Instituto de Auditores Internos de España

Los Lunes del Instituto de Auditores Internos

www.auditoresinternos.tv

#LosLunesIAI - @Auditorinterno

Auditoría Interna de los procesos robotizados de negocio

AUDITORÍA INTERNA

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 Auditores Internos de España

AUDITORÍA INTERNA

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

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.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

Índice

Instituto de Auditores Internos de España

Índice

Instituto de Auditores Internos de España

Índice

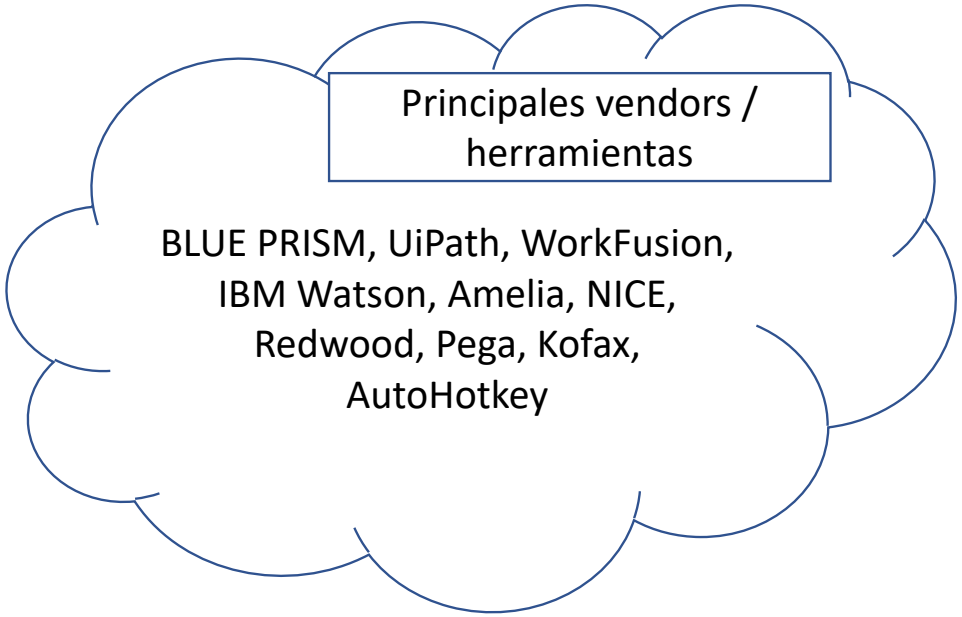
Instituto de Auditores Internos de España

Introducción a la Robotización de procesos

¿Que es la automatización o robotización de procesos?

"La automatización o robotización de procesos es el uso de **robots de software para automatizar tareas rutinarias altamente repetitivas**. Un robot pueden realizar cualquier tarea basada en reglas lógicas que se lleven a cabo en un ordenador, del mismo modo que lo hacemos los usuarios pero de forma autónoma y automática. Estas tareas se pueden llevar a cabo de manera desatendida o atendida, distinguiendo por tanto dos tipos de robots, Robots Desatendidos (RPA) y Robots Atendidos (RDA)"

RPA	RDA
Robotic Process Automation	**Robotic Desktop Automation**
Los robots desatendidos llevan a cabo las tareas y operaciones de un proceso de forma totalmente autónoma	Los robots atendidos conviven y asisten al usuario a llevar a cabo su proceso de negocio
	



Instituto de Auditores Internos de España

Índice

Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos (enfoques y técnicas)

¿Cual es el rol que puede desempeñar Auditoría Interna dentro de el contexto de la Robotización de procesos?

Como "usuario"	En revisiones de asesoramiento	En revisiones de aseguramiento
• Auditoria interna dispone de múltiples procesos internos propios, susceptibles de ser mejorados a partir de su automatización.	• Auditoria interna, tiene una visión transversal única tanto del negocio como del entorno de control, y debe asesorar cuando pueda significar una mejora, la automatización de procesos.	• Auditoria interna, tiene una visión transversal única tanto del negocio como del entorno de control, y debe evaluar el impacto que representa la implantación de robots, así como de la evolución de los riesgos al aplicar automatizaciones.

Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos

como "usuario" | **En revisiones de asesoramiento** | En revisiones de aseguramiento

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 y valor de las tecnologías de la 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

- Análisis de riesgos para la adaptación del proceso
- Requerimientos de seguridad desde la fase de diseño
- Informes para la identificación de la suficiencia, integridad y estructura
- Impacto de riesgos de la Robotización de procesos en la estrategia tecnológica

Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos

como "usuario" | En revisiones de asesoramiento | **En revisiones de aseguramiento**

En caso que la Organización disponga ya de procesos robotizados, con independencia del grado de madurez de los mismos, desde Auditoría Interna, se pueden realizar distintos enfoques de aseguramiento, que aportan valor en la identificación de principales riesgos, y en garantizar la mejora contínua.

Entre los enfoques de aseguramiento principales, destacan los siguientes:

Auditoría del gobierno y entorno tecnológico de los robots

- Roles y responsabilidades
- Modelo operativo definido para los robots
- Criterios de Robotización
- Mecanismos de prevención, detección, comunicación y corrección de incidencias en los robots
- Análisis de las herramientas y procesos para la gestión de seguridad

Auditoría del ciclo de vida de los robots

- Selección, diseño y desarrollo de robots
- Análisis funcional y técnico
- Seguridad y acceso

Auditoría de procesos afectados por los robots

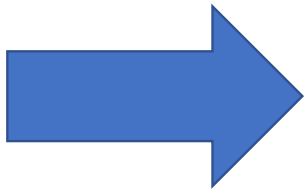
- Evaluación de la eficacia operativa de los controles del robot
- Evaluación del diseño de controles del robot
- Entendimiento de los riesgos del proceso

Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos

como "usuario" | En revisiones de asesoramiento | **En revisiones de aseguramiento**

Necesidades de conocimiento y habilidades sobre robotización en los equipos de Auditoría Interna



Competencias transversales: Pensamiento analítico, habilidades de comunicación, integridad, razonabilidad, capacidad de indagación, conocimiento de la organización, conocimiento sobre técnicas de mapeo de procesos, implicaciones y exigencias ligadas a la gestión del cambio, CURIOSIDAD.

Competencias verticales: Conocimientos del entorno tecnológico de la organización, conocimientos sobre ciberseguridad y nuevas tecnologías, conocimientos sobre procesos IT claves (gestión de incidencias, metodologías de desarrollo, gestión de cambios), y es un valor añadido **conocer las tecnologías de robotización.**

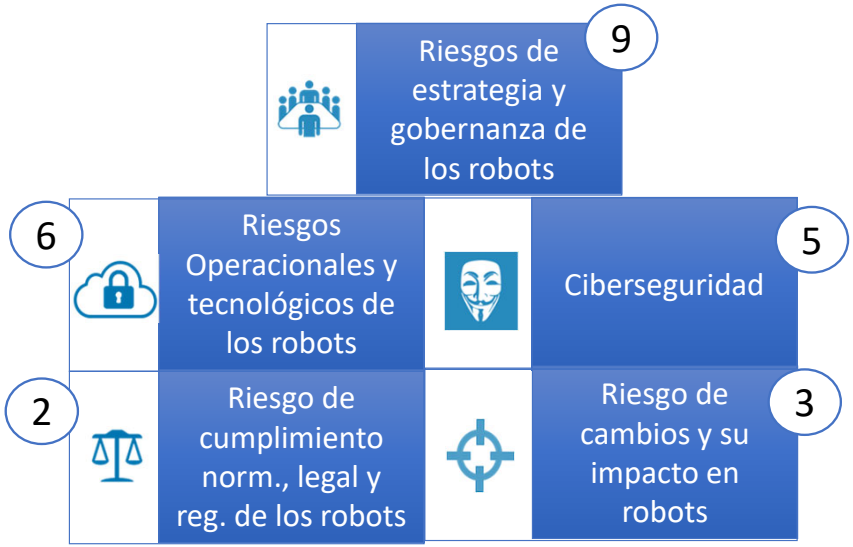
Instituto de AuditoresInternos de España

Índice

Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos

Robotizar actividades conlleva en si mismo, un riesgo que debe ser añadido a los riesgos propios del proceso y/o entornos que busca ser automatizados.



En el documento, se han incluido riesgos dentro de cada una las categorías que se pueden ver en la imagen de la izquierda (el número indica los riesgos incluidos en cada categoría).

Para cada uno de estos riesgos, se ha desarrollado una ficha, con la siguiente información:

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 *Business Case* 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.

Descripción del riesgo

Detalle de "Como Auditar" el objetivo de control

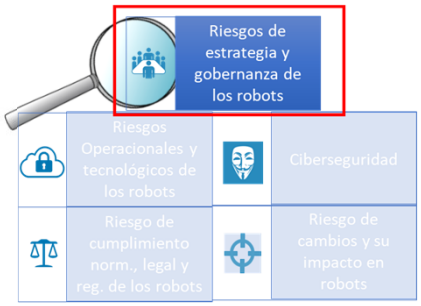
Aspectos particulares para RPA/RDA

Objetivo de control

Ejemplo práctico del riesgo

Instituto de AuditoresInternos de España

Riesgos significativos vinculados a la Robotización de procesos



Gestión de riesgos de la robotización de procesos no definida

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.

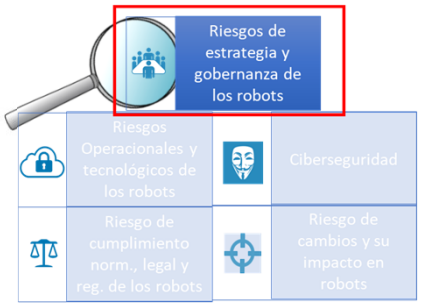
OBJETIVO DE CONTROL	CÓMO AUDITARLO
Se dispone de un modelo de gestión de riesgos específico para el programa de robotización de actividades de la organización, en el que se toman en consideración aspectos como criticidad de las actividades automatizadas, tipología de datos gestionados, complejidad de la operativa, etc. A su vez, este modelo de riesgos es reportado en el contexto del Sistema de Control Interno de la organización.	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. 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.

Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Continuidad operativa especifica de los robots

RIESGO: Continuidad operativa especifica 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.

Riesgos significativos vinculados a la Robotización de procesos

Funcionamiento inadecuado o deficiente de un proceso robotizado

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.

Instituto de AuditoresInternos de España

Riesgos significativos vinculados a la Robotización de procesos

Mecanismos de contingencia tecnológica no definidos

RIESGO: Mecanismos de contingencia tecnológica no definidos

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

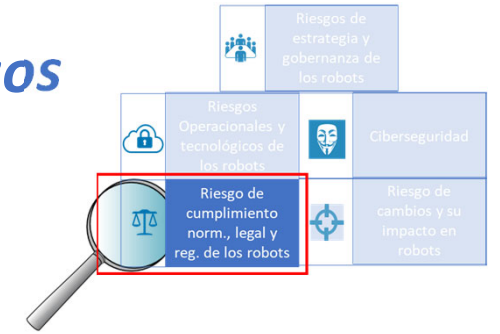
OBJETIVO DE CONTROL	CÓMO AUDITARLO
La compañía debe definir procedimientos para determinar la adecuación de la arquitectura respecto a los requerimientos de disponibilidad de negocio, así como los requerimientos de seguridad, estrategia cloud y escalabilidad.	1. Comprobar que se ha dotado a la infraestructura 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 *backups* 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.

Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Metodología de desarrollo de robots no definida

RIESGO: Metodología de desarrollo de robots no definida

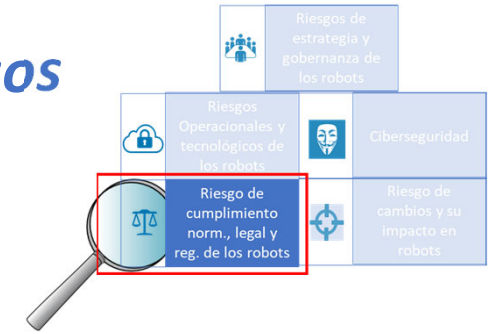
Descripción: Los desarrollos de robots no se realizan utilizando una metodología.

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.

Riesgos significativos vinculados a la Robotización de procesos



Proceso de gestión de cambios en robots no definido

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.

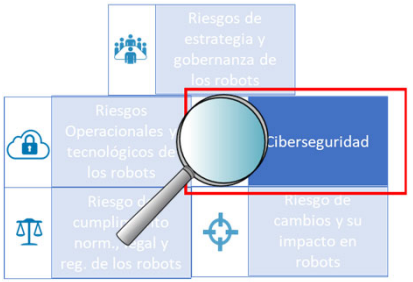
OBJETIVO DE CONTROL	CÓMO AUDITARLO
En caso de un cambio en el proceso robotizado, los responsables del robot son avisados con el tiempo suficiente para adaptarlo sin provocar una discontinuidad operativa.	1. Identificar los mecanismos manuales y automáticos para detectar cambios en los procesos robotizados. 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.

Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Gestión indebida de los usuarios de ejecución

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.

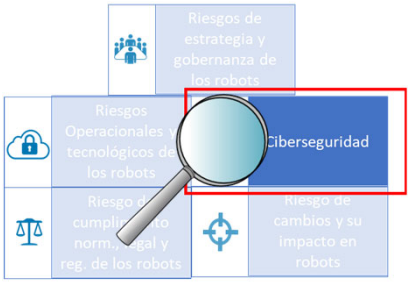
OBJETIVO DE CONTROL	CÓMO AUDITARLO
Gestión de usuarios en sistemas finales Se deben definir procedimientos que garanticen que los usuarios de ejecución de los robots se gestionan adecuadamente, queda trazabilidad de su tramitación y son revisados periódicamente.	1. Existe un procedimiento formalizado 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.

Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Obtención no autorizada de la identidad de los usuarios del robot

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.

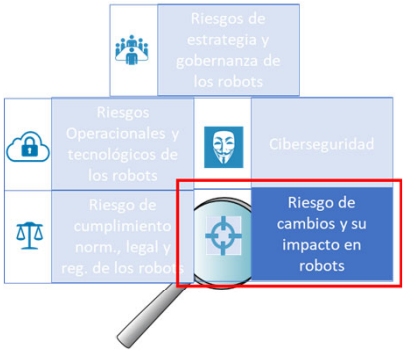
OBJETIVO DE CONTROL	CÓMO AUDITARLO
Nunca se escriben las credenciales en los *scripts* o en ficheros de configuración no protegidos. Se aplica una política de contraseñas robustas. El usuario y la contraseña de cada uno de los robots se almacenan de forma segura, utilizando productos que permitan el 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.

Instituto de AuditoresInternos de España

Riesgos significativos vinculados a la Robotización de procesos



Incumplimiento regulatorio

RIESGO: Incumplimiento regulatorio

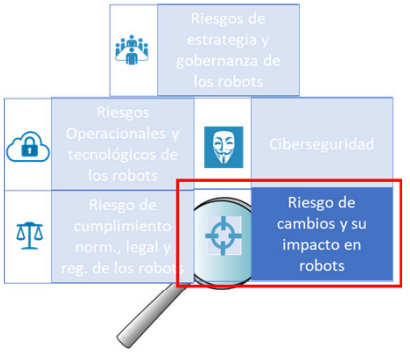
Descripción: Existencia de implantaciones de robots incumpliendo las normativas externas.

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 11/2018, 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.

Riesgos significativos vinculados a la Robotización de procesos



Incumplimiento de políticas y procesos internos

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.

Instituto de AuditoresInternos de España

Índice

Instituto de Auditores Internos de España

Implementación de Robotics – Experiencia práctica

Tecnología utilizada y ámbitos de aplicación

- Dentro de la estrategia de digitalización de Repsol, se ha desarrollado software de robotización en multitud de procesos de diferentes áreas y negocios
- El uso de RPA está extendido en múltiples ámbitos de la compañía: registro de información de contratos y pedidos, facturación, gestión de Identidades, alta de usuarios en aplicaciones de negocio, gestión de almacenes, …
- La tecnología utilizada es BluePrism alojada en una infraestructura en Cloud que cuenta por cada entorno con:
  - Un servidor IaaS donde se encuentra instalado el motor de RPA
  - Una base de datos SQL Server PaaS
  - Una granja de VDIs Windows

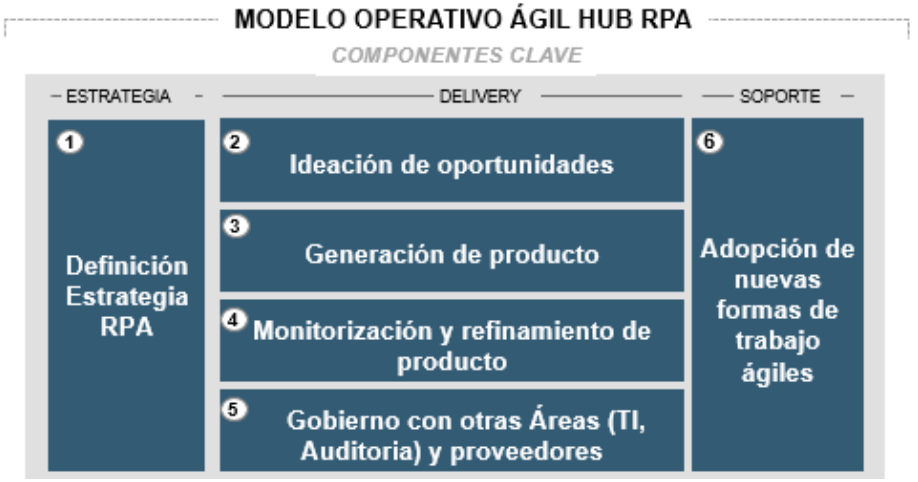
Implementación de Robotics – Experiencia práctica

Gestión de la Demanda de robotización

El conocimiento de la posibilidades de automatización está extendido en la compañía, en forma de “autogestión” con iniciativas como “DO-IT-YOURSELF” basadas en PowerApps de Microsoft o posibilidades de aplicación de RPA en forma de casos digitales.

Generalmente, los primeros pasos para comenzar un proceso de automatización son los siguientes:

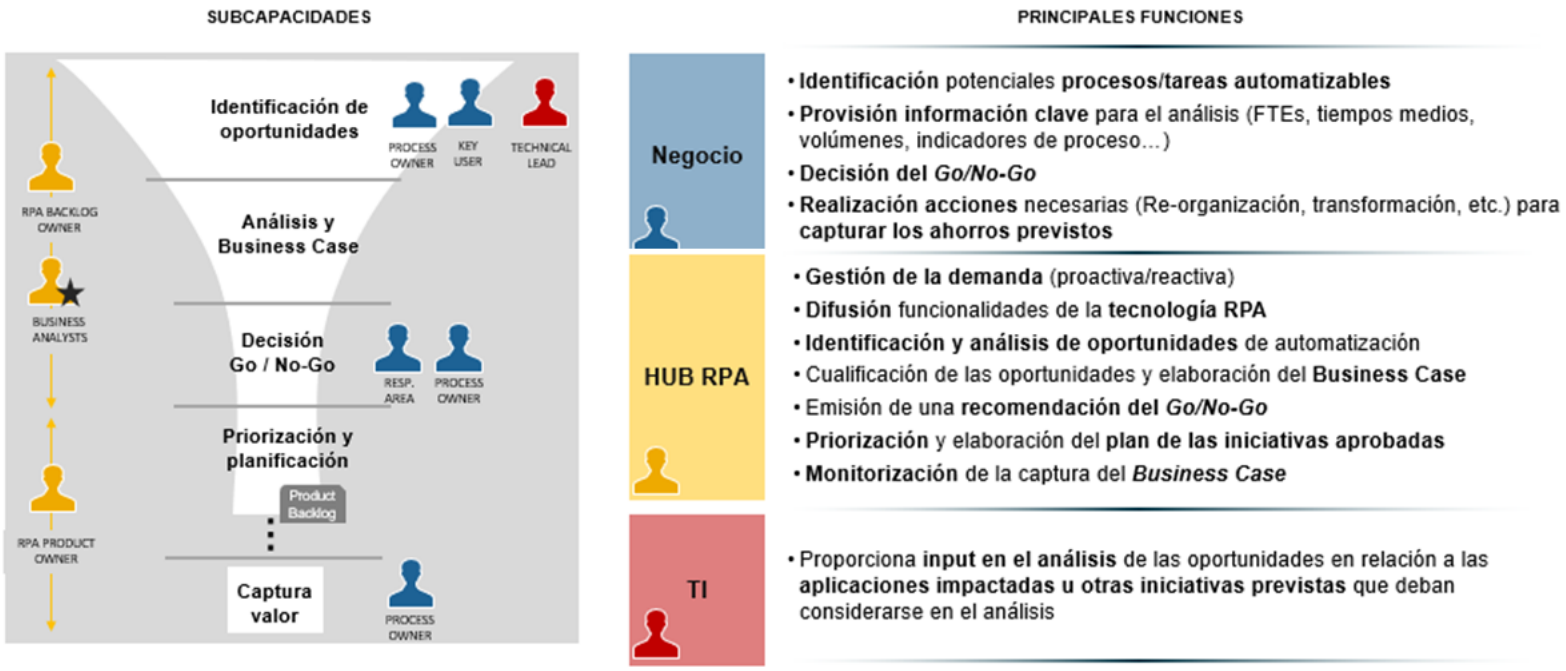
- Analizar en detalle el proceso y los sistemas que lo soportan
- Evaluar qué tecnología utilizar, ya que RPA es solo una de las muchas posibles para la automatización de procesos de negocio. Dependiendo de diferentes parámetros como pueden ser complejidad del proceso, criticidad, participación de negocio, limitaciones técnicas… la tecnología elegida puede ser una u otra.
- Elaborar un Business Case que ha de ser positivo.



Implementación de Robotics – Experiencia práctica

Roles principales en la implantación de un RPA

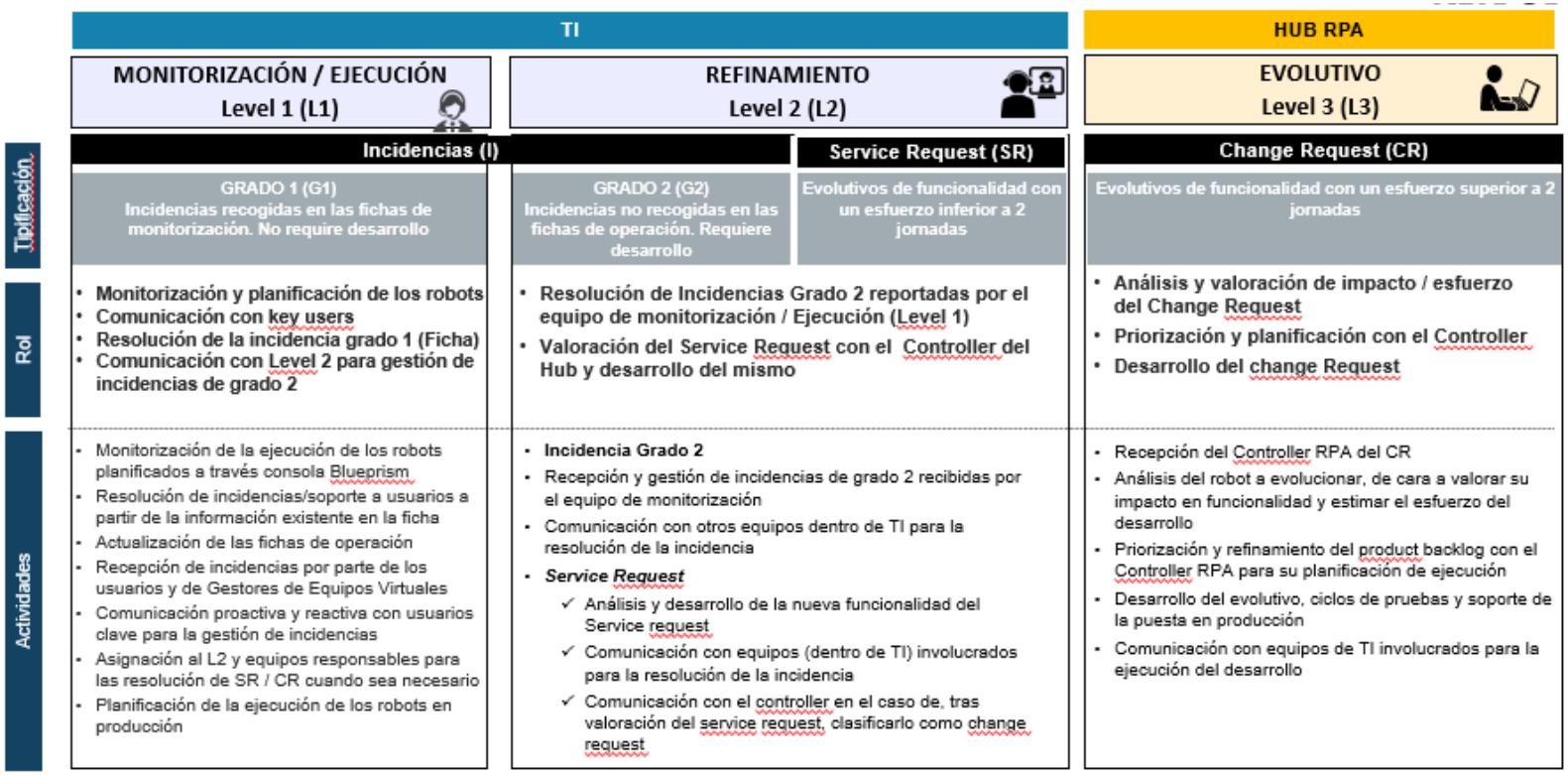
Gobierno centralizado en el Hub de RPA



Instituto de Auditores Internos de España

Implementación de Robotics – Experiencia práctica

Proceso de Gestión de incidencias y cambios



Instituto de Auditores Internos de España

Índice

Instituto de Auditores Internos de España

Ejemplos de robots – Experiencia práctica

Caso de uso: ABM de Contratos

Objetivo:

Crear o modificar contratos en SAP a partir de una petición lanzada por el negocio.

Los sistemas afectados son:

- Máquinas SAP de los negocios

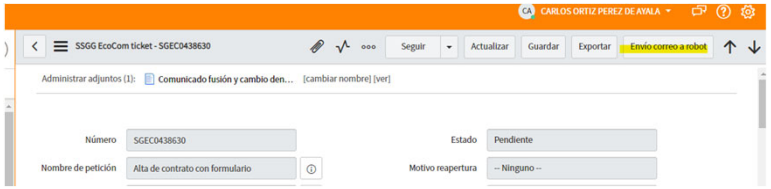
Resultado:

Crea o modifica el contrato, actualiza el libro de pedidos para todos los centros, informa del plazo de entrega real y el más largo, y el tipo de fecha de pedido. En el caso de que haya un reparto de cuotas las cumplimenta.

Al finalizar la ejecución se produce un envío de correo con el resultado de la operación al técnico de contratos.

Particularidades:

No es un proceso planificado. Las peticiones se reciben vía sistema de ticketing y se ejecutan a través de una integración realizada adhoc entre el RPA y el sistema de ticketing.



Instituto de Auditores Internos de España

Ejemplos de robots – Experiencia práctica

Caso de uso: ABM de usuarios en aplicaciones de negocio

Objetivo:

Para las áreas involucradas, actualizar los permisos de los usuarios en función de su estado en el sistema de empleados de la compañía.

Pasos previos:

- Realizar una matriz detallada Est. Organizativa/Role, para determinar a qué aplicaciones y qué tipo de acceso se deberá aplicar, identificando los responsables de cada una de ellas.
- Inventario de aplicaciones a las que se va acceder con el robot. En este caso, 8 tecnologías con las que el RPA tiene que interactuar, desde Excel y Outlook a SAP o Gestión Documental. Adicionalmente, el sistema leerá datos del sistema de RRHH para determinar que tipo de operación realizará: Alta, Baja o Modificación.
- Documento de detalle de las acciones a realizar por el robot en cada aplicación afectada considerando cada tipo de operación, llegando a nivel de campo.

Resultado:

Por cada ejecución realizada, el robot genera un reporte de todos los usuarios gestionados, dando el detalle necesario para saber que todo ha ido bien "OK", o en el caso de haber encontrado alguna dificultad, registrando las incidencias ocurridas.

Se notifica a cada responsable de aplicación el resultado de la ejecución, así como a aquellos usuarios a los que se les han actualizado los permisos correctamente.

Instituto de AuditoresInternos de España

Índice

Instituto de Auditores Internos de España

Visión de Auditoría Interna – Experiencia práctica

Auditoría 2019 – Objetivos

En 2019 se realizó una auditoría con los siguientes objetivos:

- Revisión del procedimiento de implantación de un RPA en Repsol.
- Revisión de los controles de TI asociados a un entorno automatizado mediante RPA.

Para ello se contó con los actores principales del proceso:

- Negocio/s responsables de los procesos a automatizar.
- Hub RPA. Digitalización.
- Soporte tecnológico. Servicio de Plataformas.
- Servicio de aplicaciones.

Además se contó con la participación de un responsable de Ciberseguridad como Guest Auditor.

Consideraciones a tener en cuenta:

Fase muy temprana de adopción de la tecnología por parte de la compañía (prácticamente un On-The-GO)

Instituto de Auditores Internos de España

Visión de Auditoría Interna – Experiencia práctica

Ejemplos de riesgos analizados vs Acciones llevadas a cabo

Ejemplo de riesgos analizados	Acciones
• Gestión de usuarios no adecuada en el producto RPA y/o RDA • Gestión indebida de los usuarios de ejecución • Obtención no autorizada de la identidad de los usuarios del robot	• Uso de Cyberark para gestión de usuarios en producción y custodia y rotado de sus contraseñas • En el procedimiento de GdA (Gestión de Accesos) se establece que los autorizantes son usuarios de negocio, generalmente los Process Owner. • Los robots tienen los mínimos permisos necesarios y se usa una cuenta por robot. Se ha incluido el concepto Cuenta Robotics.
• No se utilizan entornos de pruebas	• Cuatro entornos: Desarrollo, Preproducción, Certificación y Producción. El entorno de Certificación conecta con los sistemas de producción, pero las ejecuciones están controladas y el equipo de proyecto y el de negocio están presentes en las mismas.
• Imposibilidad de obtener datos de la actividad realizada en la infraestructura y el producto RPA y/o RDA	• Envío de los logs de BDD y Plataforma BluePrism al SIEM corporativo
• Metodología de desarrollo de robots no definida	• Existe un check list de Aceptación de Mantenimiento que permite comprobar si todos los requerimientos para la subida a producción están cubiertos en términos de documentación, alarmado, monitorización, estabilidad, pruebas, operación y calidad.
• Mecanismos de contingencia tecnológica no definidos	• Política de retención en Cloud adaptada para cubrir un año • El equipo de RPA está incorporado en las pruebas de PRD, comprobando el funcionamiento de los robots en caso de cambio de localización de los sistemas afectados.

Índice

Instituto de Auditores Internos de España

Conclusiones

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.**

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.

¡¡Gracias!!

Síguenos en

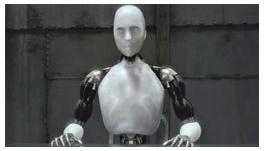
www.auditoresinternos.es

@Auditorinterno

Instituto de Auditores Internos de España

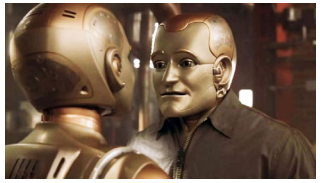
Imágenes robots (just4fun)



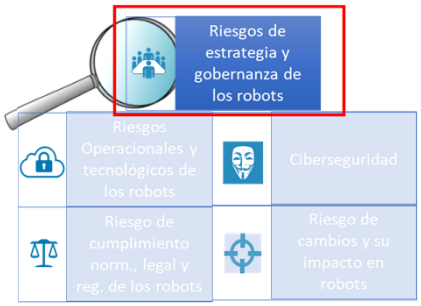




Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Estrategia de robotización de procesos no definida

RIESGO: Estrategia de robotización de procesos no definida

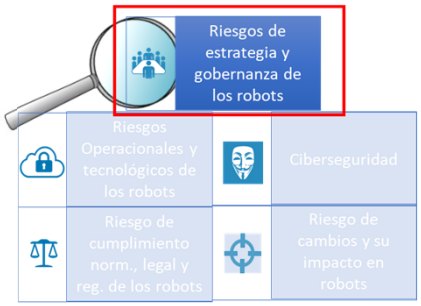
Descripción: No se dispone de una estrategia para la implantación de robots acorde con las expectativas de la compañía y aprobada por la Dirección.

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 *Business Case* 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.

Riesgos significativos vinculados a la Robotización de procesos



Funciones, responsabilidades y estructura no definida

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.

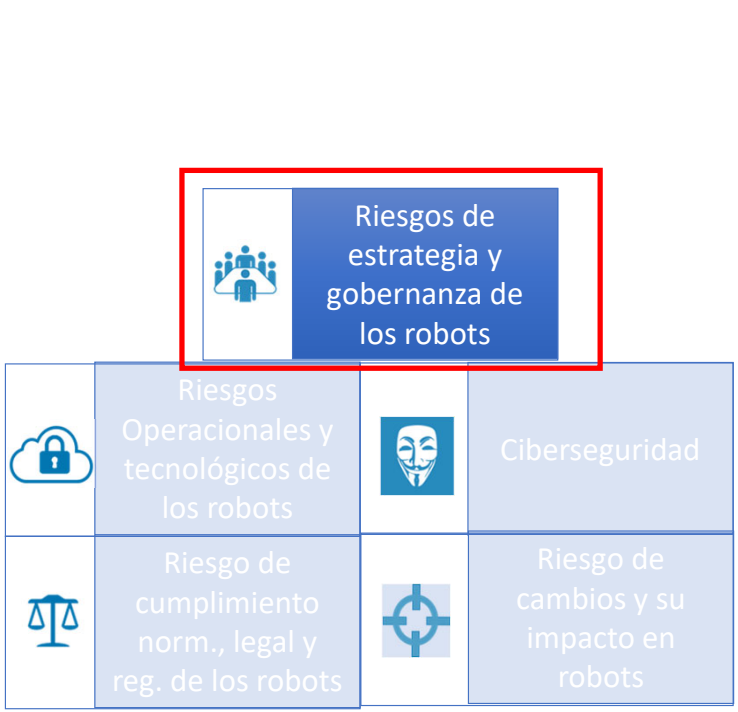
Particularidades de las tecnologías RPA / RDA: Se debe disponer de una Matriz RACI que incluya los roles y responsabilidades sobre las tecnologías de RPA / RDA y la robotización de procesos. Entre los roles, se deberían recoger:

- 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.

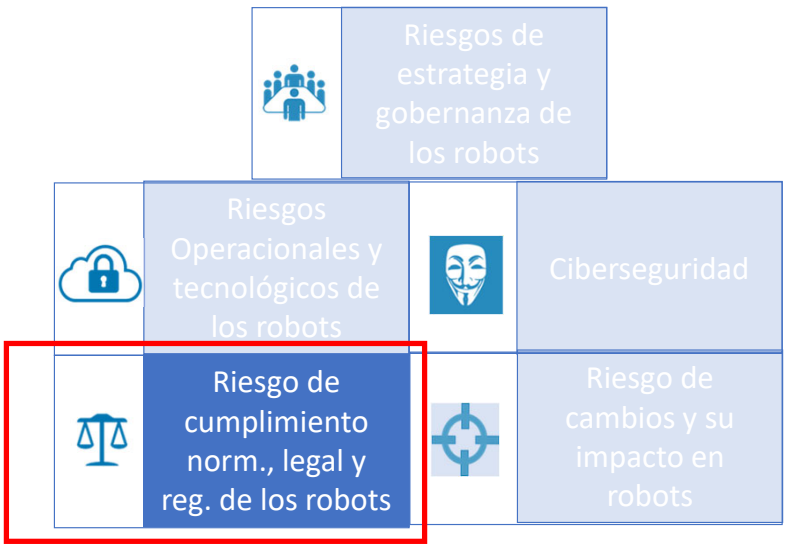
Instituto de Auditores Internos de España

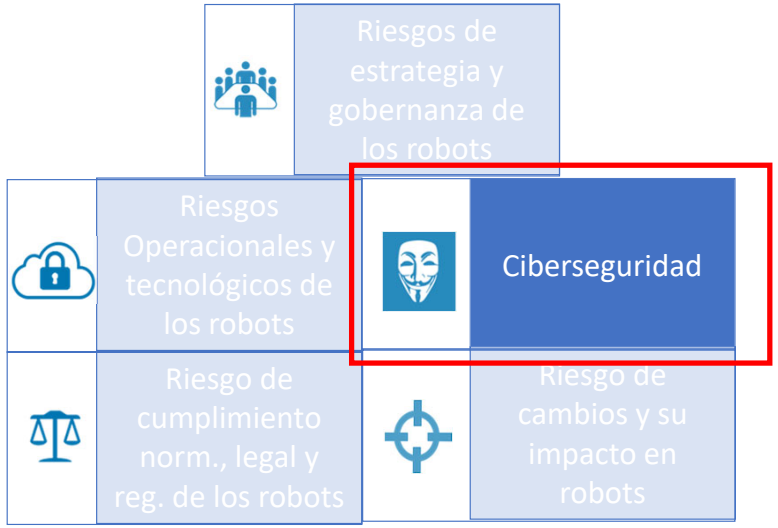
Riesgos significativos vinculados a la Robotización de procesos



Instituto de Auditores Internos de España

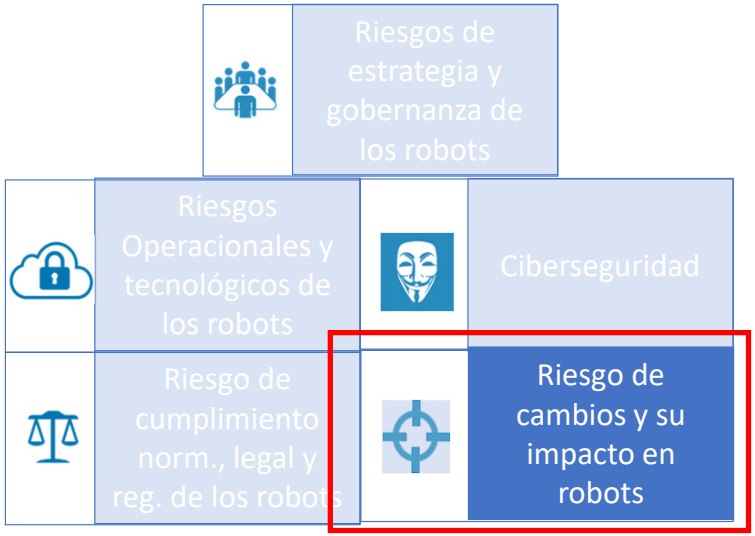
Riesgos significativos vinculados a la Robotización de procesos





Instituto de Auditores Internos de España

Riesgos significativos vinculados a la Robotización de procesos



Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos (enfoques y técnicas)

X

como “usuario”

En revisiones de asesoramiento

En revisiones de aseguramiento

Instituto de Auditores Internos de España

Auditoria Interna y la Robotización de procesos (enfoques y técnicas)

X

como “usuario”

En revisiones de asesoramiento

En revisiones de aseguramiento

Instituto de Auditores Internos de España