
Lineamientos para la Implementación de Soluciones de tipo RPA

1. Alcance.....	2
2. Automatización de Procesos Robóticos (RPA).....	2
3. Supuestos y Limitaciones.....	2
4. Lineamientos Generales.....	2
4.1 Diseño e Implementación.....	2
4.2 Mantenimiento y Operación.....	3
4.3 Seguridad y Datos.....	4
5. Control de Versiones.....	5

1. Alcance

El presente documento establece un conjunto de lineamientos y buenas prácticas para el diseño, implementación, mantenimiento, operación, seguridad y gestión de datos de soluciones basadas en Automatización Robótica de Procesos (RPA, por sus siglas en inglés) en la organización.

2. Automatización de Procesos Robóticos (RPA)

La Automatización Robótica de Procesos (RPA) es una tecnología que permite automatizar tareas repetitivas e interactuar con diversos sistemas informáticos mediante la configuración de flujos de trabajo ejecutados por agentes de software o "bots".

Estos bots emulan actividades operativas tanto de negocio como de TI, tales como la manipulación, validación y extracción de datos, la transferencia de información entre distintas aplicaciones, la activación de respuestas automáticas y la ejecución de transacciones complejas.

Las soluciones RPA no reemplazan los sistemas de información existentes, sino que interactúan con sus interfaces de usuario y servicios de manera análoga a la ejecución humana.

3. Supuestos y Limitaciones

- Se asume que la Unidad Usuaria dispone de las capacidades operativas y técnicas necesarias, ya sea propias o mediante terceros, para gestionar e implementar soluciones RPA.
- Se asume que la Unidad Usuaria posee las competencias necesarias (propias o de terceros) para la atención de incidencias, ajustes continuos y mantenimiento de las soluciones RPA desplegadas.

4. Lineamientos Generales

4.1 Diseño e Implementación

1. Previamente a la aplicación de una solución de automatización, la Unidad Usuaria ha identificado y corregido las ineficiencias en el proceso a automatizar.
2. La Unidad Usuaria debe priorizar la automatización de los procesos que están alineados a los objetivos de la organización.
3. Para el caso de sistemas gestionados por la unidad central (DTI), la Unidad Usuaria debe haber informado a DGTH en caso requiera de un usuario genérico (para la solución RPA) para interactuar contra los sistemas institucionales. La Unidad Usuaria es responsable por las acciones que se efectúen en los sistemas a través del usuario genérico solicitado.
4. La Unidad Usuaria debe verificar que cuenta con las capacidades necesarias para el despliegue y mantenimiento de la solución de tipo RPA: consideraciones técnicas del equipo sobre el que se desplegará el producto y habilidades por parte del equipo encargado de su despliegue y mantenimiento. En caso no cuenten con las habilidades necesarias, deberán gestionar la capacitación de sus colaboradores.

5. Las consultas y problemas que se tengan con relación a la herramienta de automatización, deberán ser canalizadas directamente al proveedor del servicio seleccionado por la Unidad Usuaria.
6. El proceso de automatización implica el traslado de funciones desde el colaborador hacia una solución de automatización. En consecuencia, como parte de la automatización parcial/total del proceso, la Unidad Usuaria ha identificado las funciones que la solución RPA estará asumiendo. Asimismo, en la unidad se debe asignar un responsable que valide y monitoree el adecuado funcionamiento del bot.
7. La solución RPA debe ser implementada asumiendo que pueden presentarse errores potenciales humanos.

4.2 Mantenimiento y Operación

1. La Unidad Usuaria cuenta dentro de su plan de continuidad de negocio con mecanismos que garanticen la continuidad de su operación en caso los procesos automatizados se vean interrumpidos. Asimismo, debe contar con procedimientos y tiempos establecidos para la rehabilitación de estos procesos automatizados interrumpidos.
2. La Unidad Usuaria debe contar con procesos para el respaldo de la configuración y parámetros de sus bots; en caso se requieran volver a desplegar debido a la falla y/o reemplazo del equipo en el que actualmente están instalados. Estas copias de seguridad deben ser almacenadas en una ubicación segura y - de ser posible - cifrada.
3. La Unidad Usuaria debe contar con métricas que permitan cuantificar el beneficio derivado de la automatización parcial/total del proceso.
4. La herramienta de automatización debe proporcionar información de monitoreo sobre las tareas que está automatizando. Con base en ello, la Unidad Usuaria debe contar con procedimientos de monitoreo que le permitan atender los problemas reportados por la herramienta; estos pueden incluir, de manera enunciativa más no limitativa:
 - Error en los sistemas con los que la herramienta de automatización interactúa.
 - Error en la configuración de la herramienta de automatización.
 - Error en las reglas de automatización de la herramienta.
 - Errores derivados de cambios en los sistemas con los que la herramienta de automatización interactúa.
 - Errores derivados de la actualización de otros componentes del equipo en donde se encuentra instalada la solución RPA; como: sistema operativo o antivirus.
5. En caso se decida dar de baja alguna de las tareas automatizadas que interactúan con alguno de los sistemas gestionados de forma centralizada (DTI), ya no requiriendo las credenciales asociadas, es responsabilidad de la Unidad Usuaria el informar a la Dirección de Tecnologías de Información para proceder con la baja de dicha cuenta de usuario.

6. La Unidad Implementadora (encargada de implementación de los bots) debe gestionar el catálogo de los bots actualmente desplegados, las unidades usuarias a las que brindan servicio y las labores que realizan cada uno de esos bots.
7. La Unidad Usuaria gestionará de forma autónoma los bots implementados sobre la herramienta de automatización.
8. La Unidad Usuaria debe designar dentro de su equipo a una persona responsable de validar, verificar y monitorear que los bots implementados funcionen de forma correcta. Esta persona asumirá la responsabilidad correspondiente ante escenarios específicos como omisiones en el monitoreo periódico, falta de validación oportuna de los resultados o incidentes derivados de una operación incorrecta del RPA dentro de su ámbito de competencia.

4.3 Seguridad y Datos

1. La Unidad Implementadora debe asegurar el acceso a las cuentas y credenciales utilizadas tanto para la administración de la herramienta de automatización, como por parte de la misma herramienta de automatización. Para lo cual debe tener en cuenta:
 - No se debe incluir las credenciales con privilegios dentro de los scripts de automatización y otras ubicaciones no seguras. Las credenciales deben ser almacenadas en una ubicación centralizada y cifrada.
 - Las credenciales que utilizará cada bot son de uso exclusivo de ese bot. Estas credenciales no deben ser de uso compartido con las labores que realice otro colaborador o bot dentro de la Unidad Usuaria por temas de seguimiento y para poder discriminar responsabilidades.
2. Los bots deben seguir los principios de “confianza cero”:
 - Identificar posibles riesgos derivados de la automatización del proceso; y en base a ello establecer planes de mitigación.
 - Contar con privilegios mínimos para poder realizar sus tareas.
 - Automatizar la recolección de datos para el diagnóstico de incidentes: fecha y hora, usuarios, endpoints, red, datos, backtrace, entre otros. Estos datos serán utilizados en caso se requieran realizar auditorías; o para análisis por parte de la Unidad Usuaria o Unidad Implementadora a fin de detectar comportamientos sospechosos.
3. En caso alguno de los bots en uso registre, modifique o elimine de forma incorrecta algún dato dentro de los sistemas a los que accede, es responsabilidad de la Unidad Usuaria el corregir estos datos oportunamente, a fin de evitar impactos derivados en otros procesos de la organización.
4. Los permisos que se otorgarán a la cuenta de usuario que será utilizada por el bot deben estar limitados a las funciones de la Unidad Usuaria.
5. Las credenciales utilizadas por la herramienta de automatización deberán cumplir las mismas políticas de seguridad que las cuentas de los colaboradores de la universidad (por ejemplo: reglas de complejidad o caducidad).

5. Control de Versiones

Fecha	Descripción	Versión	Autor
19 / Abr / 2022	Versión inicial	1.0	Dirección de Tecnologías de Información
26 / Abr / 2022	Ajustes lineamientos de mantenimiento y seguridad en base a retroalimentación recibida.	1.1	Dirección de Tecnologías de Información
02 / May / 2022	Se agregó un nuevo ítem sobre manipulación errónea de datos.	1.2	Dirección de Tecnologías de Información
16 / May / 2022	Se modificó un ítem relacionado a responsabilidades de la cuenta de usuario genérica.	1.3	Dirección de Tecnologías de Información