescindible para los auditores internos que tengan que afrontar trabajos en este campo.



Índice

MODELO DE ROBOTIZACIÓN DE PROCESOS	06
ENFOQUES Y TÉCNICAS DE REVISIÓN PARA AUDITAR PROCESOS ROBOTIZADOS	08
Enfoque de aseguramiento	08
Enfoque de asesoramiento	11
Necesidades de conocimiento y habilidades sobre robotización en los equipos de Auditoría Interna	12
CÓMO AUDITAR LOS RIESGOS DE LOS PROCESOS ROBOTIZADOS	13
Riesgos de estrategia y gobernanza de los robots	14
Riesgos operacionales y tecnológicos de los robots	18
Riesgos de cambios y su impacto en los robots	22
Riesgos de ciberseguridad en los robots	24
Riesgos de cumplimiento normativo, legal y regulatorio de los robots	26
CONSIDERACIONES FINALES	27
BIBLIOGRAFÍA	28
ANEXO I - ESQUEMA TECNOLÓGICO Y DE SEGURIDAD EN UNA PLATAFORMA RPA / RDA	30
ANEXO II - GLOSARIO	31

La automatización de procesos tiene un crecimiento exponencial por su rapidez de implementación y la eficiencia que aporta.



Modelo de robotización de procesos

Auditoría Interna, en los últimos años, ha tenido que adaptarse a los constantes avances tecnológicos a los que se han visto sometidas las organizaciones. Estos han requerido de una evolución y puesta al día tanto de conocimientos específicos por parte de los auditores internos, como de las técnicas y metodologías utilizadas para poder ejercer la función.

Una de las tecnologías que ha estado siempre latente en la transformación que vienen sufriendo las organizaciones, es la robotización.

El concepto de robotización puede tener múltiples enfoques: desde los robots humanoides, pasando por la robotización de las cadenas de producción industrial, hasta la tipología que nos interesa en el presente documento, la robotización o automatización de procesos del negocio.

Esta tipología de robotización ha tenido un crecimiento exponencial en los últimos años. Esto se ha debido, principalmente, a que las últimas tecnologías de automatización de procesos permiten, de forma rápida y sencilla, desarrollar robots capaces de interactuar con múltiples aplicaciones y entornos tecnológicos, ofreciendo a su vez herramientas de operación para un correcto control y permitiendo hacer más eficientes los procesos que presentaban una carga manual muy elevada.

Esta tecnología está siendo implementada en múltiples contextos empresariales, y utilizan-

do distintas aproximaciones tanto para el gobierno y gestión de las automatizaciones, como soluciones tecnológicas para su implementación.

Dentro de este contexto heterogéneo, es importante destacar que, a la hora de robotizar procesos, las soluciones adoptadas se pueden agrupar en dos categorías:

RPA (Robotic Process Automation)

Se trata de procesos robotizados que se ejecutan de forma totalmente independiente y **sin la necesidad de intervención humana** ni para el control de la operación, ni para la operación del proceso. Entre ellos se pueden destacar:



RPA

- ☒ realización de cuadros y registros contables,
- ☒ análisis de peticiones estándar registradas en herramientas corporativas,
- ☒ automatizaciones de acciones de help desk (alta, baja de usuarios, restauración de contraseñas, etc.),
- ☒ ejecución de transferencias a partir de determinadas premisas,
- ☒ elaboración de cuadros de mando, etc.



RDA (Robotic Desktop Automation):

Se trata de procesos robotizados que, para poder ser ejecutados, requieren de **intervención humana en algún punto a lo largo del flujo del proceso**. Entre ellos destacan:



De los casos detallados anteriormente como RPA y RDA, se puede derivar que los procesos que resultan ser mejores candidatos a la robotización son aquellos que:

- Utilizan grandes volúmenes de información.
- Realizan tareas manuales y repetitivas de baja complejidad.
- Tienen pocas excepciones y son procesos estables.

A la vez se entiende que no es conveniente empezar la automatización de procesos con aquellos procesos que son soportados por sistemas inestables o pendientes de sustitución, o que requieren de un alto grado de interacción humana.

Como se ha mencionado anteriormente, estas tecnologías de robotización tienen **múltiples ventajas** en términos de mejora de la eficiencia (se pueden ejecutar más operaciones con muchos menos recursos) e, incluso, en términos de estandarización de las ejecuciones (un robot siempre realizará las tareas siguiendo un patrón establecido).

No obstante, también presentan **desventajas y riesgos**, que van desde el impacto organizativo que puede representar la mejora en eficiencia de recursos y la correspondiente pérdida de conocimiento de los procesos, hasta el hecho de que un error operacional de un robot (ya sea por mal funcionamiento, por acción manual intermedia malintencionada, o por cambio en el proceso no previsto por el robot) tiene un impacto potencial mucho más amplio, ya que puede ejecutar un mayor volumen de transacciones (en este caso erróneas) de forma más rápida de lo que lo podría realizar una persona. De aquí la necesidad de establecer controles (manuales o automáticos) sobre el resultado del propio proceso robotizado.

En este contexto, Auditoría Interna debe ser capaz de realizar revisiones que puedan dar confort tanto a la Alta Dirección como a los Órganos de Gobierno, sobre si la organización ha adoptado las medidas de control suficientes en los ámbitos de gobierno, operacional y tecnológico, para minimizar la potencial materialización de los riesgos asociados al empleo de los propios robots.

La automatización, ya sea RPA o RDA, utiliza grandes volúmenes de información, realiza tareas manuales y repetitivas y son procesos estables.

El éxito de un programa de robotización de procesos depende de disponer de un modelo de gobierno apropiado que incluya una estrategia de robotización general.



Enfoques y técnicas de revisión para auditar procesos robotizados

La misión de Auditoría Interna es la de mejorar y proteger el valor de las organizaciones, proporcionando aseguramiento objetivo, asesoría y conocimiento basado en riesgos.

Para poder dar cumplimiento a esta misión en los aspectos relativos a las tecnologías de robotización de procesos, se proponen dos enfoques de colaboración de la función de Audi-

toría Interna: el enfoque de aseguramiento y el de asesoramiento. La aplicación de uno u otro, o la combinación de ambos, dependerá tanto del nivel de madurez de la organización en relación con la adopción de dicha tecnología, como de los objetivos estratégicos y el marco de actuación de la función de Auditoría Interna.

ENFOQUE DE ASEGURAMIENTO

Los riesgos que se presentan tanto a lo largo de las fases del ciclo de vida de desarrollo de RPAs y RDAs (en adelante robots), como durante el seguimiento y control del proceso robotizado, no son necesariamente nuevos, siendo habitualmente una extensión de un marco típico de gestión de riesgos de tecnología y sistemas.

Se describen a continuación las posibles áreas de actuación contempladas en el ámbito del aseguramiento proporcionado por la función de Auditoría Interna.

Auditoría del gobierno y entorno tecnológico de los robots

El éxito de un programa de robotización de procesos depende de disponer de un modelo de gobierno apropiado que incluya una estra-

tegia de robotización general. En este sentido, Auditoría Interna puede promover actividades de aseguramiento en los siguientes ámbitos:

- **Definición y comunicación de roles y responsabilidades** (para la gestión y ejecución de la estrategia de automatización de la organización), del proceso de toma de decisiones, de la designación de órganos de gobierno y de administradores de robots (responsables encargados de la implementación de la estrategia de robotización de procesos) y de la definición de los mecanismos de gestión del ciclo de vida de los robots.
- **Adecuación del modelo operativo definido para los robots** (centralizado, descentralizado o híbrido), considerando factores



tales como la madurez de la capacidad de automatización de la organización, la disponibilidad de recursos, el diseño de la infraestructura de tecnología subyacente y las necesidades comunes de robotizar procesos en toda la organización.

- **Metodologías y procesos para definir el coste total** y el consiguiente valor de negocio del programa de robotización.
- **Supervisión y adecuación de la eficiencia de los recursos**, incluidas las habilidades, la capacitación y participación de las partes intervinientes, tanto internas como externas.
- **Definición de marcos de análisis del *business case* con anterioridad a la implementación de los robots** (análisis *ex-ante*). En dichos análisis se deben tomar en consideración aspectos vinculados tanto a las mejoras en eficiencia, y por lo tanto en costes de la implementación del robot, como a los distintos riesgos vinculados al *business case*, que permitan dictaminar la viabilidad de este.
- **Establecimiento de mecanismos de control y aseguramiento transversal de la fiabilidad e integridad de la operación de los robots**, a través del Modelo de las Tres Líneas.
- **Suficiencia y adecuación de los mecanismos de reporting** y generación de información sobre el marco de gobierno y gestión de robots.
- **Análisis de mecanismos de prevención, detección, comunicación y corrección de incidencias en los robots.**

- **Definición de procedimientos de identificación de aspectos de mejora continua**, tanto del programa de robotización como de los distintos robots individuales implementados. A su vez, definir mecanismos de evaluación de impacto en cuanto a la eficiencia y eficacia de los distintos robots (análisis *ex-post*).
- **Análisis** —en el entorno tecnológico que da soporte a los robots— **de las herramientas y procesos establecidos para la gestión de vulnerabilidades**, de las configuraciones de seguridad, de la gestión de accesos, de la monitorización de la actividad, de la gestión de los cambios tecnológicos, de la identificación y respuesta a incidentes, así como de los criterios de contingencia tecnológica del entorno y su alineamiento con los requerimientos de continuidad operativa de los procesos y actividades robotizadas.

Auditoría del ciclo de vida de los robots

Un modelo operativo eficiente, con procesos y controles claramente definidos y bien documentados, afecta directamente a la capacidad de una organización para abordar los riesgos que rodean la adopción de robots. En este sentido, Auditoría Interna puede promover actividades de aseguramiento en los siguientes ámbitos:

- **Procesos de selección, diseño y desarrollo de robots.**
 - Revisión de los criterios definidos de selección de actividades susceptibles de robotización y análisis de factores de impacto en procesos y categorías de riesgo existentes.

Un modelo operativo eficiente, con procesos y controles claramente definidos y documentados, permite abordar los riesgos que rodean la adopción de robots.

En el uso actual de los robots, su implementación no siempre permite cubrir un proceso de principio a fin, sino alguna tarea concreta del mismo.

- Revisión de metodología definida para la evaluación de estándares de desarrollo de robots e implementación de procesos para automatización (sistemas asociados, consideraciones éticas y de cumplimiento, implicaciones en marco de control SOX, evaluación de capacidad robótica de la organización, etc.).
 - Etapas del proceso de diseño y de desarrollo para la robotización, incluidos riesgos y controles, así como evaluación y consideración de procesos alternativos (análisis de viabilidad de *business case*).
 - Garantía de calidad técnica, revisiones de código, pruebas de demostración y pruebas de aceptación de usuario.
 - Toma de decisiones final de *Go / No-Go* para el desarrollo de robots y su pase a producción.
 - Transición a *Business-As-Usual* (BAU) y propiedad de unidad / función de negocio.
- **Análisis funcional y técnico.**
 - Monitorización continua tanto del entorno tecnológico que da soporte a los robots, como de la operación de estos (monitorización detallada de la ejecución).
 - Seguimiento de la información de gestión sobre el uso de los robots, tales como indicadores clave de rendimiento y de riesgo (KPIs y KRIs) sobre su utilización, incidentes y problemas.
 - Revisión periódica de los robots implementados en lo relativo, entre otros aspectos, a algoritmos y códigos, medidas de seguridad y robustez, eficacia y eficiencia. Todo ello considerando las reglas de diseño y funcionamiento esperadas inicialmente.
 - **Gestión de cambios de los robots, incluido el repositorio de código, el manual de soporte y los controles del historial de versiones.**
 - **Seguridad de acceso.**
 - Políticas y procedimientos de acceso de usuarios: autenticación, autorización, revocación, adecuación y revisión de acceso de usuarios.
 - Cuentas con derechos de acceso elevados.
 - Uso y seguimiento de las cuentas genéricas / servicio de la aplicación.
 - Cumplimiento de las normas de privacidad de datos, incluidos los requisitos del RGPD, tanto a nivel interno como de terceros (en su caso).
 - Segregación de funciones de controles sobre ámbitos tecnológicos sensibles (desarrollo e implementación de los robots en el entorno real, etc.).

Auditoría de procesos afectados por los robots

El uso actual de los robots implica que su implementación, en muchas ocasiones, no permite cubrir un proceso de principio a fin, sino que únicamente es posible robotizar alguna actividad dentro de dicho proceso. Desde Auditoría Interna es habitual realizar revisiones de procesos en su totalidad. En este sentido, si un proceso dispone de parte de sus actividades robotizadas, el enfoque de la revisión no debe ser distinto del enfoque tradicional de llevar a cabo la auditoría de un proceso



completo. No obstante, para las actividades robotizadas presentes en esas partes del proceso, deberán tenerse en consideración los siguientes aspectos:

- **Sesiones de entendimiento para comprender completamente el proceso (o partes)** recién robotizado, mediante la revisión de los siguientes atributos:
 - El documento de definición de la actividad/ proceso robotizado.
 - El documento de diseño de la solución (SDD).
 - Y cualquier otra documentación que se haya creada durante la fase de diseño de la robotización.
- **Entendimiento de los riesgos y mecanismos de control** definidos en cada actividad/proceso robotizado y el grado de formalización, formación y comunicación de aquellos.

ENFOQUE DE ASESORAMIENTO

Si las organizaciones se encuentran en fases exploratorias de adopción de tecnologías de robotización de procesos, las funciones de Auditoría Interna deberían valorar involucrarse durante la fase previa a la implementación de la robotización. Algunas consideraciones para tener en cuenta por parte de los departamentos de Auditoría Interna en este sentido incluyen:

- Asesorar a la organización sobre su capacidad para dar cuenta de los factores de riesgo involucrados en dicho proceso.
- Proporcionar orientación sobre prácticas líderes para impulsar un mayor rendimiento

- **Evaluación del diseño de los mecanismos de control implementados** para mitigar los riesgos anteriormente identificados, en base a los siguientes criterios:

- Adecuación del propósito del control y su correlación con el riesgo vinculado.
- Competencia y autoridad de las personas que ejecutan y supervisan el control objeto de revisión.
- Frecuencia y consistencia con la que se realiza el control.
- Nivel de agregación y previsibilidad.
- Criterios de investigación y proceso de seguimiento.

- **Evaluación de la eficacia operativa**, desarrollando programas de auditoría sobre dichos controles con un enfoque continuo o rotatorio, y en base a riesgo, para dar seguridad sobre la fiabilidad de las operaciones.

y valor de las tecnologías de robotización de procesos.

- Elevar el perfil de Auditoría Interna, demostrando conocimiento sobre el tema, a la par que se mantiene la objetividad e independencia de su actividad.

Se describen a continuación posibles áreas y ámbitos de asesoramiento de la función de Auditoría Interna.

- **Análisis de riesgos para la adaptación del proceso continuo de evaluación de riesgos** de la organización, que incluyan nue-

Las empresas que estén explorando la robotización de procesos deberían valorar involucrar a Auditoría Interna en la fase previa a la implementación.

Auditoría Interna debe revisar los requerimientos de seguridad desde la fase de diseño para verificar que se preserve la privacidad de los datos.

vos factores de riesgo dentro de las categorías tradicionales, tales como (entre otros):

- **operacionales**, creando un riesgo de concentración y puede incrementarse la dificultad de recuperación ante desastres;
 - **organizativos**, la capacitación y el desarrollo pueden quedar rezagados con respecto a la tecnología y mantener los niveles de talento especializado puede ser un desafío;
 - **tecnológicos**, el incremento en el procesamiento de datos puede aumentar la exposición a riesgos cibernéticos y las inconsistencias de desarrollo pueden generar problemas de soporte a largo plazo;
 - **financieros**, incumplimiento del ROI del programa de robotización, errores de configuración y desarrollo en operaciones financieras con posibles implicaciones fiscales.
- **Requerimientos de seguridad desde la fase de diseño** de los robots, asegurando que en la robotización de los procesos:
 - se toman en consideración aspectos relativos a la privacidad de los datos, tanto en el tratamiento como en el almacenamiento de estos, y
 - se evalúa la necesidad de rediseñar los controles asociados al proceso de negocio, para minimizar potenciales errores operacionales.

- **Informes para la identificación de la suficiencia, integridad y estructura** de los informes necesarios para el negocio, relativos a procesos impactados por la implementación de robotizaciones.

A su vez, también se espera de Auditoría Interna que, en la medida de lo posible, identifique, analice y asesore de forma anticipada ante los riesgos emergentes que puedan afectar a la organización. En este sentido, es importante desarrollar estrategias e implantar técnicas para:

- **Detectar y analizar riesgos, anticipándose a la implementación de robots.** Auditoría Interna puede incorporar análisis de datos y herramientas de detección de riesgos para identificar proactivamente los riesgos emergentes y obtener información sobre el mejor enfoque para auditar estas nuevas tecnologías.
- **Impacto de riesgos de robotización de procesos en la estrategia tecnológica.** En este aspecto, Auditoría Interna puede establecer un marco de priorización interno para auditar los riesgos clave que plantea la implementación de tecnologías de robotización, contrastándolo, además, con el apetito de riesgo de la organización. Todo ello con el objeto de aportar su punto de vista en el establecimiento de la estrategia de riesgo corporativo en el campo de las tecnologías disruptivas.

NECESIDADES DE CONOCIMIENTO Y HABILIDADES SOBRE ROBOTIZACIÓN EN LOS EQUIPOS DE AUDITORÍA INTERNA

Los perfiles profesionales de los auditores internos se encuentran en permanente evolución, a medida que la naturaleza y caracterís-

ticas del entorno en el que desarrollan su profesión también lo hace.

Independientemente de que asuma labores de aseguramiento o de asesoramiento, es generalmente aceptado que el perfil de auditor interno debe ser lo más completo posible, por lo que debe presentar una combinación equilibrada de una serie de competencias transversales y verticales (más específicas y/o técnicas), que le permitan ejercitar su profesión diligentemente y aportando valor a la organización.

Entre las **competencias transversales** destacan el pensamiento analítico, las habilidades de comunicación, la integridad, la razonabilidad, la capacidad de indagación, y el conocimiento de la organización y del negocio en el que esta desarrolla sus actividades. Igualmente, es interesante contar con conocimientos sobre técnicas de mapeo de procesos, análisis causa-raíz y herramientas de análisis de datos, así como entender las implicaciones y exigencias ligadas a la gestión del cambio.

Por lo que respecta a las **competencias verticales**, se han ido ampliando y sofisticando de forma muy significativa en los últimos tiem-

pos, a medida que se ha ido afrontando la transformación digital de las organizaciones y, sobre todo, teniendo en cuenta los avances tecnológicos continuos adoptados por estas.

Para abordar los trabajos de Auditoría Interna en el ámbito de la robotización de procesos, es necesario destacar que los equipos deben contar con perfiles que, de manera conjunta, dispongan de los conocimientos y habilidades necesarios para ser capaces de entender tanto el entorno tecnológico de la organización, como sus riesgos asociados. Adicionalmente, se estima necesario disponer también de conocimientos sobre sistemas de información, ciberseguridad y nuevas tecnologías, así como sobre los procesos de implementación de estas. De manera específica, y en la medida de lo posible, no deberían faltar en los equipos de Auditoría Interna conocimientos básicos y/o experiencia sobre lenguajes de programación, habilidades de codificación y conocimientos de plataformas y herramientas como *Blue Prism*, *Automation Anywhere*, *Inflectra*, *Rapise*, *OpenSpan*, *UiPath*, *NICE* o *Contextor*, por mencionar algunas de las más conocidas.

Para estas tareas, los equipos deben contar con conocimientos tecnológicos, sobre TICs, ciberseguridad, protección de datos y algo de programación.



Cómo auditar los riesgos de los procesos robotizados

La robotización de procesos aporta numerosas ventajas a las organizaciones; tanto en materia de eficiencia, como de estandarización del funcionamiento de dichos procesos. Sin embargo, estas ventajas van acompañadas de nuevos riesgos, o de variaciones de los

riesgos tecnológicos tradicionales que se deben tener en consideración.

Por ello, una vez determinada en el Plan de Auditoría Interna la necesidad de realizar una revisión sobre la tecnología de robotización

de procesos y/o sobre la robotización de procesos específicos, es necesario realizar una identificación preliminar de riesgos, que contribuya, a su vez, a visualizar los controles implementados para mitigarlos, permitiendo, así, determinar el programa de trabajo que va a ser utilizado por Auditoría Interna para la ejecución de la revisión.

A continuación, se listan y desarrollan los principales riesgos asociados a las tecnologías de robotización de procesos, así como los controles esperados y una propuesta de pasos para auditar dichos controles.



RIESGOS DE ESTRATEGIA Y GOBERNANZA DE LOS ROBOTS

La robotización de procesos mediante tecnologías RPA y RDA, requiere de una estrategia alineada con la Dirección, en la que se establezcan los objetivos, así como las principales directrices que permitan su consecución. Por

otro lado, es necesario definir un modelo de gobierno, en el que se establezcan los roles y responsabilidades; tanto dentro del proceso de creación del robot, como en la operación de este.

RIESGO: Estrategia de robotización de procesos no definida

Descripción: No se dispone de una estrategia para la implantación de robots acorde con las expectativas de la compañía y aprobada por la Dirección.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
La estrategia de implementación de las tecnologías de robotización de procesos en las unidades de negocio implicadas, tanto a nivel operativo, como de estructura tecnológica y de seguridad, debe estar definida, documentada y alineada con la estrategia global de la compañía.	1. Comprobar que existe una estrategia definida en la compañía para la implementación de tecnologías de robotización de procesos. 2. Comprobar que la arquitectura tecnológica para el desarrollo de los robots está conforme a la estrategia tecnológica de la organización (analizando aspectos tales como si se dispone de un entorno tecnológico centralizado o descentralizado, etc.). 3. Valorar si los requisitos de seguridad del entorno de robots están conforme a la estrategia de seguridad de la organización. 4. Analizar si el despliegue de la estrategia de implementación de robots se ha realizado conforme a lo que se ha definido. 5. Asegurar que se dispone de un <i>Business Case</i> para la implementación de robots en la organización, y que se definen mecanismos para el seguimiento del cumplimiento de sus objetivos.

Particularidades de las tecnologías RPA / RDA: Posibilidad de formalizar un Comité de Seguimiento sobre la implantación de las tecnologías de RPAs y RDAs en la organización, que sirva tanto de espónsor, como de responsable de evaluar la consecución de los objetivos estratégicos.

Ejemplo de riesgo: No disponer de una estrategia única y aprobada por la Dirección, puede dificultar o, incluso, retrasar la adopción de la tecnología de robotización de procesos, a la vez que puede implicar un uso ineficiente de recursos.

RIESGO: Políticas y estándares no formalizados

Descripción: No se han establecido políticas y normas asociadas que sirvan como requisitos mínimos para el uso de robots a nivel global.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
La Política de Seguridad de la Información (TIC), así como las otras políticas y normas asociadas (la política de control de acceso lógico, la de gestión de activos tecnológicos, la de gestión de proyectos IT, etc.) deben de considerar los requisitos mínimos del entorno tecnológico de los RPAs y RDAs. Las políticas y normas deben estar aprobadas por el órgano competente, ser revisadas periódicamente y ser de obligado cumplimiento por el personal de la organización y terceros vinculados a robots.	1. Comprobar que el desarrollo de robots está conforme con el contenido de la Política de seguridad de la Información (TIC) y las Políticas y normas asociadas definidas por la organización, como, por ejemplo: - Copias de seguridad. - Activos tecnológicos. - Control de acceso lógico. - Gestión de incidentes de seguridad. - Gestión de proyectos tecnológicos. - Procedimiento de gestión de operaciones. - Procedimiento de seguridad. - Uso de los recursos digitales. 2. Comprobar que, en dichas políticas, se han considerado las particularidades de los robots. 3. Validar que la Política de la seguridad de la Información (TIC) se encuentra formalizada y aprobada por parte del órgano / Dirección pertinente en cada organización. 4. Comprobar el adecuado seguimiento y cumplimiento de las políticas aplicables.

Particularidades de las tecnologías RPA / RDA: Se debería disponer de normativa específica vinculada a:

- La gestión de usuarios y contraseñas de los procesos robotizados.
- La gestión de cambios para los procesos robotizados.
- El ciclo de vida de los robots (alta / baja / modificación).
- La operación de los procesos robotizados.
- Establecer indicadores de medida de la eficacia y eficiencia aportada por los robots.

Ejemplo de riesgo: Si en las políticas y normas vinculadas a la Seguridad de la Información, no se tienen en consideración las particularidades de los robots, se pueden dar situaciones de ambigüedad a la hora de decidir qué controles implementar en la robotización de procesos, pudiendo dejar el entorno más vulnerable.

RIESGO: Funciones, responsabilidades y estructura no definida

Descripción: No se han definido las funciones, las responsabilidades y la estructura organizativa para desarrollar, operar y mantener los robots desarrollados en la organización.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Disponer de una matriz de funciones y responsabilidades RACI documentada (responsable, aprobador, consultado e informado) que englobe toda la estructura involucrada en el desarrollo, operación y mantenimiento de los robots.	1. Comprobar la existencia de matriz RACI (Responsable, Aprobador, Consultado e Informado) donde se define la supervisión, la propiedad y la rendición de cuentas entre los principales interesados en los robots (Dirección, unidades de negocios, tecnología, etc.). 2. Analizar junto con la Dirección los roles y responsabilidades definidos para la gestión de robots.

Particularidades de las tecnologías RPA / RDA: Se debe disponer de una Matriz RACI que incluya los roles y responsabilidades sobre las tecnologías de RPA / RDA y la robotización de procesos. Entre los roles, se deberían recoger:

- El responsable de la tecnología de robotización.
- El responsable de los robots implementados.
- El órgano responsable de decidir sobre la implantación de un robot en un proceso crítico.
- Establecer el responsable de seguridad tecnológica.
- Establecer un rol específico que vele por la privacidad / protección de datos.

Ejemplo de riesgo: No disponer de una asignación clara de roles y responsabilidades de la tecnología de robotización, así como de los robots implementados, puede crear conflictos o ineficiencias en el propio proceso como en el caso de respuesta ante un incidente.

RIESGO: Gestión de riesgos de la robotización de procesos no definida

Descripción: No se han definido los mecanismos de evaluación, supervisión y mitigación de los riesgos asociados a la identificación, el desarrollo, el despliegue y las operaciones de robots en la organización.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Se dispone de un modelo de gestión de riesgos específico para el programa de robotización de actividades de la organización, en el que se toman en consideración aspectos como criticidad de las actividades automatizadas, tipología de datos gestionados, complejidad de la operativa, etc.	1. Verificar que se dispone de una metodología propia de evaluación de riesgos para la robotización de actividades, en la que se tomen en consideración aspectos como la criticidad de las actividades a robotizar, así como tipología de datos gestionados o complejidad de la operativa.
A su vez, este modelo de riesgos es reportado en el contexto del Sistema de Control Interno de la organización.	2. Asegurar que se hayan definido y aprobado por parte de la Dirección, los criterios en base a los que se pueden robotizar actividades a partir de los resultados de la evaluación de riesgos, así como el flujo de aprobación de los mismos.
	3. Definir indicadores de riesgo, que nos permitan medir de forma continua la exposición al riesgo por el hecho de disponer de procesos robotizados (por ejemplo: número de incidentes producidos en los robots, volumen de ejecuciones previstas respecto a las efectuadas, etc.)
	4. Verificar que los indicadores de riesgo son reportados e integrados en el marco del Sistema de Control Interno de la organización.

Particularidades de las tecnologías RPA / RDA: Se deben realizar evaluaciones de riesgo de las actividades a robotizar, con el objetivo de valorar, en base a unos criterios previamente establecidos, si estas actividades pueden ser robotizadas, o hacerlo implica una exposición a riesgos legales / operacionales / tecnológicos por encima del apetito al riesgo de la organización.

Ejemplo de riesgo: Si no se dispone de una metodología de evaluación de riesgos de las actividades a robotizar, puede implicar que se implementen robots para los que, en caso del incidente, el impacto de este esté por encima de la tolerancia al riesgo propia de la organización.

RIESGO: Continuidad operativa específica de los robots

Descripción: No se ha documentado la manera de proceder en caso de una eventual caída o retirada forzosa del robot, ocasionando una discontinuidad operativa.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Ante cualquier incidente de un robot, se dispone de mecanismos documentados para que el personal del negocio, y / o otro personal designado, pueda ejecutar el proceso de manera manual mientras se soluciona la incidencia.	1. Consultar que existe documentación (procedimientos y guías) y las herramientas necesarias que permitan ejecutar y operar el proceso sin la utilización del robot.
	2. Analizar y revisar que se dispone del personal, y que este tiene el conocimiento necesario (operativo y tecnológico) para operar el proceso sin la utilización del robot en caso de ser necesario.

Particularidades de las tecnologías RPA / RDA: La organización debe asegurarse que, en todo momento, las unidades de negocio disponen de los conocimientos necesarios para la ejecución de la tarea / actividad de forma manual, para el mantenimiento, desarrollo o actuaciones ante un incidente del Robot, asegurando una continuidad operativa.

Ejemplo de riesgo: En caso de incidencia sobre un robot específico, si no se dispone de mecanismos de continuidad operativa (documentación sobre la actividad robotizada, procedimiento para la ejecución manual, etc.) se puede producir una discontinuidad operativa.

RIESGO: Plan de comunicación no definido

Descripción: No se dispone de un plan de comunicación específico que dé a conocer a las distintas áreas de la organización la posibilidad de robotizar procesos.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Debe existir un plan de comunicación periódico que garantice que todas las áreas de la organización conocen la posibilidad de robotizar procesos. El plan de comunicación identifica a los responsables con quien contactar para iniciar el proceso de robotización.	Comprobar que: 1. Existe un plan de comunicación. 2. El plan de comunicación se distribuye a la organización (correo, portal del empleado, etc.)

Particularidades de las tecnologías RPA / RDA: El éxito de un programa de robotización de procesos depende de que los propietarios de los procesos conozcan la posibilidad y ventajas de robotizarlos.

Ejemplo de riesgo: No comunicar o distribuir a las distintas áreas de la organización la posibilidad de robotizar procesos y de las ventajas que ello conlleva, puede derivar en la pérdida de eficacia de posibles procesos objeto de robotización, o en desarrollos aislados menos efectivos por las distintas direcciones de la organización.

RIESGO: Robotización no autorizada por parte de proveedores de servicio a los que se les han externalizado actividades

Descripción: No conocer, aceptar y supervisar, la robotización de una actividad (o parte de la misma) por parte del proveedor de servicios al que le ha sido externalizada, puede derivar en impactos operacionales no controlados.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Se debe exigir a los proveedores a los que se les haya externalizado servicios que, en caso de querer robotizar alguno de los procesos incluidos en los servicios prestados, esta robotización sea informada y aprobada, y a su vez, se realice bajo unos criterios y condiciones establecidos por la organización. Para los servicios externalizados de mayor criticidad, establecer controles técnicos (por ejemplo: indicadores de tiempo de ejecución, número de operaciones ejecutadas, captchas, etc.) que permitan identificar si el proveedor ha robotizado parte del proceso.	1. Comprobar el listado de servicios externalizados susceptibles de que el proveedor haya robotizado o pueda robotizar parte de la actividad (por ejemplo, servicios de <i>back office</i>). 2. Analizar los requerimientos (criterios y condiciones), bajo los que se podría permitir a los proveedores, que roboticen parte de las actividades que se les han externalizado. 3. Si aplica, verificar el cumplimiento de los requerimientos (criterios y condiciones) establecidos con los proveedores respecto a la implementación de robots. 4. Analizar los controles técnicos implementados para monitorizar si un proceso vinculado a un servicio "crítico", ha sido robotizado.

Particularidades de las tecnologías RPA / RDA: La posibilidad de que un proveedor de servicios, al que se le ha externalizado una actividad, automatice la ejecución de esta actividad mediante un robot –desarrollado con su propia tecnología y utilizando sus propias metodologías– es un riesgo propio de la tecnología RPA / RDA.

Ejemplo de riesgo: La implementación de un robot no autorizado por parte de un tercero para robotizar parte de un servicio que le ha sido externalizado, puede generar dependencias no esperadas con dicho proveedor, así como conllevar a errores operacionales masivos no controlados, generados por un incidente (ya sea derivado de un problema en el propio robot, o de un cambio en el sistema final sobre el que actúa el robot, que no ha sido notificado).

RIESGO: Inventario de robots no definido

Descripción: Desconocimiento y descontrol de los procesos robotizados. Falta de gobierno de los robots.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Mantener un inventario completo, actualizado y centralizado de los procesos robotizados.	1. Comprobar que la organización ha designado a un responsable del mantenimiento y actualización del inventario de los procesos robotizados. 2. Comprobar la existencia de mecanismos de control que garanticen que el inventario de procesos robotizados incluye la totalidad de implementaciones de robots en la organización. 3. El inventario debe contener al menos: a) Nombre e id del robot. b) Tipo de robot. c) Propietario del robot y responsable de su utilización. d) Interfaces con las aplicaciones de TI, aplicaciones de usuario finales y otros robots. e) Procesos de negocios relacionados. f) Gestión de información sensible. g) Estado de implementación (en desarrollo, en test, etc). h) Porcentaje de avance. i) Clasificación en base a la criticidad (Confidencialidad, integridad y disponibilidad).

Particularidades de las tecnologías RPA / RDA: Mecanismos de control para identificar los robots operativos en la organización.

Ejemplo de riesgo: No disponer de un inventario centralizado de procesos robotizados puede conllevar a no disponer de una visión completa de como explotar eficientemente los robots para toda la organización.

RIESGO: Criterios de valoración y seguimiento de proveedores de tecnologías de robotización no definidos

Descripción: No disponer de mecanismos de control para la evaluación de proveedores de robotización de procesos.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Comprobar que se ha realizado una valoración de los proveedores de tecnologías de robotización de procesos para garantizar la correcta ejecución de los servicios prestados.	1. Identificar que los proveedores que suministran soluciones tecnológicas de robotización de procesos están catalogados (listado de proveedores, base de datos, etc.) y estos se encuentran homologados / certificados según los procedimientos internos de la compañía. 2. Comprobar que se realiza una valoración del servicio prestado por los proveedores de tecnologías de robotización.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: No realizar una correcta evaluación y / o seguimiento de los proveedores de tecnologías de robotización de procesos puede ocasionar un incidente que afecte a la reputación de la compañía.

**RIESGOS OPERACIONALES Y TECNOLÓGICOS DE LOS ROBOTS**

La implantación de soluciones RPA o RDA implica, en esencia, la implantación de un nuevo sistema de TI que necesita integrarse con el

entorno de gestión de riesgos de TI y que deberá ser gestionado de manera adecuada. Esta integración nos debe hacer considerar los

potenciales nuevos riesgos operacionales derivados de eventos causados por la inadecuación o fallos en la red y los sistemas informá-

ticos, la seguridad y la gestión operativa llevada a cabo.

RIESGO: Funcionamiento inadecuado o deficiente de las plataformas de robots

Descripción: No se establece un proceso adecuado de detección, solución y análisis de causa raíz de los errores e incidentes generados por las plataformas de robots.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de incidencias: La compañía debe definir procedimientos para la monitorización, escalado y resolución de las incidencias que afecten a las plataformas de robots para asegurar su operación efectiva de manera continua.	1. Asegurar una monitorización continua de las incidencias técnicas identificadas en el ámbito de las plataformas de robots. 2. Asegurar la realización y documentación de un análisis de causas raíz para cada una de las incidencias técnicas identificadas. 3. Verificar que, tras la detección y análisis de incidencias técnicas, se informa a las áreas involucradas en los procesos robotizados. 4. Verificar que las respuestas recibidas por parte de las áreas involucradas se tienen en cuenta en la actualización del diseño del robot, si aplica.

Particularidades de las tecnologías RPA / RDA: Las incidencias sobre las plataformas de robots, deben ser notificadas a las áreas usuarias de los distintos robots.

Ejemplo de riesgo: Una incidencia técnica sobre las plataformas de robots no debidamente identificada y solucionada, puede generar indisponibilidades e impactos operacionales en los procesos automatizados.

RIESGO: Funcionamiento inadecuado o deficiente de un proceso robotizado

Descripción: No se establece un proceso adecuado de detección, solución y análisis de causa raíz de las incidencias técnicas detectadas durante el funcionamiento de un robot.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de incidencias: La compañía debe definir procedimientos para la monitorización, escalado y resolución de las incidencias que afecten a los robots para asegurar su operación efectiva de manera continua.	1. Asegurar una monitorización continua de las incidencias técnicas identificadas en el ámbito de los sistemas finales, con el objetivo de detectar, prevenir y gestionar dichas incidencias. 2. Asegurar la realización y documentación de un análisis de causas raíz para cada una de las incidencias técnicas identificadas. 3. Verificar que, tras la detección y análisis de incidencias técnicas, se informa a las áreas de negocio involucradas en los procesos robotizados. 4. Verificar que las respuestas recibidas por parte del área de negocio a su análisis de impacto de la incidencia técnica en el proceso, se tienen en cuenta en la actualización del diseño del robot, si aplica.

Particularidades de las tecnologías RPA / RDA: Se deben establecer mecanismos de comunicación entre los responsables de los sistemas finales y los responsables de las plataformas de robots, para que, en caso de incidencia en el sistema final, se pueda notificar a tiempo a los responsables del robot, para evitar problemas en las ejecuciones de este, así como para poder realizar las actualizaciones que sean necesarias en el robot.

Ejemplo de riesgo: Problemas en el proceso automatizado, debido a incidencias con el sistema final.

RIESGO: Costes de mantenimiento indebidos

Descripción: No se establecen controles que garanticen que los robots son dados de baja oportunamente si su funcionalidad ya no es necesaria o si la relación coste-beneficio dejó de ser adecuada.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Monitorización negocio La compañía debe definir procedimientos para que las áreas de negocio realicen una adecuada monitorización de la actividad y funcionamiento del robot y de las actividades clave del proceso automatizado.	1. Verificar que el área de negocio participa en el diseño del Robot realizando análisis de riesgos, definiendo responsables, identificando tareas a desarrollar, información a la que debe acceder el robot y excepciones o comportamientos anómalos para la elaboración de un informe de excepciones. 2. El área de negocio evalúa periódicamente si el robot sigue siendo necesario, verificando si su funcionalidad está en uso y si compensa el coste-beneficio. a. Si un robot es modificado o dado de baja, se comunica oportunamente para la modificación del inventario de robots de la compañía. 3. Verificar que negocio, con una periodicidad establecida, extrae el informe de excepciones del robot y realiza un análisis causa-raíz. a. Se elabora (y se realiza seguimiento de) un plan de remediación. 4. Verificar que negocio realiza una monitorización y revisión periódica de las actividades y controles clave del proceso validando la completitud e integridad de las operaciones realizadas por el robot. a. Se verifica periódicamente que los sistemas finales están preparados y configurados para garantizar una monitorización adecuada. b. En caso de identificarse excepciones, se realiza seguimiento para su remediación. 5. Verificar la existencia de controles sobre los disparadores de la ejecución de los robots que generan alertas en tiempo real en el caso de que se produzcan actuaciones sospechosas o comportamientos anómalos (activación fuera de tiempo, parámetros de entrada inadecuados, etc.) 6. Verificar que negocio analiza las incidencias comunicadas por el área técnica, e identifica y documenta: a. Impactos potenciales en el proceso que deban ser corregidos. b. Actualizaciones necesarias en el diseño del robot.
Monitorización de las plataformas de robots La compañía debe definir procedimientos para realizar una adecuada monitorización de la actividad y funcionamiento de las plataformas de robots.	1. Asegurar la realización de un análisis proactivo de la actividad registrada en las plataformas de robots, verificando que: a. Existe un registro adecuado y completo de la actividad. b. Los periodos de retención de logs son suficientes de acuerdo con la criticidad del proceso robotizado. 2. El registro de la información deberá incluir, al menos: a. Registro de la persona que ejecuta actividades relacionadas con el robot. b. Actividades realizadas. c. Fecha en que se registró la acción. 3. Adicionalmente, se verificará el almacenamiento de los logs de forma no manipulable en una herramienta externa tipo SIEM. 4. Verificar que existen controles orientados a detectar cambios sobre las actividades permitidas en la ejecución de un robot, concretamente: a. Cambios en las reglas de negocio del robot. b. Cambios en la configuración de seguridad en el sistema de administración del robot, tales como parámetros de auditoría, cambios en las cuentas de acceso.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Monitorización Sistema Final La compañía debe definir procedimientos para realizar una adecuada monitorización de la actividad y funcionamiento de las plataformas de robots.	- Se realiza un análisis proactivo de la actividad registrada por los usuarios que utilizan los robots, verificando que: - Existe un registro adecuado y completo de la actividad. - Los periodos de retención de <i>logs</i> son suficientes de acuerdo con la criticidad del proceso robotizado. - El registro de la información deberá incluir, al menos: - Actividad realizada por el robot. - Fecha en que se registró la acción. - Adicionalmente, se verificará el almacenamiento de los <i>logs</i> de forma no manipulable en una herramienta externa tipo SIEM.

Particularidades de las tecnologías RPA / RDA: No aplica

Ejemplo de riesgo: El robot se sigue ejecutando y manteniendo sin considerar si sigue siendo necesario o si compensan los costes.

RIESGO: Bastionado no adecuado en los activos de la plataforma de robots

Descripción: El software base (*firmware*, sistema operativo y sistemas gestores de bases de datos, de comunicaciones y de virtualización) de los servidores que conforman la plataforma de robots, así como la de los ordenadores donde se ejecuten los robots, presenta vulnerabilidades, tanto conocidas como latentes, que habilitan la toma del control por parte de un atacante.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión del bastionado: La plataforma de robots de la organización debe estar correctamente bastionada, siguiendo estándares y mejores prácticas de mercado.	- Verificar la existencia de una Política de Seguridad que requiera el bastionado de la plataforma de robots, así como de un marco procedimental destinado a verificar y mantener: - Las contraseñas, acordes a la complejidad y renovación requerida por la organización. - El software base actualizado y protegido frente a las vulnerabilidades conocidas. - El software estrictamente requerido para la correcta ejecución de la plataforma y los robots, eliminando cualquier otro. - Activos los puertos de comunicación estrictamente requeridos para la correcta ejecución de la plataforma y los robots, desactivando cualquier otro. - Software <i>antimalware</i>, que éste está en ejecución y protegido frente a intentos de desactivación. - Las firmas, heurísticas e IOC actualizadas en los sistemas de protección de las comunicaciones (<i>firewall</i>, <i>ips</i> e <i>ids</i>) - Que la plataforma de robots está localizada en una red segmentada del resto de redes y la visibilidad entre redes es acorde al principio de mínima exposición. - Se dispone de estándares de bastionado de los fabricantes de los productos específicos de RPAs y RDAs, y se configuran los mismos en base a dichos estándares. - Comprobar que todos los activos que conforman la plataforma de robots cumplen con los requerimientos expuestos en el punto anterior.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Un atacante puede utilizar algunas vulnerabilidades conocidas para tomar el control o introducir *malware* en los servidores de la plataforma de robots o los equipos de ejecución.

RIESGO: Activos tecnológicos de las Plataformas de robots no debidamente actualizados

Descripción: No disponer de activos debidamente actualizados en la plataforma de robots, puede derivar en indisponibilidades o incidentes de seguridad en dicho entorno.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de la obsolescencia: El entorno tecnológico (servidores físicos y virtuales, sistemas operativos, servidores de bases de datos, etc), así como los productos específicos de RPAs y RDAs, deben de utilizar versiones debidamente actualizadas.	1. Analizar la infraestructura utilizada para la plataforma de robots, e identificar el nivel de actualización de los distintos activos. 2. Validar si los activos se han actualizado de acuerdo con el proceso de actualización de activos tecnológicos de la organización.

Particularidades de las tecnologías RPA / RDA: Se debe validar, además del versionado de los activos tecnológicos que componen la infraestructura, el nivel de actualización de los productos de mercado específicos para robotización utilizados. A su vez, dichos productos deben utilizar licencias válidas y siguiendo los criterios establecidos por el proveedor.

Ejemplo de riesgo: La utilización de versiones obsoletas o no debidamente actualizadas en los activos del entorno de robotización, puede provocar indisponibilidades por vulnerabilidades conocidas, así como incidentes de seguridad.

RIESGO: Mecanismos de contingencia tecnológica no definidos

Descripción: No existen mecanismos de contingencia tecnológica para la plataforma de robots.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
La compañía debe definir procedimientos para determinar la adecuación de la arquitectura respecto a los requerimientos de disponibilidad de negocio, así como los requerimientos de seguridad, estrategia cloud y escalabilidad.	1. Comprobar que se ha dotado a la infraestructura asociada a la plataforma de robots de mecanismos de contingencia acordes con los requerimientos de disponibilidad de los procesos de negocio automatizados, tanto respecto al dimensionamiento, como a la gestión de <i>backups</i> de los activos. 2. Comprobar la existencia de procedimientos y / o mecanismos de vuelta atrás en caso de fallo o caída de la plataforma de robots. 3. Comprobar si la plataforma de robots se tiene en cuenta en la definición de los Planes de Continuidad de negocio de los distintos procesos afectados. 4. Comprobar si la plataforma de robots se tiene en cuenta en la definición y pruebas de los Planes de Recuperación de Desastres.

Particularidades de las tecnologías RPA / RDA: Es necesario definir los requerimientos en términos de infraestructura, no solo de los activos propios de la plataforma de robots, sino adicionalmente de los puestos virtuales definidos sobre los que actúan los robots.

Ejemplo de riesgo: Una indisponibilidad de la infraestructura que soporta la plataforma de robots puede generar fallos en la operativa del robot con el correspondiente impacto operacional a los responsables del proceso automatizado, así como pérdida de información.

**RIESGOS DE CAMBIOS Y SU IMPACTO EN LOS ROBOTS**

Los RPA y RDA son, en esencia, automatizaciones sobre aplicaciones o sistemas ya existentes. Dichas automatizaciones se basan en el desarrollo de una solución tecnológica. En

este sentido, es relevante que se emplee una metodología que garantice un desarrollo adecuado, así como un proceso de gestión de cambios, tanto para la puesta en producción

de robots como para la identificación de cambios en los sistemas finales, que puedan generar la necesidad de modificar los robots ya en funcionamiento.

RIESGO: Metodología de desarrollo de robots no definida

Descripción: Los desarrollos de robots no se realizan utilizando una metodología.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
La organización dispone de una metodología de desarrollo que tiene en consideración las particularidades de los robots, así como mejores prácticas para el desarrollo adecuado de robots.	1. Existe una metodología definida en la organización para la implementación de robots, ya sea específica o utilizada por otros desarrollos. 2. Comprobar que la metodología se aplica correctamente en el desarrollo de una muestra de robots.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Desarrollar robots sin utilizar una metodología definida y acordada, puede derivar en la implementación de soluciones no adecuadas a los requerimientos de negocio.

RIESGO: Proceso de gestión de cambios en robots no definido

Descripción: No se dispone de un procedimiento para la gestión de cambios en sistemas y procesos robotizados que puedan impactar a la ejecución del robot.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
En caso de un cambio en el proceso robotizado, los responsables del robot son avisados con el tiempo suficiente para adaptarlo sin provocar una discontinuidad operativa.	1. Identificar los mecanismos manuales y automáticos para detectar cambios en los procesos robotizados. 2. Revisar que se han establecido mecanismos de comunicación entre los propietarios de los procesos robotizados y los responsables de los robots, en tiempo y forma.

Particularidades de las tecnologías RPA / RDA: Este es un riesgo específico de los robots.

Ejemplo de riesgo: Un cambio en una aplicación con un proceso robotizado no es comunicado a los responsables de los robots.

RIESGO: No se utilizan entornos de pruebas

Descripción: No existe un entorno de pruebas para los robots desarrollados que permita hacer pruebas fuera de los entornos productivos.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Definición de entornos de testeo y desarrollo, que garanticen que un robot no compromete el funcionamiento de los entornos productivos.	1. Verificar que existen actividades de control que permiten realizar pruebas sobre el funcionamiento de los robots sin comprometer la confidencialidad, integridad y disponibilidad de los datos que se mantienen en los entornos productivos. 2. Verificar que existen actividades de control que permiten realizar pruebas sobre el funcionamiento de los robots sin comprometer la operativa de los entornos productivos.

Particularidades de las tecnologías RPA / RDA: Por la tipología de desarrollos que representan los robots, es importante realizar pruebas funcionales junto al usuario, y poder hacerlo con ejecuciones escalonadas del robot.

Ejemplo de riesgo: Realizar pruebas en real puede implicar desde un riesgo operacional, al lanzar robots no funcionales contra aplicaciones productivas, hasta riesgos de privacidad y confidencialidad, por el acceso a datos de producción por parte de usuarios no autorizados.



RIESGOS DE CIBERSEGURIDAD EN LOS ROBOTS

El entorno tecnológico de las plataformas de robots, como cualquier entorno tecnológico está expuesto a los principales riesgos de ciberseguridad.

RIESGO: Gestión indebida de los usuarios de ejecución

Descripción: No existen controles que garanticen que los usuarios de ejecución del proceso robotizado se solicitan, aprueban y revisan de forma adecuada.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de usuarios en sistemas finales Se deben definir procedimientos que garanticen que los usuarios de ejecución de los robots se gestionan adecuadamente, queda trazabilidad de su tramitación y son revisados periódicamente.	1. Existe un procedimiento formalizado de solicitud y autorización de cuentas Robot en los sistemas finales. 2. Se aplica el principio de mínimos privilegios. 3. Verificar que la creación de usuarios robots: a. Queda registrada. b. Existe una adecuada trazabilidad de su gestión (desde la petición hasta el alta). c. La asignación de roles / perfiles se realiza en base al principio de mínimos privilegios y se cumple con la normativa de segregación de funciones de la empresa. d. Se identifican claramente los responsables de las cuentas de usuario para robots creadas en los sistemas finales. 4. Verificar que las cuentas robot (y perfiles asociados) creadas en los sistemas o aplicaciones finales son aprobadas por sus responsables periódicamente.

Particularidades de las tecnologías RPA / RDA: Los robots utilizan usuarios cuyos permisos se crean en base al usuario o usuarios de negocio cuyas funciones automatizan, pudiendo generarse nuevos roles con más permisos de los que podría tener un usuario de negocio habitual.

Ejemplo de riesgo: Creación de robots con permisos inadecuados que puedan ejecutar acciones no permitidas y / o que generen un funcionamiento indebido.

RIESGO: Gestión de usuarios no adecuada en el producto RPA y/o RDA (Usuarios de producto)

Descripción: No existen controles que garanticen que los usuarios del producto RPA y/o RDA se solicitan, aprueban y revisan de forma adecuada

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de usuarios en la plataforma RPA y/o RDA. Se deben definir procedimientos que garanticen que los usuarios del producto RPA y/o RDA se gestionan adecuadamente y queda trazabilidad de su tramitación y son revisados periódicamente.	1. Existe un procedimiento formalizado de gestión de usuarios y permisos en la plataforma RPA y/o RDA. 2. Verificar que la gestión de usuarios en la plataforma RPA y/o RDA: a. Queda registrada. b. Existe una adecuada trazabilidad de su gestión (desde la petición hasta el alta / baja / modificación). c. La asignación de roles / perfiles se realiza en base al principio de mínimos privilegios y con una adecuada segregación de funciones. 3. Comprobar que las cuentas creadas para el producto RPA y/o RDA son verificadas por sus responsables periódicamente.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Existencia de usuarios en la plataforma de gestión con permisos inadecuados para eliminar o modificar configuraciones de ejecución de robots.



RIESGO: Obtención no autorizada de la identidad de los usuarios del robot

Descripción: No disponer de mecanismos de almacenado seguro de las contraseñas de los usuarios utilizados por los robots, ni limitar el *login* a las aplicaciones y máquinas estrictamente necesarias.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Nunca se escriben las credenciales en los <i>scripts</i> o en ficheros de configuración no protegidos. Se aplica una política de contraseñas robustas. El usuario y la contraseña de cada uno de los robots se almacenan de forma segura, utilizando productos que permitan el almacenamiento centralizado y cifrado de las credenciales y el rotado de claves. Los usuarios asignados a los robots deben tener restringido el acceso a cualquier máquina o aplicaciones que no sea aquellas en la que se va a ejecutar.	1. Verificar que las directrices de codificación contemplan que no se escriban credenciales directamente en el código. 2. Verificar que existe una política de contraseñas y que ésta se aplica. 3. Verificar que los usuarios tienen el acceso restringido a cualquier máquina que no sea la de ejecución.

Particularidades de las tecnologías RPA / RDA: Los robots utilizan usuarios con un rol que puede abarcar más permisos de los que un usuario normal suele tener (ya que puede automatizarlas tareas de varias personas), con lo que los accesos de los que disponen son potencialmente sensibles.

Ejemplo de riesgo: Si las contraseñas no están correctamente almacenadas (por ejemplo, introducidas directamente en el código, o en ficheros o herramientas fácilmente accesibles), estas pueden ser accedidas por personas no autorizadas y utilizadas de forma malintencionada.

RIESGO: Accesos al entorno de producción no autorizados

Descripción: No se disponen de mecanismos que permitan limitar y controlar los accesos al entorno de producción de la infraestructura del robot.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Existen procedimientos que regulan la realización de accesos, en situaciones de emergencia o con elevados privilegios a las infraestructuras TIC de entornos en producción. Estos accesos son identificados, registrados, autorizados y revisados, con el fin de realizar un seguimiento de estos y prevenir accesos no autorizados o fraudulentos.	1. Comprobar: a. Usuarios que han accedido a producción en un periodo de tiempo (el que se defina según el alcance de la auditoría). b. Usuarios que han accedido a la administración de robots un periodo de tiempo (el que se defina según el alcance de la auditoría).

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Un acceso no autorizado a un entorno de producción, puede derivar en incidentes operacionales intencionados o no.

RIESGO: Imposibilidad de obtener datos de la actividad realizada en la infraestructura y el producto RPA y/o RDA

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Existen registros de la actividad en las infraestructuras TIC productivas y sistemas. Dichos registros (o <i>log</i>) se almacenan y revisan de acuerdo con los criterios y periodicidades definidos en los procedimientos existentes. El objetivo principal es detectar actividad anómala en las operaciones realizadas por el robot y, en caso de incidencia, poder recuperar las condiciones y eventos que las produjeron. Los <i>logs</i> más típicos serían los del servidor de aplicaciones y base de datos, y aquellos relacionados con la ejecución del robot.	1. Verificar la existencia de: a. Un registro de actividad. b. Una plataforma SIEM. c. Informes SIEM de las infraestructuras. 2. Analizar la siguiente información: a. Informes SIEM último semestre. b. Periodicidad envío de los <i>logs</i> al SIEM.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Si no se registran las trazas y se gestionan con las herramientas y procedimientos adecuados, puede ocurrir un incidente de seguridad, y este no ser detectado en el plazo esperado, ni poder establecer las condiciones en las que ocurrió.



RIESGOS DE CUMPLIMIENTO NORMATIVO, LEGAL Y REGULATORIO DE LOS ROBOTS

El entorno normativo interno y externo de la organización (legal y/o regulatorio), puede generar situaciones en las que se esté en dis-

posición de incumplir los mandatos establecidos, en relación con las situaciones en las que se encuentre presente la robotización.

RIESGO: Incumplimiento regulatorio

Descripción: Existencia de implantaciones de robots incumpliendo las normativas externas.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Comprobar que los desarrollos de robots, cumplen con la normativa vigente y estándares internacionales y de negocio.	1. Verificar que los desarrollos de robots cuentan con un análisis previo a su implementación que garantice el cumplimiento con todos los requisitos regulatorios de ámbito nacional o internacional (Ley Orgánica 3/2018, Real Decreto Ley 11/2021, etc.). 2. Verificar, en caso de nueva normativa o modificación de normativas vigentes, que la Dirección comunica la misma a los responsables de los desarrollos de robots para su correcta implementación.

Particularidades de las tecnologías RPA / RDA: Cumplimiento / seguimiento de estándares internacionales (OWASP –*Open Web Application Security Project*–, MITRE ATT&CK, ISO, UNE, etc.).

Ejemplo de riesgo: Un robot puede realizar pagos a un país / región considerada paraíso fiscal o puede estar incumpliendo la normativa de Protección de Datos y Garantías de Derechos Digitales.



RIESGO: Incumplimiento de políticas y procesos internos

Descripción: Existencia de implantaciones de robots incumpliendo las políticas y procesos internos.

OBJETIVO DE CONTROL	CÓMO AUDITARLO
Comprobar que se cumple con las políticas y procesos internos establecidos en la compañía.	1. Comprobar que el desarrollo de robots se realiza conforme a la política de seguridad de la información (TIC) y las políticas y normas asociadas definidas por la organización.

Particularidades de las tecnologías RPA / RDA: No aplica.

Ejemplo de riesgo: Tener un robot en producción sin haber sido aprobado previamente pudiendo perjudicar de forma operativa o financiera a la compañía.

Consideraciones finales

Las organizaciones, en la búsqueda de una mayor eficiencia, están apostando con fuerza por tecnologías de robotización como los RPA y RDA. Estas tecnologías aportan muchos beneficios en materia de estandarización, escalabilidad y eficiencia en la ejecución de procesos. No obstante, como se ha descrito en el presente documento, dichos beneficios van acompañados de nuevos riesgos, así como variantes de riesgos ya conocidos.

A la vez que se debe disponer de un entorno tecnológico robusto y escalable, que permita la correcta operación de los robots implementados, es especialmente relevante que haya una adecuada involucración de las áreas de negocio responsables del proceso a robotizar, con los equipos responsables de la implementación de los robots. Dicha coordinación entre equipos permitirá entender claramente los requerimientos de las actividades a robotizar,

así como valorar la mejor solución para la consecución de los beneficios previstos. Adicionalmente es relevante destacar que la robotización de actividades y procesos no puede solventar los problemas intrínsecos asociados.

Ante esta situación, Auditoría Interna debe tomar consciencia del impacto transformacional potencial de este tipo de tecnologías, y contar con equipos de profesionales que dispongan de los conocimientos y habilidades necesarias para proporcionar aseguramiento a la Comisión de Auditoría y a la Alta Dirección sobre los principales riesgos que afectan a la organización en este campo.

En este sentido, se debe analizar, en primera instancia, el grado de implantación de las tecnologías de robotización y valorar la tipología de trabajos que se pueden realizar para poder

aportar valor, tanto desde el punto de vista del aseguramiento, como desde el de asesoramiento para la implantación de este tipo de tecnologías.

Para ello, en términos de aseguramiento, Auditoría Interna debe realizar trabajos que permitan analizar tanto los controles del entorno tecnológico asociado a la tecnología de robotización, como los flujos y metodologías de robotización de procesos, así como, los mecanismos utilizados para la operación de los RPA y RDA.

Por lo que respecta al asesoramiento (para empresas con un menor grado de madurez en la implantación de esta tecnología), es necesario aportar valor, desde la perspectiva de la identificación de los principales riesgos tecnológicos, operacionales y legales en los que se puede incurrir durante el transcurso de la robotización de procesos o actividades de negocio.

Dichos trabajos deben permitir identificar recomendaciones y planes de acción que aporten valor y aseguramiento a la organización.

Bibliografía

THE INSTITUTE OF INTERNAL AUDITORS

- *Marco Profesional para la Práctica Profesional de Auditoría Interna (MIPP)*. 2017.
- *Global Technology Audit Guide (GTAG): Understanding and Auditing Big Data*. 2017.
- *Risk in Focus 2020 - Hot topics for internal auditors*.
- *Risk in Focus 2021 - Hot topics for internal auditors*.
- *Risk in Focus 2022 - Hot topics for internal auditors*.
- *Risk in Focus 2023 - Hot topics for internal auditors*.

INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

- LA FÁBRICA DEL PENSAMIENTO. *Auditoría Interna del proceso de inversión en tecnologías emergentes*. Noviembre 2020.

REGULACIÓN

- Brussels, 21.4.2021 COM(2021) 206 final. Propuesta del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. 2021.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

ESTANDAR DE BUENAS PRÁCTICAS

- OWASP: <https://owasp.org>
- ATTACK.MITRE: <https://attack.mitre.org/>

ARTÍCULOS, DOCUMENTOS, GUÍAS

- IBERDROLA. *La automatización robótica de procesos (RPA) en las empresas y su impacto en la industria*.
- ISACA Journal. *How Internal Audit Can Help Capture Value in Robotic Process Automation Projects*. (<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2>).
- ISACA South Florida. *Robotic Process Automation (RPA) and the Auditor*. Septiembre 2020.
- GARTNER. *Robotic Process Automation. Implications for Internal Audit*. 2018.
- HELPSYSTEMS. *Una guía sobre RPA*.
- DELOITTE. *Auditing the RPA environment. Our approach towards addressing risks in a BOT environment*. March, 2018.
- DELOITTE. *Automatización robótica de procesos*. Febrero 2017.
- KPMG LLP. *Internal audit and intelligent automation*. 2018.
- KPMG LLP. *Internal audit and robotic process automation*. 2018.
- NIMBUL CONSULTING. *RPA - Automatización Robótica de Procesos*.
- OWASP. Top ten (<https://owasp.org/Top10/>). *How to use the OWASP Top 10 as a standard*.
- PWC. *Robotics process automation a primer for internal audit professionals*. October, 2017.

BLOGS, REVISTAS Y OTROS ENLACES DE INTERÉS

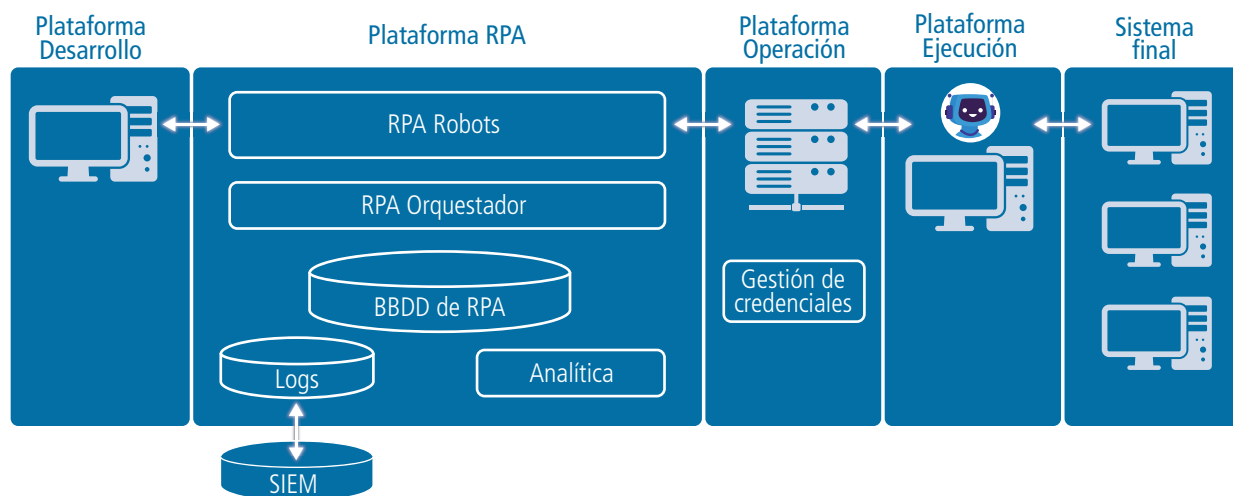
- EXEVI
<https://www.exevi.com/siete-formas-en-las-que-rpa-puede-resolver-los-problemas-de-it-y-negocio/>
- EY
https://www.ey.com/es_es/gobierno-corporativo/impacto-de-la-propuesta-de-normativa-europea-sobre-ia-en-organos-de-gobierno
- GFT
<https://blog.gft.com/es/2018/04/10/automatizacion-robotica-de-procesos-liberar-al-personal-de-las-tareas-rutinarias/>
- HARPIA
<https://harpia-software.com/por-que-falla-el-despliegue-del-rpa/>
- IBERDROLA
<https://www.iberdrola.com/innovacion/>
- ISACA
<https://www.isaca.org/resources/isaca-journal/issues>
- TEKNEI
<https://www.teknei.com/2019/10/07/problemas-y-soluciones-en-la-implantacion-de-un-rpa/>



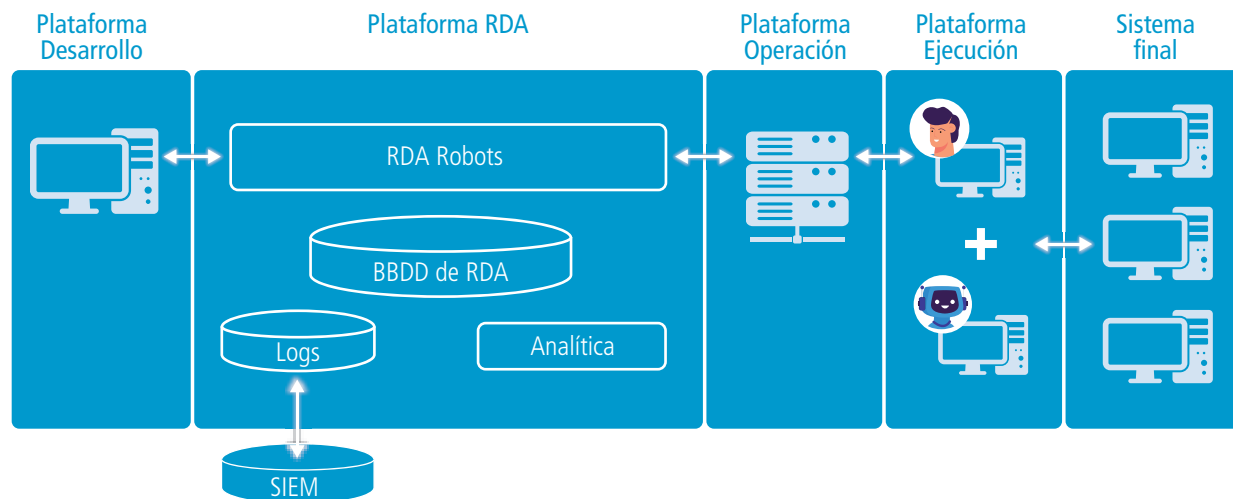
Anexo I

Esquema tecnológico y de seguridad en una plataforma RPA / RDA

En la siguiente figura se incluye un ejemplo de un esquema genérico de los elementos tecnológicos y de seguridad claves en la implementación de una plataforma RPA.



En la siguiente figura se incluye un ejemplo de un esquema genérico de los elementos tecnológicos y de seguridad claves en la implementación de una plataforma RDA.



Los términos de estas figuras están recogidos en el Anexo II - Glosario





Anexo II - Glosario

BBDD de RPA / RDA

Bases de datos en la que se almacenan tanto los códigos fuente de los RPAs y RDAs, como aspectos específicos de su configuración. *(Figura Anexo I).*

IDS (Intrusion Detection System)

Sistemas que alertan de potenciales intrusiones.

IPS (Intrusion Protection System)

Sistemas capaces de implementar mecanismos automáticos de respuesta ante potenciales intrusiones.

ISO (International Organization of Standardization)

Organización que desarrolla y publica estándares internacionales. Entre los estándares importantes dentro del alcance de este documento, destacan ISO 27001/2 sobre seguridad de la información, ISO 22301 sobre continuidad de negocio, ISO 31000 sobre gestión de riesgos, ISO 37500 sobre gobierno de las TIC o ISO 27031 sobre contingencia tecnológica.

KPIs (Key Performance Indicators)

Indicadores clave de rendimiento de un proceso, alineado a un objetivo fijado previamente. Deben ser alcanzables, medibles, relevantes, periódicos y exactos.

KRIs (Key Risk Indicators)

Indicadores clave de riesgo, relevantes para proporcionar a la organización información y predicciones de riesgos. Deben ser objetivos, consistentes y fáciles de monitorizar y de cuantificar.

Logs

Trazas informáticas de los eventos que se producen en las actividades ocurridas en los sistemas y procesos. *(Figura Anexo I).*

Malware

Software maligno que trata de afectar a un dispositivo.

Matriz RACI

(Responsable, Aprobador, Consultado, Informado)

Matriz de asignación de responsabilidades utilizada generalmente en gestión de procesos y proyectos.

MITRE Att&ck

Marco de referencia sobre técnicas y tácticas que son utilizadas en ataques cibernéticos e intrusiones.

Orquestador RPA / RDA

Entorno tecnológico utilizado para la monitorización y administración centralizada de los robots. *(Figura Anexo I).*

OWASP (Open Web Application Security Project)

Proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.

Plataforma de desarrollo

Entorno tecnológico en el que se realizan los desarrollos de los robots y que dispone de todos los mecanismos y controles para el versionado y gestión de su código fuente.

Plataforma de ejecución

Entorno tecnológico desde el que se ejecutan los robots (por ejemplo, máquinas virtuales). *(Figura Anexo I).*

Plataforma de operación

Entorno tecnológico desde el que se pueden operar/controlar las ejecuciones individuales de los robots y se pueden realizar acciones en tiempo de ejecución. En la misma se integran habitualmente los mecanismos de gestión segura de contraseñas. *(Figura Anexo I).*

Plataforma robots

En el presente documento, cuando se habla de plataforma de robots, se hace referencia a la infraestructura y sistemas responsables de la orquestación y ejecución de los robots. *(Figura Anexo I).*

RDA (Robotic Desktop Automation)

Robots Atendidos, los cuales conviven y asisten al usuario a llevar a cabo su proceso de negocio.

ROI (Return on Investment)

Retorno sobre la inversión.

RPA (Robotic Process Automation)

Robots Desatendidos, los cuales se encargan de llevar a cabo las tareas y operaciones de un proceso de forma totalmente autónoma.

SIEM (Security Information and Event Management)

Sistemas para la gestión de eventos e información de seguridad, encargados de centralizar el almacenamiento y la interpretación de los datos relevantes de seguridad.

Sistema final

En este documento, cuando se habla de sistema final, se hace referencia a las aplicaciones o sistemas sobre los que se han implementado robots (ya sean RPAs o RDAs).

TIC

Tecnologías de la Información y la Comunicación.

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: 978-84-124893-7-8

Diseño y maquetación: desdezero, estudio gráfico

Propiedad del Instituto de Auditores Internos de España. Se permite la reproducción total o parcial y la comunicación pública de la obra, siempre que no sea con finalidades comerciales, y siempre que se reconozca la autoría de la obra original. No se permite la creación de obras derivadas.

OTRAS PRODUCCIONES DE LA FÁBRICA DE PENSAMIENTO

NUEVAS FORMAS DE TRABAJO EN REMOTO DE AUDITORÍA INTERNA

Esta guía de buenas prácticas analiza todos los aspectos necesarios para desarrollar el trabajo en remoto en la Dirección de Auditoría Interna, incluyendo sus implicaciones en las relaciones con los stakeholders y los retos y limitaciones –y cómo hacerles frente– de esta forma de trabajar.

AUDITORÍA INTERNA DE LA GESTIÓN DE CRISIS Y RESILIENCIA DEL NEGOCIO

Abarca el rol de Auditoría Interna en la supervisión de los mecanismos de gestión de crisis y la resiliencia del negocio, así como el papel que asume en la fase previa, durante y después de que se produzca una crisis, e identifica las mejores prácticas relacionadas con la actuación de Auditoría Interna en este tipo de trabajos.

GESTIÓN ESTRATÉGICA DEL TALENTO EN AUDITORÍA INTERNA

La gestión del talento es fundamental para la consecución de los objetivos de la compañía y de cada uno de los departamentos que la integran. Este documento abarca distintas dimensiones de la gestión del talento desde la óptica de la consecución de los objetivos de la Dirección de Auditoría Interna y en el ámbito del *Marco Internacional para la Práctica Profesional de la Auditoría Interna*.

GUÍA PARA IMPLANTAR CON ÉXITO UN MODELO DE AUDITORÍA CONTINUA

Implantar un modelo de Auditoría Continua permite a la Dirección de Auditoría Interna mejorar la calidad del aseguramiento que proporciona a la Alta Dirección y al Consejo de Administración de forma proactiva, proyectiva y continua. La guía analiza exhaustivamente todas las cuestiones relevantes a considerar y no olvidar cuando se emprende la implantación de un modelo de Auditoría Continua, sus beneficios y desafíos.



LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

Este documento aborda los diferentes tipos de robotización de procesos del negocio y los distintos roles que puede asumir Auditoría Interna (aseguramiento y asesoramiento) frente a una tecnología que está cada vez más presente en la operativa de las empresas y que presenta oportunidades, pero también riesgos que hay que gestionar y minimizar.