


Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

# Diseño de un marco de seguridad orientado a RPA (Robotic Process Automation) en la empresa Bridgestone SSC Costa Rica

Jiménez Rodríguez Emanuel

Matamoros Araya Luis

Noviembre, 2020

## Declaratoria de derechos de autor

Este documento es propiedad de los autores, los cuales, autorizan la reproducción parcial o total del mismo solamente para fines académicos, de lo contrario, queda prohibida su transmisión o reproducción bajo ningún medio.

## Agradecimientos

Primeramente, a Dios, porque sin Él nada de esto sería posible.

A nuestros padres, que han sido el eje central con su apoyo incondicional, siempre estando ahí cuando los necesitamos y que han contribuido enormemente a impulsarnos para lograr esta meta.

Queremos agradecer a nuestros profesores de Maestría, en especial a nuestro tutor Miguel Pérez, que con su esfuerzo logran compartir conocimiento para la correcta formación académica, y muchas veces dando la milla extra sin pedir nada a cambio. Sin duda que es algo digno de señalar. También agradecer a todos los miembros administrativos de la Universidad Cenfotec, que son los que hacen posible que las cosas pasen, al aportar su grano de arena para ofrecer una educación excelente y de calidad diferenciándose y poniendo en alto la educación privada.

A Pablo Aguilar, líder del equipo de Bridgestone RPA en Costa Rica, quien desde un inicio mostró su mayor disposición en colaborarnos en la tesis, en todo lo que fuera necesario, y siempre nos instó a la superación.

Por último, agradecer a nuestros amigos y amigas de carrera tanto de especialidad como de Maestría, que con sus palabras y consejos han servido de motivación y un pilar fundamental para lograr terminar este largo recorrido.

## Dedicatoria

La dedicatoria del presente proyecto va dirigida a nuestras familias, tanto padres como hermanos, tíos, abuelos y primos.

Emanuel Jiménez

También a mis ahijados Jocsan, Michelle, Sebastián, Anthony, a quienes deseo transmitirles el estudio como una de las mejores herramientas para defenderse en la vida, y a mi novia, Kathia, por el apoyo brindado a través de toda esta etapa.

Luis Matamoros

# Hoja de aprobación del proyecto

universidad cenfotec
tecnologías digitales

**Universidad Cenfotec**
*Carrera de Postgrado*
*Maestría en Ciberseguridad*

## TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para los estudiantes: **Emanuel José Jiménez Rodríguez** y **Luis Enrique Matamoros Araya**

Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2020.11.05 08:39:52 -06'00'

*M. Sc. Miguel Pérez Montero*
Tutor

WILLIAM RODRIGUEZ CALVO (FIRMA)
Digitally signed by WILLIAM RODRIGUEZ CALVO (FIRMA)
Date: 2020.11.05 09:57:39 -06'00'

*MSEG. William Rodríguez Calvo*
Lector 1

Ignacio Trejos Zelaya
Firmado digitalmente por Ignacio Trejos Zelaya
Fecha: 2020.11.20 09:59:25 -06'00'

*M. Sc. Ignacio Trejos Zelaya*
Lector 2

San José, Costa Rica, 04 de noviembre de 2020

*Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-*

## Tabla de Contenido

Declaratoria de derechos de autor ii

Agradecimientos iii

Dedicatoria iv

Hoja de aprobación del proyecto v

Resumen Ejecutivo 12

Capítulo 1. Introducción 13

1.1 Generalidades 13

1.2 Antecedentes del Problema 16

1.2.1 Historia de RPA en Bridgestone 21

1.2.2 Estado actual de Seguridad 30

1.2.2.1 Estándares de seguridad actualizados 31

1.3 Definición y Descripción del Problema 34

1.4 Justificación 35

1.5 Viabilidad 35

1.5.1 Punto de Vista Técnico 35

1.5.2 Punto de Vista Operativo 36

1.5.3 Punto de Vista Económico 36

1.6 Objetivos 36

1.6.1 Objetivo General 36

1.6.2 Objetivos Específicos 36

1.7 Alcances y Limitaciones 37

1.7.1 Alcances 37

1.7.2 Limitaciones 37

1.8 Estado de la Cuestión 37

1.8.1 Planificación de la revisión 37

1.8.1.1 Formulación de la pregunta 37

1.8.1.2 Selección de fuentes 38

1.8.1.2.1 Definición del criterio de selección de fuentes 38

1.8.1.2.2 Lenguaje de estudio 38

1.8.1.2.3 Identificación 38

1.8.1.3 Selección de los estudios 38

1.8.2 Ejecución de la revisión 39

1.8.2.1 Ejecución de la revisión en la fuente: Safari Books 39

1.8.2.2 Ejecución de la revisión en la fuente: BluePrism 40

1.8.2.3 Ejecución de la revisión en la fuente: Google Scholar 41

1.8.3 Análisis de Resultados 42

1.8.3.1 Presentación de Resultados 42

1.8.3.2 Comentarios finales 42

Capítulo 2. Marco Teórico 43

2.1 Amenazas, vulnerabilidades e impacto 45

2.2 Marcos de seguridad de la información y buenas prácticas 49

2.3 Gestión de la seguridad de la información 53

2.4 Herramienta de gobernanza, riesgo y cumplimiento (GRC) 53

2.5 Cumplimiento 56

2.6 Gestión de identidades 56

2.7 Auditoría 57

2.8 Robótica 57

Capítulo 3. Marco Metodológico 67

3.1 Tipo de Investigación. 67

Capítulo 4. Desarrollo de la solución. 71

Capítulo 5. Conclusiones y Recomendaciones. 84

5.1 Conclusiones. 84

5.2 Recomendaciones. 87

Capítulo 6. Trabajos de futuro. 88

Tabla de Acrónimos 89

Bibliografía 92

Anexos 94

Anexo 1 94

1 Solution Overview 97

1.1 Solution Description 97

1.1.1 Download Invoices 98

1.1.2 Send Email 100

2 Process Data 102

3.1 Triggers 102

2.1 Output 102

2.2 Scheduler 103

2.3 Work Queues 103

2.3.1 Invoices 103

2.4 Additional Controls 103

2.4.1 Environment Variables. 103

2.4.2 Credentials. 103

3.1 Technical 104

3.2 Business 104

Anexo 2 105

Portada 106

Categorías de riesgo 108

Eventos de Riesgo 112

Vectores de amenazas 115

Lista de controles con detalles de objetivos y actividades 118

Lista de controles con procedimientos de prueba y ejemplos de requerimientos de evidencia 175

Lista de controles según marcos de seguridad de la industria 254

## Lista de imágenes y tablas

Imagen 1 - Modelo DMAIC ..... 14

Imagen 2 - Las plataformas RPA se están convirtiendo rápidamente en el pegamento que une la automatización empresarial ..... 19

Imagen 3 - Resultados en el negocio de implementación de RPA PR to PO ..... 20

Imagen 4 - OPEX Onboarding, 2019..... 23

Imagen 5 - ¿Quiénes somos? ..... 24

Imagen 6 - ¿Qué hacemos?..... 24

Imagen 7 - Ciclo de vida de RPA ..... 25

Imagen 8 - La estrategia de triple ganancia ..... 29

Imagen 9 - Screenshot de página de Blue Prism..... 40

Imagen 10 - Captura de pantalla de página de Blue Prism ..... 41

Imagen 11 - Manejo de riesgos..... 56

Imagen 12 - Media Center ..... 61

Imagen 13 - Captura de pantalla de BluePrism ..... 62

Imagen 14 - Captura de Object Studio del software Blue Prism ..... 63

Imagen 15 - Aplicaciones de Blue Prism..... 64

Imagen 16 - Diagrama de Flujo en Object Studio ..... 65

Imagen 17 - Esperas Globales..... 66

Imagen 18 - Investigación aplicada ..... 68

Imagen 19 - Diagrama de Ishikawa: Análisis causa-efecto de los problemas ..... 71

Imagen 20 - Queue Populator ..... 79

Imagen 21 - Queue Populator ..... 80

Imagen 22 - Invoice Copies FSIP SAP Downloader ..... 81

Imagen 23 - Invoice Copies SAP Downloader ..... 82

Imagen 24 - Diseño por capas ..... 83

Imagen 25 - Captura de pantalla de Invoice Copies Report ..... 84

## Resumen Ejecutivo

El proyecto en curso y toda su investigación está dirigido específicamente hacia la operación del departamento de RPA de la empresa Bridgestone.

RPA es una tecnología emergente, la cual ha venido siendo adoptada de manera gradual por empresas en el nivel mundial, sin embargo, lleva de la mano varios retos, entre ellos el tema de la ciberseguridad o seguridad de la información. RPA, que en español significa automatización de procesos por medios de robots, es una rama que viene a sustituir el típico modelo de automatización comúnmente conocido, donde un desarrollador de software crea una aplicación con interfaz gráfica para llevar a cabo una serie de acciones, al utilizar interfaces de programación de aplicaciones (APIs) o lenguajes de *scripting*.

Al tener robots (*bots*) como una nueva fuerza laboral, éstos deben ser administrados, controlados y supervisados para verificar su rendimiento, seguridad y eficiencia.

Dado esto, es que se planea diseñar un marco o una matriz de controles de seguridad de la información que permita a la empresa Bridgestone evaluar sus robots durante el ciclo de vida de su desarrollo e incluso cuando estén en producción, con la finalidad de detectar posibles riesgos de seguridad y aplicar controles para disminuir el riesgo asociado a dicha tecnología.

**Palabras Clave:** RPA, robotic process automation, riesgos, amenazas, marco, matriz, controles, robótica

# Capítulo 1. Introducción

## 1.1 Generalidades

Debido al gigantesco avance tecnológico en la última década, el nacimiento de nuevas tecnologías conocidas como "emergentes" han sido clave para la innovación, automatización y revolución de lo que usualmente conocemos. La incorporación de nuevas ramas en dicha materia ha ocasionado la necesidad de una rápida adaptación y un escaso o a veces nulo planeamiento. El mercado laboral y la industria económica giran en torno al aumento de las ganancias para satisfacer los requisitos de sus accionistas, socios, fundadores e interesados, quienes esperan que su negocio sea fructífero a través del tiempo. Es por esto que muchas empresas han decidido cambiar la forma de hacer las cosas tomando esta nueva era tecnológica como su principal aliado y es precisamente en este punto donde los altos jerarcas (CEO, CIO, entre otros) buscan la mejor manera de ser agentes de cambio.

Como parte de esta evolución digital, toma auge la inteligencia artificial, conocida por sus siglas IA o en inglés AI. Las técnicas y aplicaciones desarrolladas en IA son numerosas, entre ellas destaca la automatización inteligente, al dar paso a *chatbots*, automatización cognitiva, automatización de procesos por medio de robots, en inglés *Robotic Process Automation* y conocida por sus siglas como RPA, entre otros, siendo esta última el punto de enfoque para el presente trabajo de investigación.

Como grupo de trabajo se ha aprendido y adoptado, a lo largo de esta carrera, que buscar y generar impacto siempre ha sido uno de los pilares por cumplir, por ende, la innovación es vital para lograr dicho objetivo. RPA es una derivación de la inteligencia artificial y es un tema relativamente nuevo, las fuentes y recursos de información son escasos por lo que el avance en esta investigación dejará grandes contribuciones a la empresa Bridgestone, y posiblemente a un mercado emergente que tenderá en el futuro próximo a usar estas tecnologías, especialmente los SSC. El establecimiento de centros de excelencia (CoE) de RPA en empresas transnacionales de gran renombre, ha despertado una latente preocupación en diversas áreas como la seguridad de la información y la ciberseguridad, la cual busca ser abarcada y minimizada por medio de este trabajo. Más allá de esto, Bridgestone, al ser una empresa de origen japonés, tiene muy arraigados los conceptos de calidad y de mejora continua. La identificación de diversas brechas y puntos por

mejorar definitivamente es un aspecto muy importante en sus labores diarias, por medio de metodologías como Lean Six Sigma, y el modelo Shingo.

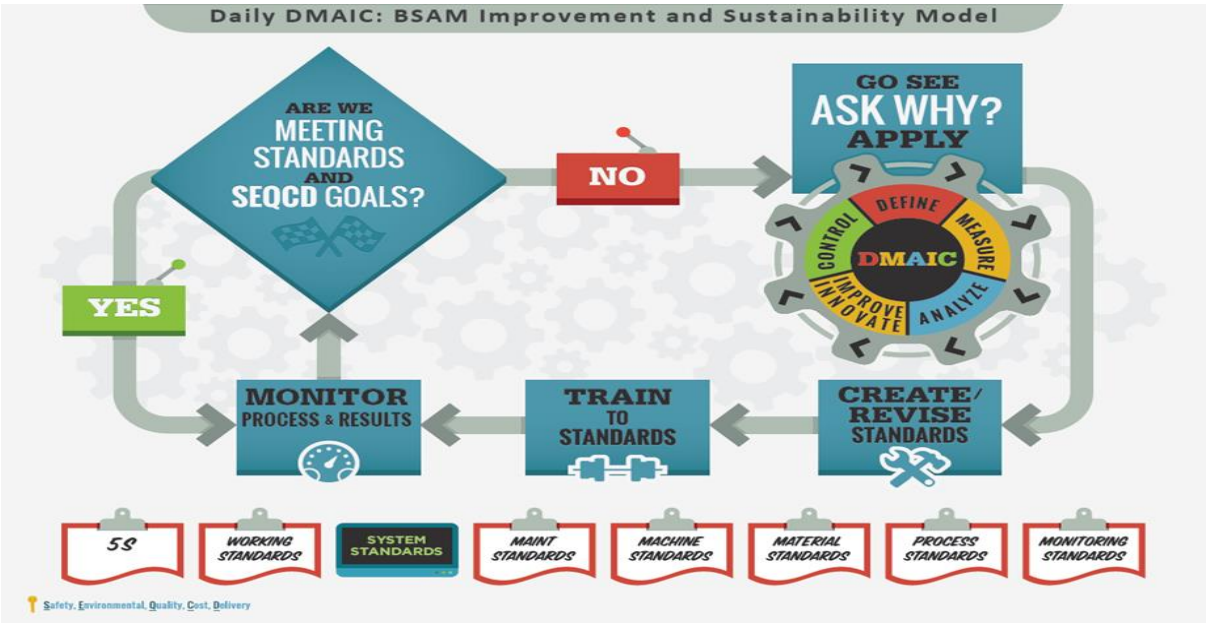



Imagen 1 - Modelo DMAIC

Fuente: Presentación OPEX 2020, Bridgestone

La falta de experiencia de personal en el tema de la ciberseguridad, o incluso la poca o escasa presencia de especialistas en seguridad de la información al tomar decisiones, llevan a empresas medianas e incluso algunas de gran renombre, a adoptar tecnologías emergentes como RPA sin una debida planificación, donde lastimosamente dejan áreas como la seguridad, fuera de la estrategia y el diseño, provocando que el riesgo empresarial aumente al usar tecnologías que deberían funcionar bajo un ambiente controlado y de cumplimiento.

Al no existir una adecuada evaluación y gestión de riesgos, surge como consecuencia una ausencia de controles de seguridad, necesarios para operar la tecnología de manera segura, exponiendo a la empresa a posibles riesgos, estos varían dependiendo de la probabilidad de ocurrencia y el impacto de las amenazas. De la mano con esta problemática, se une la falta de gobernanza de seguridad en las organizaciones, entre ellos la falta de comunicación de políticas, estándares y normas que regulen a la tecnología, así como la carencia de un marco de seguridad específico en el departamento, que sirva como una guía hacia los colaboradores e interesados.

Actualmente no existe ningún marco de seguridad a nivel industrial que guíe y oriente sobre seguridad de la información en RPA. Adicionalmente, tampoco ha sido creada alguna norma o estándar como una buena práctica de mercado que establezca controles para dicha tecnología. Tal como se mencionaba anteriormente, las investigaciones son pocas y la información disponible es escasa, por consiguiente, se busca llenar ese faltante y ayudar a empresas como Bridgestone a reducir su superficie de ataque, al disminuir sus niveles de riesgo mediante controles de seguridad diseñados y adaptados a las necesidades del negocio en términos legales, de cumplimiento, regulatorios, internos, operativos, entre otros.

La inexistencia de normas o estándares globales de seguridad en RPA, se debe primero a la rápida evolución de esta tecnología en los últimos años, seguidamente del poco interés que han manifestado organizaciones internacionales como la ISO, NIST, ISACA, etc. en la construcción de materiales disponibles para el público necesitado de asegurar y acomodar dichas prácticas a sus ecosistemas de RPA. Por último, la creciente demanda de servicios de seguridad en este tema ha ocasionado que muchos esfuerzos se estén realizando en privado, con el fin de vender el servicio o producto enfocado en solucionar dicha incertidumbre. Dentro de estos esfuerzos podemos resaltar soluciones como CyberArk.

Finalmente, los líderes de software RPA, tales como UiPath, Blue Prism y Automation Anywhere, a pesar de haber incorporado características de seguridad como parte del diseño del software, estas han quedado cortas dado que son bastante básicas y venden una sensación de falsa de seguridad en los compradores. Esta situación señalada es común en varias empresas que fabrican productos o que venden servicios-productos digitales.

Bajo todo ese contexto descrito es que el presente trabajo de investigación tiene un valor importante como apoyo para la organización Bridgestone y su centro de excelencia de RPA.

Teniendo claro todo esto, lo que se busca es generar un marco híbrido de controles de seguridad tomando en cuenta regulaciones, normas, políticas, necesidades del negocio, etc. Dicho marco se asemeja a una matriz cruzada de controles para automatizar labores de auditoría, evaluar y añadir controles al actual proceso de diseño de robots y gestionar los riesgos pertinentes. Dentro de estos controles se hizo el análisis del departamento de RPA de Bridgestone SSC.

El interés, finalmente, siempre será mantener la operación de RPA en funcionamiento sin afectar la producción, asimismo que no se detengan las operaciones por la inclusión de controles de seguridad, por el contrario, se busca que la seguridad sea un aliado del proceso de planeamiento, diseño y puesta en marcha de los robots para que Bridgestone asegure el uso de esta tecnología, cumpla con las necesidades del negocio, tanto en el nivel de clientes, aliados, proveedores e interesados. Como parte de los entregables, se genera un manual de introducción al marco, para que la curva de aprendizaje no sea complicada y en el nivel de empresa se reduzcan tiempos, tanto de estudio, como planeamiento y de reacción y respuesta a amenazas, a la vez que los riesgos se minimizan.

## 1.2 Antecedentes del Problema

Conscientes de la rápida adopción de RPA por parte de la industria y diferentes negocios, en términos de beneficios, tal y como señala el Instituto de RPA e IA (IRPAAI), entre ellos destacan la reducción de costos de un 25% a 50%, la ejecución 24x7x365, una mejora en el servicio entregado, reducción de la necesidad de entrenamientos, eliminación de tareas rutinarias y el aprovechamiento de las capacidades de los empleados en procesos más analíticos (Definition and Benefits | IRPAAI, n.d.), sin duda alguna RPA es una de las tendencias tecnológicas con mayor crecimiento.

"La automatización robótica de procesos tiene la flexibilidad de adaptarse a las demandas cambiantes sin limitaciones de recursos para la redistribución" (Kalra & Eisnor, 2015). RPA es un habilitador de alto valor para procesos con picos estacionales. Por ejemplo, los departamentos de ventas tienen picos estacionales regulares antes de la temporada navideña. Cuando una empresa recibe una cantidad excepcional de pedidos, los robots pueden programarse fácilmente para satisfacer la demanda actual de tareas que son de suma importancia (Smith, 2016). Sin embargo, es evidente que un empleado necesita mucho más tiempo para adaptarse y volverse competente para las nuevas responsabilidades. Otros beneficios incluyen reducción de costos, mayor eficiencia y capacidad.

El líder de automatización de Cognizant, Matthew Smith (2016) explica que las tareas manuales, repetitivas y detalladas completadas por mano de obra humana a menudo pueden contener errores y requerir mucho más tiempo. Además de eso, implica que una fuerza de trabajo

digital trae el beneficio de una implementación 24/7. En consecuencia, con RPA integrada en los procesos comerciales centrales, las empresas pueden eliminar los cuellos de botella operativos. Un robot desplegado normalmente puede hacer el trabajo entre dos y cinco equivalentes a tiempo completo (Craig et al., 2015). En adelante, la reducción de los costos equivalentes a tiempo completo (FTE) puede proporcionar a las empresas un gran retorno de la inversión (ROI). La automatización brinda oportunidades para redistribuir la fuerza laboral humana en más tareas de valor agregado, resolución de problemas y orientadas al cliente. De hecho, si aumenta la intensidad de la tecnología y la automatización, los empleados se vuelven más creativos, productivos, colaborativos y mejores tomadores de decisiones" (Indruškevičs, 2018, p14).

Múltiples estudios demuestran que muchas personas no disfrutan lo que hacen en sus trabajos, gran parte de sus tareas son repetitivas o no tienen valor agregado alguno, incluso no son atractivas ni productivas si se analizan de cerca. Es por esto que RPA busca sacar ese robot del ser humano, ocasionando así beneficios colaterales como los mencionados anteriormente:

Según el informe reciente de Harvard Business Review, el 30% o más de las actividades laborales actuales pueden automatizarse mediante tecnologías disponibles o futuras (Chui, Manyika y Miremadi, 2015).

Según estimaciones de los investigadores de la Universidad de Oxford, alrededor del 47 por ciento del empleo total en Estados Unidos se encuentra en la categoría de alto riesgo (Frey y Osborne, 2013). Frey y Osborne concluyen que, con más del 95% de certeza, las profesiones administrativas en seguros, corretaje, bancos, contabilidad, auditoría y finanzas se consideran altamente aplicables a la automatización. Además, se espera que estos trabajos se automaticen durante las próximas dos décadas. (Indruškevičs, 2018, p. 9).

RPA nos habilita para ser humanos de nuevo, permitiendo a las personas interactuar creativamente, al colaborar en actividades y proyectos que son inspiradores y alineados con un propósito, brindando realmente un valor agregado a la empresa. RPA puede llegar a eliminar el estrés asociado a tareas complejas y mecánicas, mejorar la productividad y creatividad de los empleados, permitiéndoles realizar tareas más analíticas e inteligentes. Además, no presenta problemas para los diferentes departamentos, al contrario, es de ayuda:

> Sin embargo, RPA se diferencia al extinguir varias limitaciones, al no ser disruptivo y al trabajo flexible y compatible con los sistemas existentes. Se considera que el RPA no es invasivo para los sistemas de TI porque es posible conectarse a la planificación de recursos empresariales (ERP) existente y la gestión de relaciones con el cliente (aplicaciones CRM (Bindal, 2015). Además, los desarrolladores tienen como objetivo programar los procesos para replicar directamente acciones, por lo tanto, el software RPA se considera no invasivo tanto para los sistemas de TI como para los procesos comerciales. (Indruškevičs, 2018)

Uno de los antecedentes principales de RPA es la automatización que utiliza computación tradicional (.NET, SQL, python, Selenium, Postman, por citar unas cuantas herramientas). Las citadas áreas emplean software para automatizar procesos de negocio, pero RPA toma un paso gigante en varios aspectos donde la computación tradicional no puede competir, entre ellos se destaca el fácil uso del software con una interfaz gráfica amigable, una sencilla y rápida automatización sin necesidad de contar con personal altamente calificado, así permitiendo a gente que conozca del negocio, poder aportar en la automatización de sus propios procesos; personalización y flexibilidad de adaptación con otras aplicaciones, servicios, y otros, además de brindar un enfoque mayor hacia las tareas que los humanos realizan, en lugar de las que realizan las aplicaciones, en comparación con la computación tradicional, la cual se traduce en programación como base, el uso de APIs, los problemas con el código fuente, sistemas heredados, involucración de varias áreas de TI para implementar una solución, personal capacitado para soportar las plataformas y muchas otras desventajas contra las que no puede competir contra RPA.

**¿Qué es RPA?**

"Robotic Process Automation es un software con capacidades de aprendizaje e Inteligencia Artificial preparado para manejar tareas repetitivas de alto volumen en las que previamente se requería a un humano para poder ejecutarlas" (CyberArk, 2020)

Por medio de RPA podemos manipular diferentes programas, y así recrear la labor de un humano, tomando en cuenta todo el ecosistema de aplicaciones que utiliza.

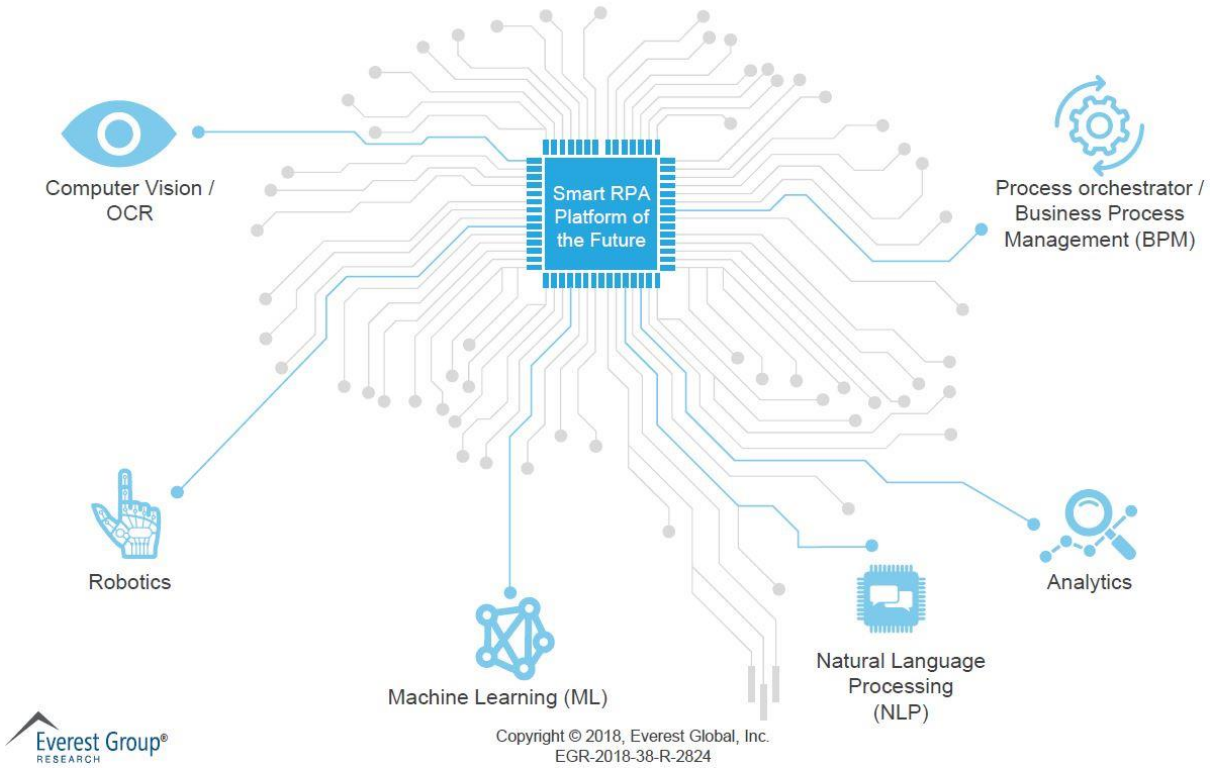



Imagen 2 - Las plataformas RPA se están convirtiendo rápidamente en el pegamento que une la automatización empresarial

Fuente: Lacity, M. & Willocks, L., 2017

La automatización robótica de procesos (RPA) es una tecnología comercial lista para usar de bajo código o sin código que se puede utilizar para automatizar tareas repetitivas basadas en reglas. Como una macro de Excel que opera dentro de una hoja de cálculo, RPA puede registrar acciones realizadas en una computadora personal, sistemas de acceso y realizar tareas delineadas para usuarios humanos. Los productos RPA varían en sus capacidades exactas, pero todas las tecnologías RPA emulan acciones humanas, lo que permite a los propietarios de procesos o al personal con la capacitación adecuada diseñar, probar e implementar automatizaciones rápidamente y reducir drásticamente la carga de trabajo de bajo valor de una organización. Los usos populares de RPA incluyen la entrada de datos, la reconciliación de datos, la

manipulación de hojas de cálculo, la integración de sistemas, la generación de informes de datos automatizados, el análisis y la comunicación y el contacto con los clientes. (The Federal RPA Community of Practice, 2020)

**Beneficios de RPA:**

- Reducción considerable de costos
- Ayuda 24/7, sin cansancio, sin enfermedades, sin retrasos, sin excusas
- Los robots hacen exactamente “lo que se les dice”
- Reduce los tiempos promedio de ejecutar transacciones típicas de humanos
- Menor probabilidad de fallos

Ejemplo

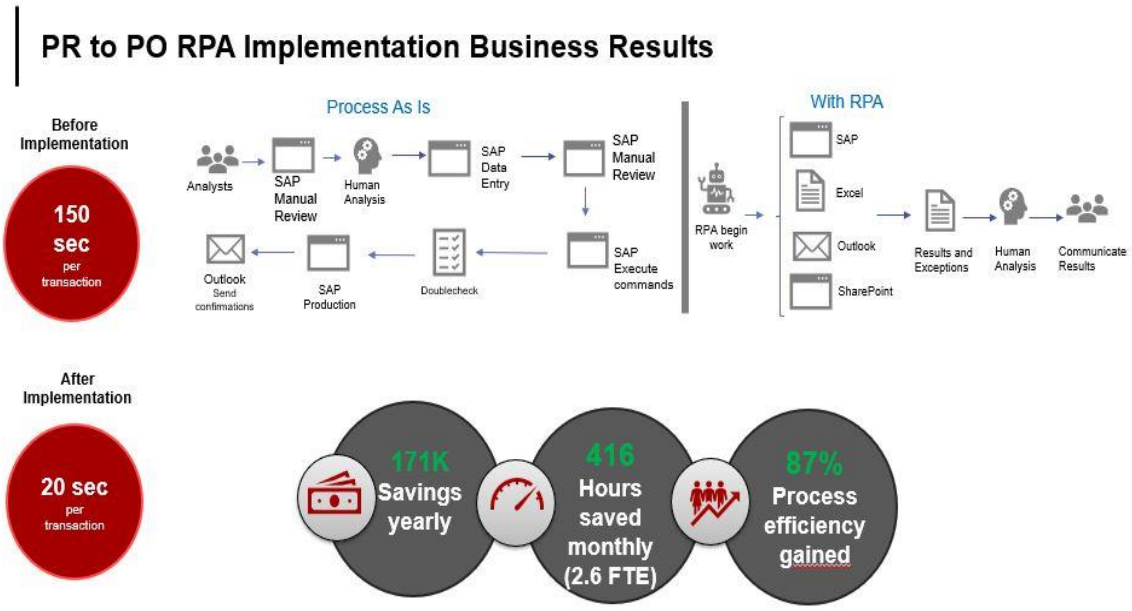



Imagen 3 - Resultados en el negocio de implementación de RPA PR to PO

Fuente: Bridgestone, 2019

**Riesgos de RPA**

- Credenciales en repositorios hechos a la medida
- Las credenciales son guardadas en el código, compartidas o reutilizadas
- Las credenciales a menudo permanecen sin cambios (Mala práctica: “Si no falla, no lo toques”)
- Nadie monitorea la creación de procesos RPA en las consolas de administración
- Exfiltración de datos en robots sin seguimiento
- Mayor superficie de ataque

(CyberArk, 2020)

RPA está actuando como una iniciativa de cambio de juego en la construcción del siguiente nivel de capacidades de excelencia operativa internamente, que se convierte directamente en una estrategia de ventas para negocios adicionales con clientes existentes o potenciales. En algunos casos, el negocio adicional puede resultar en la canibalización de los flujos de ingresos existentes, pero los proveedores de servicios están reconociendo que esto es inevitable. Cualquier reticencia para hacerlo puede correr el riesgo de perder clientes existentes frente a la competencia. Por el contrario, esto también podría ser una estrategia para recuperar clientes previamente perdidos. (Mindfields, 2015)

### 1.2.1 Historia de RPA en Bridgestone

“El Centro de Servicios Compartido Bridgestone SSC Costa Rica fue puesto en funcionamiento en octubre del 2012 y es resultado de una decisión estratégica orientada a abrir un centro de servicios compartidos para la región con sede en Costa Rica”. Durante el 2016, se amplía la cantidad de personal en 100 plazas, mientras se posiciona como una de las empresas más destacadas para trabajar a escala de Centroamérica y el Caribe, según el Instituto Great Place To Work (2020).

Rápidamente, se crea OPEX, dentro del centro de servicios compartido, con el fin de crear un área de optimización de procesos dentro del mismo, utilizando las mejores prácticas:

> Apoyar al Negocio para lograr mejores resultados a través de una metodología común que ayude a aprovechar herramientas y sistemas, desarrollar comportamientos alineados con nuestros principios fundamentales enfocados en valor agregado, reducción de costos, mejora continua, yokoten, simplicidad inteligente y resultados sustentables (Bridgestone Operational Excellence, 2019)

Dentro de los proyectos que maneja OPEX, definitivamente se toma en cuenta la automatización como uno de los medios para mejorar los procesos, y se comienza a formar un equipo de programación.

Inicialmente, las soluciones de automatización de procesos se manejaban por medio de macros y SAP scripting (SAP 5). Estas fueron de gran ayuda, lograron automatizar trabajos manuales que realizaban los trabajadores con macros de Excel y también SAP, sin embargo, a partir de estas se cae en noción que no se lograban satisfacer todas las necesidades del negocio, y estaban limitadas a ciertas aplicaciones. Aparte, la falta de estándares y normas provocaba que no se tuviera un orden adecuado.

A finales del 2017, se decide crear el departamento de RPA de Bridgestone para automatizar procesos y generar ahorros dentro del Centro de Servicios Compartido. Primeramente, se intentó coordinar con el departamento de TI para la creación de este, sin embargo, al departamento la propuesta no le llamó mucho la atención, por lo que finalmente se creó dentro del centro de excelencia en la parte de finanzas (OPEX). Dentro de este centro de excelencia, muchas de las probables soluciones que se planeaban crear requerían de automatización avanzada, es por esto por lo que se crea el departamento de RPA, como una mano del centro de excelencia.

Después de ciertas reuniones entre los encargados del centro de excelencia, estos son encargados para comenzar a automatizar ciertas tareas.

Luego de analizar diferentes opciones y buscar ayuda de empresas externas, se comienza una prueba de concepto de RPA, al utilizar el software Blue Prism, con un robot para la planta de México y otro para la planta de Norteamérica. Los resultados fueron exitosos, de manera que seguidamente se aumenta la prueba de concepto, y se realiza con un robot para cada área. Se implementan los primeros robots fuera de finanzas, se completa la POC (Prueba de concepto), y se crea oficialmente el departamento de automatización.

En ese momento se cae en la noción de *Compliance Acceptance*, ya que el producto se convierte en algo bastante serio. Cuesta encontrar en el mercado una solución adecuada en el nivel de seguridad y *Compliance* en RPA.

Como la creación del departamento de RPA se realiza en el departamento de finanzas, las mejores prácticas de TI no están alineadas con el departamento de RPA, hay una desconexión entre las mejores prácticas y políticas de TI hacia RPA. Esto provoca que poco a poco, mientras el departamento crece, se vayan identificando ciertas brechas que se deben ir cerrando.

Hasta este momento, la organización del equipo es un poco "lineal"

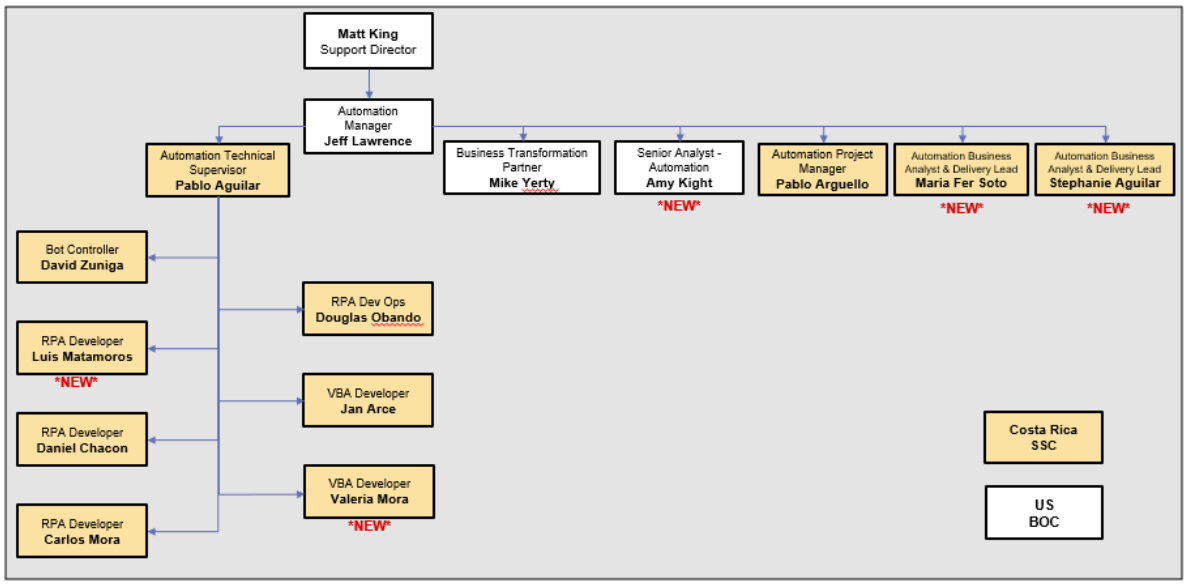



Imagen 4 - OPEX Onboarding, 2019

Fuente: Presentación OPEX 2019, Bridgestone

En el 2020, después de cierta madurez en el equipo de RPA, se definen ciertos subgrupos, llamados "squads" dentro del mismo. Esto son, equipos de trabajo con metodología scrum con trabajos específicos, con el plan de acelerar los procesos y planes de RPA, con metas bastante grandes, volviéndose mucho más dinámicos.

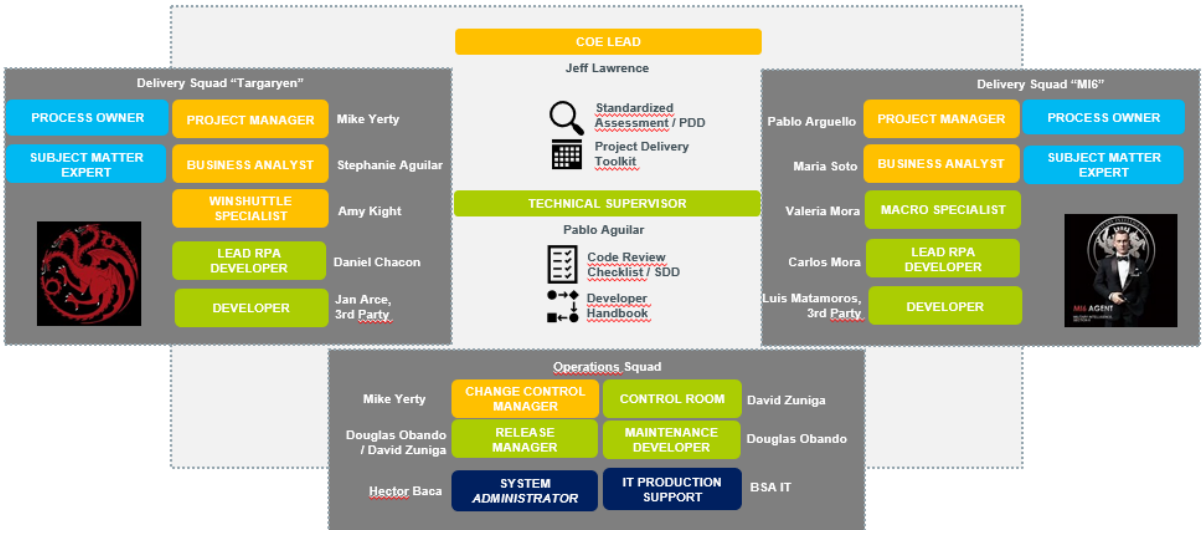



Imagen 5 - ¿Quiénes somos?

Fuente: Bridgestone, 2020

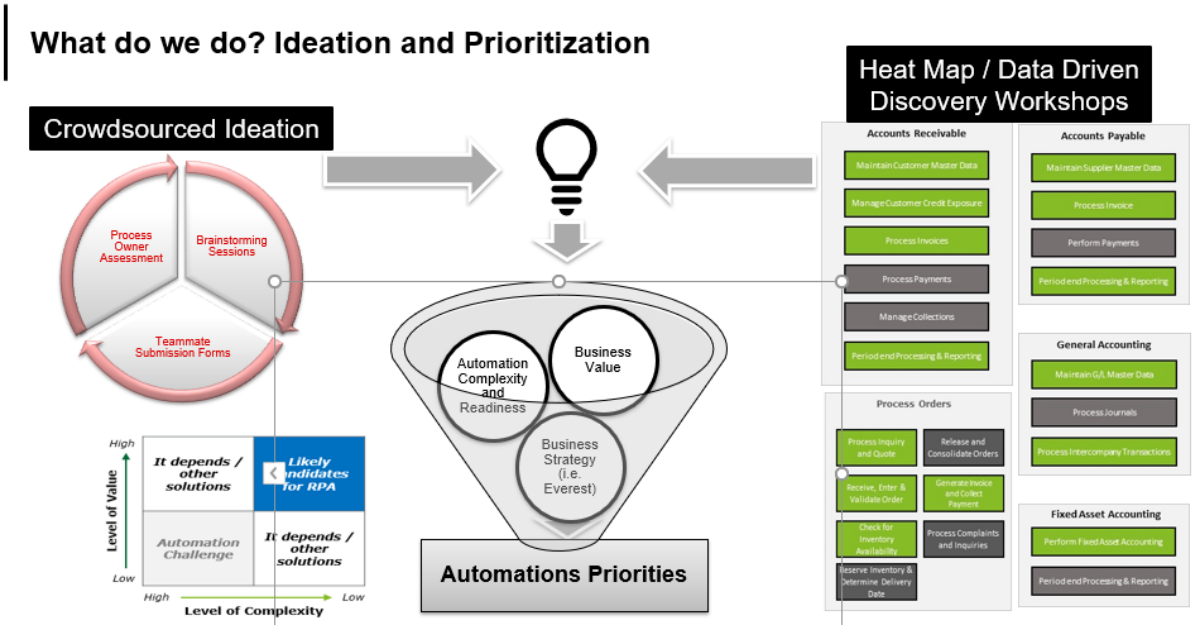



Imagen 6 - ¿Qué hacemos?

Fuente: Bridgestone, 2020

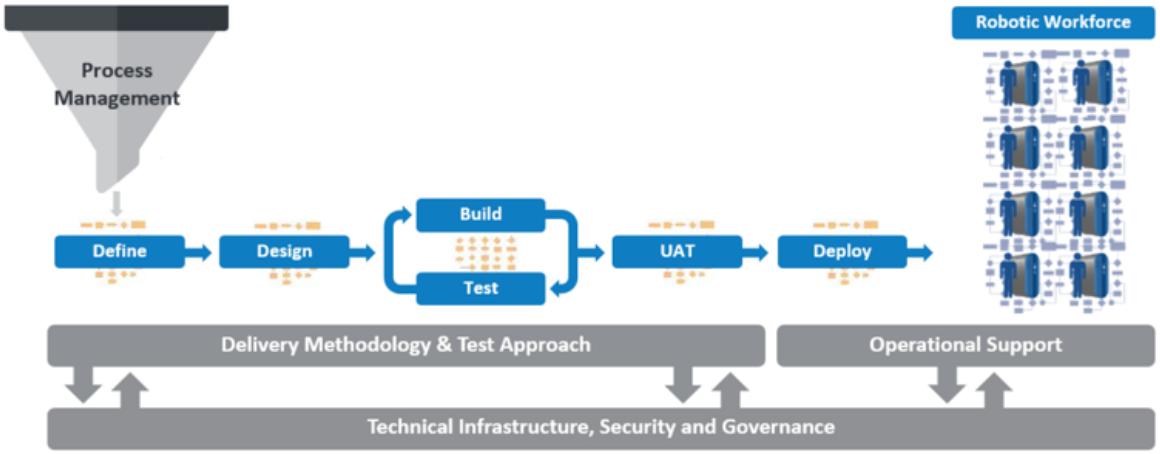



Imagen 7 - Ciclo de vida de RPA

Fuente: Bridgestone, 2020

En el nivel de seguridad, tal como se había mencionado en secciones anteriores, los diseñadores de software para RPA han venido agregando funcionalidades importantes, compatibilidad con otras herramientas y servicios de seguridad, pero esto no basta para cubrir con todos los riesgos que implica adoptar una tecnología como esta. Por ejemplo, el software RPA de la compañía Automation Anywhere utiliza la técnica de *hashing* para controlar contraseñas al usar un algoritmo detallado y personalizado, el de Blue Prism cuenta con un control de credenciales, sin embargo, para poner por ejemplo uno de estos riesgos, fácilmente cualquier programador puede tener acceso a estas contraseñas, directamente en Blue Prism. El solo hecho de implementar RPA crea nuevos riesgos. Ernst & Young, (2016) afirma:

"La automatización robótica de procesos afecta los procesos comerciales centrales y numerosas partes interesadas; por lo tanto, la implementación de un software RPA lleva varios riesgos importantes. Entre el 30 y el 50% de los proyectos iniciales de RPA fracasan".

Sin embargo, las empresas pueden mitigar los riesgos y evitar fallas creando una evaluación de riesgos, formando un marco de gobierno y un diseño de procesos. "Las cinco dimensiones del modelo operativo de RPA incluyen: organización, gobernanza, personas y cultura, tecnología y procesos" (Bauermann, 2017). Según Bauermann (2017), las empresas que no han creado un modelo operativo antes de la implementación de RPA a gran escala están bajo

la amenaza de un mayor tiempo de inactividad de los procesos comerciales y una sostenibilidad vulnerable. Además, un modelo operativo establecido con éxito crea mecanismos de control, pautas de desarrollo y se denomina Centro de Excelencia.

> Un CoE es un símbolo de su compromiso con la automatización de procesos y su dedicación a agregar valor e identificar oportunidades para mejorar. Una vez que haya creado su Centro de Excelencia, su CoE se convierte en un imán para desarrollar y atraer lo necesario en cuanto a habilidades y capacidades. Levante la bandera sobre su CoE, y esto se convierte en una invitación para cada operación comercial en su organización para identificar nuevas necesidades de optimización y descubrir oportunidades para aumentar la eficiencia y reducir los costos. Su CoE de automatización también ayuda a garantizar una gobernanza estructurada. Con la asistencia de expertos adecuada, su CoE establecerá metodologías, creará formación, identificará las mejores prácticas y adoptará las herramientas más eficaces.
>
> Puede pensar en un CoE como una oficina o departamento dentro de su organización, pero esa vista pierde el elemento más importante: las personas dentro del centro, lo que hacen y cómo el centro y su gobernanza fomenta colaboraciones fructíferas. La composición del equipo de gobierno de su CoE es una parte fundamental de su plan de mejora. Al igual que cualquier otro tipo de equipo de gestión, el CoE está compuesto de miembros que utilizan su experiencia y habilidades para lograr los resultados esperados. Crear tu centro significa traer juntos los analistas de negocios adecuados, expertos en conectividad, ciberseguridad, desarrolladores de automatización, formadores y gurús de la gestión del cambio.
>
> Un excelente gerente de proyectos coordinará todos estos recursos en múltiples proyectos de automatización. El equipo de CoE proporciona el cerebro detrás de los proyectos de automatización, y trabaja directamente con representantes de varios departamentos de la empresa que se convierten en propietarios de negocios de los proyectos individuales. El equipo de CoE ayuda a identificar posibles proyectos de automatización y medir su valor, y luego colaborará con el propietario de negocios para diseñar, entregar y mantener estos proyectos.

Este proceso es continuo, vivo y dinámico. Incluso después que un proyecto ha resultado en una implementación de automatización, el trabajo no está listo. El equipo de CoE se mantiene en contacto con el ámbito empresarial, donde se ha entregado la automatización. El contacto continuo asegura que se han realizado los cambios correctos y que el valor se realiza a largo plazo. (Kaelble, 2018)

Para llegar a un Centro de excelencia de automatización de procesos robóticos, las empresas deben mitigar los riesgos evaluados previamente. Si bien algunos riesgos son distintos y requieren una gran atención en las primeras etapas de los proyectos *piloto, otros* riesgos son continuos. **"Los riesgos de RPA se pueden clasificar en tres categorías integrales: riesgos de gobernanza, riesgos tecnológicos y riesgos operativos."** (Indruškevičs, 2018)

**Los roles clave en los CoE:**

Tenga en cuenta que cada organización es única y diferente, y una misma receta definitivamente no sirve para todas. También sepa que en algunos casos la misma persona puede ser llamada para llenar más de uno de estos roles en el equipo de automatización CoE:

- Gerente de CoE. El gerente de CoE dirige y coordina todos los recursos y actividades relacionados con el centro de automatización de excelencia.
- Analista de negocio de automatización. La persona que desempeña esta función es un experto en la materia que analiza los desafíos potenciales e identifica soluciones de automatización. El analista trabaja con grupos empresariales para priorizar posibles casos de uso, luego crea los documentos de diseño detallados que el equipo de desarrollo utiliza para completar cada proyecto.
- Responsable técnico de automatización. Esta función puede denominarse maestro de desarrollo de automatización y supervisa la calidad de los resultados de los desarrolladores y difunde las mejores prácticas en Equipo de desarrollo. Este rol también ayuda a definir la capa de implementación (común o local).

- Desarrollador de automatización. Esta es la solución de un extremo a otro creador, el experto que ejecuta las diversas automatizaciones y procesos mediante el uso de herramientas como NICE APA Designer para crear proyectos de automatización robótica.
- Ingeniero de conectividad de automatización. Es la persona que gestiona y mantiene la capa de integración.
- Administrador de automatización. Este es el rol responsable de gestión técnica y mantenimiento de soluciones de automatización.
- Líder de gestión de cambios y despliegue de automatización. La implementación exitosa depende de esta persona, que maneja las actividades de educación y capacitación para todas aquellas personas que utilizarán la solución de automatización. Esta persona supervisa todas las actividades de gestión del cambio, sin cuya máxima adopción es difícil de lograr.
- Analista de datos de automatización. Este miembro del equipo define y mide el valor de automatización.
- Automation tester. Este miembro del equipo de CoE que ejecuta las pruebas de soluciones de extremo a extremo. El ejecuta la prueba de varios procesos de automatización, generalmente al utilizar tales herramientas como software NICE Automations en el entorno de prueba.
- Las pruebas incluyen el manejo de errores y la validez de los datos. (NICE RPA Team, 2018)

Las soluciones tecnológicas de tendencia como RPA son blanco de ataque por sus débiles y escasos controles de seguridad para proteger el ecosistema, debido a su obvia falta de madurez en campos como la ciberseguridad. También, aumenta el peligro el saber que estos softwares actúan y tienen acceso a muchos datos delicados como lo suele hacer un humano. Los líderes de empresas que adquieren dichas soluciones no toman en cuenta aristas cruciales en la seguridad dentro de un ambiente de RPA. Algunas de éstas son el marco regulatorio, la ciberseguridad, el riesgo tecnológico, el manejo de riesgos de terceros, riesgo de operaciones, etc. Dependiendo de la madurez en el nivel de seguridad de una empresa, la adquisición de RPA puede llevar consigo un gran riesgo inherente que si no es gestionado de manera correcta podría impactar al negocio gravemente.

Los ejecutivos y supervisores de RPA no deben centrarse solo en el retorno de la inversión (ROI) y la reducción de costos equivalente a tiempo completo (FTE). Puede haber muchos beneficios magníficos a corto plazo, pero con una estrategia incorrecta, existe una buena posibilidad que la empresa lo pague en riesgo y escala, a largo plazo (Hodge, 2017).

La Figura 5 representa el marco de Willcocks & Lacity (2017), y describe la estrategia de "triple ganancia", donde los accionistas, clientes y empleados comparten mutuamente el valor creado a partir de la automatización."




Imagen 8 - La estrategia de triple ganancia

Fuente: Lacity, M. & Willocks, L., 2017

A partir de los riesgos a los que se ve expuesto RPA si no se toman las medidas necesarias, es que se piensa en la implantación de un *framework* de seguridad, ya que el mismo puede ayudar a minimizar los riesgos. Por medio de este *framework*, se planea ayudar especialmente a las organizaciones que no cuentan con un equipo de RPA suficientemente maduro, sin embargo, se pretende que el contenido de este documento también sea útil para ayudar a empresas con una gran madurez en seguridad, que se encuentren comenzando en RPA.

También se considera material de gran ayuda para empresas de tipo Centro de servicios compartido que tengan incertidumbre acerca de la seguridad en RPA.

### 1.2.2 Estado actual de Seguridad

Con el fin que este documento sea del máximo provecho para Bridgestone, se hace un análisis inicial de seguridad para resaltar las fortalezas y debilidades, con el fin de priorizar y trabajar sobre los principales riesgos. Solo para empezar, y tomar en cuenta la gravedad de incumplimiento de temas de seguridad, más allá de los riesgos dentro de la misma empresa, PricewaterhouseCoopers (2017) indica que "casi de forma predeterminada, los robots acceden a múltiples sistemas y cada uno puede ser una vulnerabilidad potencial en la privacidad de los datos". Según el comunicado de prensa de la Comisión Europea de enero de 2018, **se aplicarán sanciones de hasta 20 millones de euros o el 4% de la facturación anual por violaciones de datos basadas en el Reglamento general de protección de datos (RGPD)**.

El RGPD entró en vigor en mayo de 2018, por lo que ha adquirido una importancia creciente. Para mitigar los riesgos de violación de datos y tarifas elevadas, **se sugiere que las empresas lleven a cabo un inventario de datos y una auditoría de flujo de datos y políticas de cumplimiento (Ross, 2016).** Explica que las empresas deben verificar si sus procesos cumplen con la nueva regulación e implementar controles para abordar el fraude externo" (Indruškevičs,2018)

Tomando esto en cuenta, se realizó una investigación con el fin de saber si realmente no existen normas a nivel de RPA de Bridgestone, si es que no se aplican o si más bien es que ni siquiera se sabe de normas que existan actualmente que puedan ser replicadas en RPA.

Después de esto nos damos cuenta de que realmente sí existen una serie de reglas y políticas a nivel de Bridgestone, las cuales, en defecto que no tengan algunas más específicas en cierto departamento, deberían ser replicadas.

En el presente documento se cita información sobre las políticas de seguridad de Bridgestone, siempre y cuando no se pongan en riesgo sus sistemas.

#### 1.2.2.1 Estándares de seguridad actualizados

Debido a que no se cuenta con documentación oficial de seguridad para RPA, acudimos a los documentos de seguridad globales de Bridgestone.

Dentro de las políticas y estándares de seguridad, se pueden encontrar documentos de políticas y estándares de seguridad de las aplicaciones, retención de la información, clasificación de datos, encriptación, SSL-TLS Estándar, contratistas, Vulnerabilidades y manejo de actualizaciones, así como manejo de usuario y control de acceso, dentro de otros.

Dentro de los documentos se le da énfasis a estar alineados con el OWASP Top ten risks, y mantener estándares de encriptación adecuados. Se debe de manejar máximos estándares de confidencialidad de la información, y se debe de tener especial cuidado en no aplicar técnicas desactualizadas o inseguras. Todos los datos que son guardados, transmitidos y usados en la empresa deben de cumplir con los estándares de clasificación de datos correspondiente. Además, los servidores deben de contar con medidas apropiadas para asegurar la seguridad y confidencialidad de la información, estas medidas deben de ser proporcionalmente similares al más alto nivel de sensibilidad de la información almacenado en el servidor.

El código de software no puede ser almacenado en ningún repositorio público como github.

Los sitios web y aplicaciones web deben de ser testadas para asegurarse que los estándares de seguridad están siendo aplicados. Escaneos de vulnerabilidades deben de ser aplicados en toda la aplicación o sitio web, no solo en ciertas partes.

Se debe aplicar un adecuado “hardening” en los servidores web, dentro y fuera de la empresa, este debe de ser aplicado a todo nivel. Se debe cumplir con un adecuado monitoreo, así como chequeos programados de *compliance* (*checklists*).

Todos los desarrolladores, incluyendo contratistas, deben cumplir con los entrenamientos definidos por las políticas y estándares.

Se debe de realizar auditorías manuales y pruebas con los datos, los cuales deben ser almacenados en un lugar remoto, a prueba de desastres naturales que puedan afectar a las oficinas primarias. Anualmente se debe de hacer una prueba de restauración completa, para

verificar la validez de los datos, así como otros sistemas e infraestructuras empleados en el proceso.

Los datos deben ser destruidos o sobrescritos después de cierto periodo. Los datos utilizados con propósitos de archivo deben de ser adecuadamente encriptados y asegurados de acuerdo su sensibilidad.

Existe un equipo encargado de asegurarse del cumplimiento de estas políticas (Infosec GRC). Dentro de sus tareas se encuentran el desarrollo, o facilitación de desarrollo de procesos o estándares para el cumplimiento adecuado. El director de "Solutions Delivery" es responsable de asegurarse que todos los desarrolladores cumplan con cualquier entrenamiento requerido por los estándares y políticas.

BSA se encarga de publicar en un repositorio central todas las políticas para que todos los trabajadores las puedan ver cuando sea necesario. El OCIO Governance Team se debe de alinear con IT Communication para afirmarse que las actualizaciones de las políticas sean adecuadamente comunicadas.

Se tienen definidas las políticas de retención y resolución, así como la calidad y longevidad de los medios en los que se almacena la información. El sistema de negocio o los propietarios de los datos deben de determinar y definir el RPO (Recovery point objective) de la data esencial, por medio de BIA, u otras formas de evaluación de riesgo.

Los estándares de clasificación de los datos son de los más importantes aspectos por tener en cuenta en una empresa.

Dentro de la empresa se utiliza la clasificación de los datos desde S1 hasta S4:

- S1: Es estrictamente confidencial y de valor del negocio. En estos casos los más altos estándares de seguridad se deben de aplicar, y en algunos casos hasta esos no serán permitidos. Es necesaria la encriptación para estos datos, se debe de utilizar VPN para la transmisión de los datos, y el acceso a estos datos debe ser registrado y reportado.
- S2: Restringida: De Alto riesgo, altamente evaluable y de alta importancia para la organización. Si no se tiene conocimiento del nivel de clasificación de un archivo, asumirlo con S2. Esta información no puede ser transmitida de manera encriptada. Los

servidores que almacenen este tipo de información deben de ser segregados adecuadamente, al igual que en S1.

- S3: Es importante para la organización y representa un riesgo medio. La mayoría de las medidas de seguridad son recomendadas, aunque no obligatorias. Con estos datos no es necesario el *logging*.
- S4: Información pública que incluye todos los datos que han sido publicados y no representan un riesgo para la empresa.

> Si bien la retención describe la longevidad de una copia de seguridad determinada, la resolución se utiliza aquí para describir la frecuencia con la que se realizan las copias de seguridad. Esta característica reconoce la volatilidad o la cantidad de cambio que tiene lugar dentro de los datos. Una mayor resolución (copias de seguridad realizadas con mayor frecuencia) minimiza la posible pérdida de información que puede tener lugar entre la última copia de seguridad y el evento de pérdida de datos inadvertida. (Bridgestone, 2018)

**Políticas de encriptación**

Para los datos de carácter confidencial, se debe utilizar AES, RSA, o Hash seguro. Además, se deben de mantener documentación informativa para cualquier otro protocolo disponible, incluyendo HTTP, SSL, SSH y VPN.

Para la encriptación de los datos durante la transmisión se debe de utilizar TLS, SSH, AS2, VPN, PKI, PGP dentro de otras opciones.

Los datos en descanso también deben de ser encriptados. Los dispositivos móviles como laptops, tabletas y smartphones deben tener habilitada la inscripción de los datos en reposo.

Además, se tiene un estricto control sobre las llaves públicas y privadas.

**Empresas Contratistas**

Los llamados *third party vendors* deben cumplir con todas las leyes del país, así como las reglas definidas por la empresa.

Existe un ranking de riesgo de los diferentes vendedores. La mayoría de los terceros externos deben de proveer reportes de auditoría externa, y claramente si van a manipular datos de tarjetas deben cumplir con los estándares PCI DSS. Además, cumplir con las regulaciones de protección de datos, recuperación de desastres y continuidad de negocio. Los entes externos deben de cumplir con la mayoría de las reglas que se deben de cumplir en Bridgestone, además de otras por ser personas de otras empresas que acceden a los datos de Bridgestone.

**Estándares de control de acceso y usuarios**

Los controles de acceso son proveídos de acuerdo con el nivel de sensibilidad de la información que necesita ser accedida. La empresa se basa en el principio del mínimo privilegio. Los accesos provistos a los nuevos trabajadores se basan en las responsabilidades del puesto. Con los terceros aplica de manera muy similar, excepto porque se les define fecha de expiración desde un inicio. Dependiendo de los casos se utiliza autenticación multifactor y se aplican políticas de bloqueo después de un tiempo de inactividad.

Cualquier usuario que no cumpla con las reglas establecidas, puede ser objeto de acciones disciplinarias, incluyendo inclusive la terminación de la relación laboral. Las leyes federales, nacionales y de estados o de la ley local pueden aplicarse si se encuentra evidencia de actividad criminal. En casos necesarios de transporte de los datos, se debe de hacer conforme con todas las políticas respectivas incluyendo que el proceso sea auditable y verificable.

## 1.3 Definición y Descripción del Problema

RPA forma parte de la Industria 4.0 o “Transformación digital”, al ser esta una tecnología reciente, cuando se busca documentación y bibliografías, se encuentra muy poco.

Hemos identificado el principal problema como la necesidad de proveer un marco de seguridad de la información enfocado en RPA para mejorar la madurez de los controles existentes y verificar si nuevos controles requieren ser implementados en la empresa Bridgestone.

Por otro lado, la rápida adopción de RPA en la empresa y la poca planeación al adquirirla han causado un crecimiento inadecuado de la tecnología en términos de seguridad. Nuestro objetivo, es poder proporcionar a la empresa Bridgestone, un marco híbrido de controles de

seguridad que sirva como guía y apoyo para reducir los riesgos introducidos, que puedan desarrollar robots en cualquier área requerida por el negocio cumpliendo con aspectos regulatorios, legales y de privacidad a los cuales están sujetos.

Actualmente se dan auditorias y verificaciones de controles de seguridad hacia todos los departamentos, y por la falta de alineación, en RPA muchas veces realmente no se sabe qué responder hacia ciertos cuestionamientos que los encargados realizan. Dentro de esto existe otro problema: Los mismos encargados o auditores tampoco conocen mucho acerca de RPA, de manera que no pueden realizar una auditoría adecuada sobre el departamento, o exigen cosas inadecuadas. Parte de la justificación en ocasiones es que el departamento es muy reciente y falto de madurez, así como la tecnología, sin embargo, sabemos que esta justificación no omite de grandes riesgos a los que se podría exponer la empresa.

Debido a esto, encontramos muy importante facilitar a Bridgestone un marco que facilite realizar las tareas prioritarias en el nivel de seguridad.

## 1.4 Justificación

En Internet existen escasas fuentes que guían vagamente al usuario en temas de seguridad en RPA, pero a un alto nivel sin entrar en muchos detalles.

El valor agregado en este proyecto se encuentra en aportar una matriz de controles provenientes de diferentes normas y buenas prácticas del mercado de la ciberseguridad en un solo marco híbrido con el fin de ayudar a la empresa Bridgestone a gestionar el riesgo en su tecnología de RPA. Con este aporte, se solventa un problema de cumplimiento, gobierno y riesgo en la empresa. Adicionalmente, se analiza la madurez de los controles existentes y su sistema de seguridad de la información.

## 1.5 Viabilidad

### 1.5.1 Punto de Vista Técnico

Al analizar desde el punto de vista técnico, existen los medios técnicos tanto para la empresa que respalda el proyecto como los autores de este proyecto. Queda en evidencia la viabilidad de este. En caso de necesitar alguna recomendación o referencia, la empresa se compromete a facilitar la ayuda técnica necesaria.

### 1.5.2 Punto de Vista Operativo

Desde el punto operativo, la investigación es viable, ya que no entorpece ni altera las tareas del día a día en la empresa ni el ciclo de vida de diseño y construcción de robots. El proyecto se planea realizar en su gran mayoría de manera remota con reuniones puntuales y con acompañamiento o reuniones esporádicas con distintos interesados de Bridgestone, lo cual deja en evidencia la viabilidad del punto operativo.

### 1.5.3 Punto de Vista Económico

El punto de vista económico no está ligado a un gasto por parte de la empresa Bridgestone, ya que las herramientas y licencias de Blue Prism son propiedad de esta, así también como el "costo teórico", es por eso que se hace la salvedad, para que la empresa esté consciente de ello. En el momento que se necesite alguna licencia o software de pago, se evaluará entre ambas partes (empresa e investigador) para sufragar las mismas.

## 1.6 Objetivos

### 1.6.1 Objetivo General

Diseñar un marco híbrido de controles de seguridad basado en las buenas prácticas y normas relevantes de la industria de seguridad de la información para evaluar los ecosistemas de RPA en la empresa Bridgestone.

### 1.6.2 Objetivos Específicos

- Definir una serie de controles por medio de una matriz integrada para satisfacer requisitos de cumplimiento y necesidades del negocio relacionados con RPA.
- Establecer y documentar una guía para el uso del marco de controles de seguridad por parte de la audiencia por cubrir.
- Soportar el ciclo de vida de desarrollo actual de RPA en la empresa y cualquier otro tipo de metodología de desarrollo o herramientas de automatización.
- Analizar el actual sistema de seguridad de la información de Bridgestone, esto con el fin de asegurar la compatibilidad con su gobierno de seguridad.
- Detectar riesgos al utilizar RPA y herramientas de automatización y el impacto al no contar con controles de seguridad apropiados en la empresa Bridgestone.

## 1.7 Alcances y Limitaciones

### 1.7.1 Alcances

Siguiendo los objetivos, se tiene como base el diseño de un marco híbrido de controles de seguridad basado en las buenas prácticas y normas relevantes de la industria. Para que luego dichos controles sean evaluados y gestionados en el nivel de riesgo.

### 1.7.2 Limitaciones

1. Este proyecto pretende ser un punto de partida para concientizar y ayudar al centro de RPA de Bridgestone a gestionar la seguridad en sus *robots* de mejor manera, donde surge la necesidad de utilizar una guía que permita revisar controles asociados a la seguridad de los robots y a su vez tome en cuenta la protección de los datos contenidos en ellos.
2. El desarrollo y el logro de toda la investigación dependerá del interés que se le dé por parte de los actores que participan en él.
3. No se ha constituido un centro de excelencia para gobernar la gestión de RPA como un todo. Esta limitante provoca que el conocimiento está distribuido en varios grupos y por ende se dificulta recabar información entre los involucrados.

## 1.8 Estado de la Cuestión

### 1.8.1 Planificación de la revisión

El propósito de esta revisión es descubrir si existen y cuáles son los últimos avances en materia de seguridad informática en RPA. Se pretende documentar si existen alternativas, en especial de herramientas o marcos, similares a la que se propone en la presente investigación. Además de la búsqueda de herramientas similares, se realizará una revisión bibliográfica, en diferentes fuentes de confianza que permitan la detección de investigación teórica en el tema de las herramientas de RPA y su relación con la seguridad informática y ciberseguridad.

#### 1.8.1.1 Formulación de la pregunta

La pregunta por responder es la siguiente: ¿Cuáles son los últimos avances existentes respecto a herramientas o marcos de RPA y su integración con la seguridad informática y ciberseguridad?

La pregunta anterior obligó a investigar la existencia de alternativas adicionales a la herramienta que se plantea desarrollar en la presente investigación. De tal manera que, en las secciones subsiguientes, no solo se da respuesta a esa interrogante, sino también, al problema investigativo como tal.

#### 1.8.1.2 Selección de fuentes

##### 1.8.1.2.1 Definición del criterio de selección de fuentes

Las fuentes debían cumplir con el siguiente criterio: motores de búsqueda, bases de datos en línea o librerías digitales que permitan la búsqueda u obtención de artículos de investigación de los cuales esté disponible al menos el resumen ejecutivo del artículo consultado o que provean artículos informativos sobre el tema de investigación. Además, deben ser fuentes que se mantengan dentro del área de las tecnologías de la información, y de preferencia aquellas que provean resultados en el área de la seguridad de la información.

##### 1.8.1.2.2 Lenguaje de estudio

Los lenguajes de estudio son españoles e inglés, esto porque son los idiomas que dominan los investigadores, además que aquellas herramientas útiles para el mercado costarricense se encuentran en esos idiomas. Además, muchos de los trabajos de investigación, así como software existente, se encuentran escritas en inglés.

##### 1.8.1.2.3 Identificación

La identificación de fuentes se realiza por medio del sondeo inicial para descartar aquellas fuentes que no guardan relación con el tema de investigación, dicho sondeo se realizó al utilizar motores de búsqueda en línea.

#### 1.8.1.3 Selección de los estudios

La selección de estudios se realizó por medio de la búsqueda en las fuentes previamente identificadas, al utilizar las siguientes consultas (cuando estaba disponible la búsqueda por medio de operadores booleanos):

(RPA Security OR RPA Security Framework OR (RPA AND Security)) AND (Framework OR Best Practices)

Es importante resaltar que, no necesariamente se trata de estudios formales los resultados que se eligieron durante esta fase, ya que podrían haberse encontrado resultados que muestran las investigaciones para soportar la seguridad de RPA, a pesar de esto, no necesariamente dichos resultados cuentan con artículos científicos o estudios formales, sino que provienen de otras fuentes. Otro aspecto por considerar es que, en los casos en que la fuente no proveía una búsqueda por medio de operadores booleanos, se utilizó búsqueda sencilla al utilizar las siguientes consultas (según sea el idioma de la fuente consultada):

"RPA Security"

"RPA Security Framework"

"Robotics Security"

"RPA Cybersecurity Framework"

"RPA Security Risks"

"RPA Security Best Practices"

"Seguridad en RPA"

"Mejores prácticas de seguridad de RPA"

"Seguridad en RPA"

### 1.8.2 Ejecución de la revisión

#### 1.8.2.1 Ejecución de la revisión en la fuente: Safari Books

Safari Books Online es una librería digital que provee suscripciones por demanda. Tiene acceso a miles de libros, videos y actividades de aprendizaje de los publicadores líderes en el mundo. Estos recursos pueden ser accesados en cualquier tiempo y en cualquier lugar. Puede ser accedido mediante la dirección: https://www.safaribooksonline.com/home/

### 1.8.2.2 Ejecución de la revisión en la fuente: BluePrism

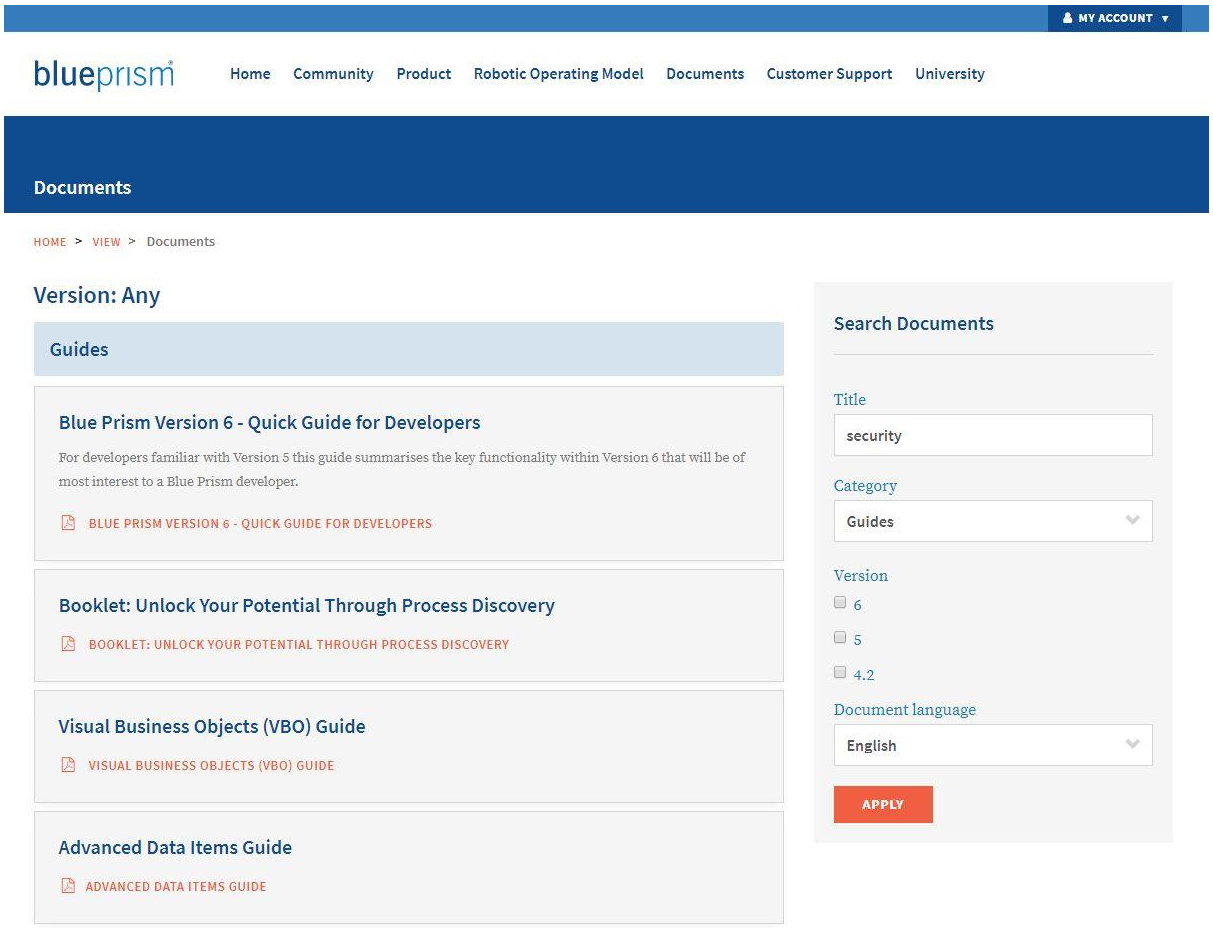



Imagen 9 - Screenshot de página de Blue Prism.

Fuente: www.blueprism.com

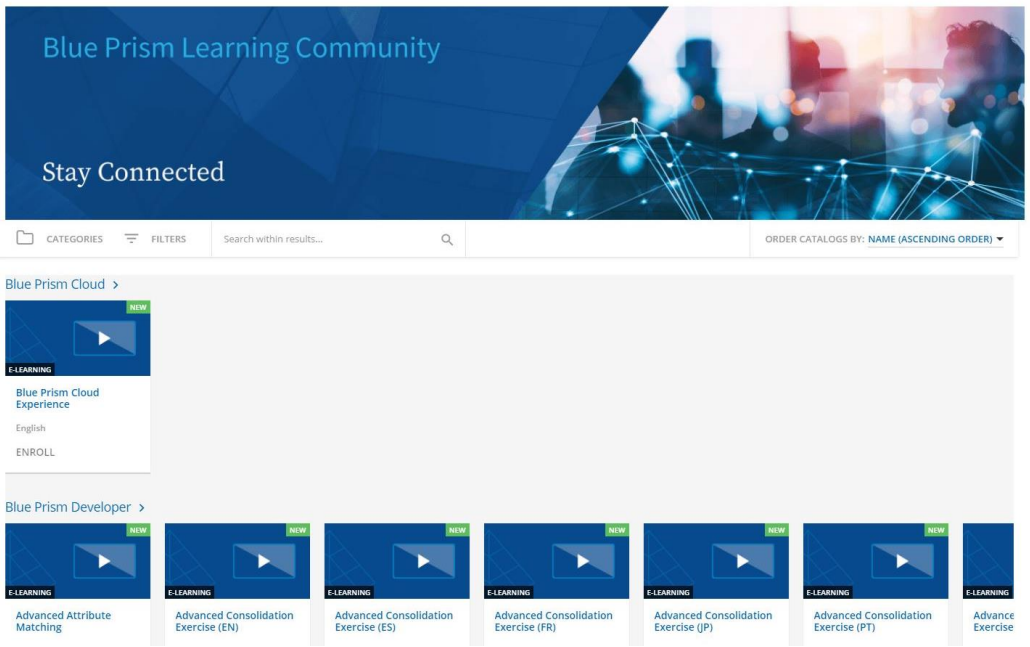



Imagen 10 - Captura de pantalla de página de Blue Prism

Fuente: www.blueprism.com

Blue Prism cuenta con un portal para sus afiliados, en el cual se tiene un gran repositorio de fuentes referentes a este software de RPA.

Esto incluye “roadmap”, “online product help”, “guides and datasheets”, “online help”, “support center”, “Global Support Programs”, además de una sección dedicada al aprendizaje, llamada “University”, la cual incluye “Training Updates”, “Training Offering (via LMS), Academia program, y “Learning Community”

### 1.8.2.3 Ejecución de la revisión en la fuente: Google Scholar

Este es un motor de búsqueda centrado en artículos académicos en el que se pueden encontrar documentos de múltiples ámbitos incluyendo el de esta investigación. Puede ser accedido mediante la dirección: https://scholar.google.com.

### 1.8.2.4 Ejecución de la revisión en la fuente: Research Gate

ResearchGate es un sitio de redes sociales para que científicos e investigadores compartan artículos, y hagan preguntas sobre las respuestas y encuentren colaboradores. Puede ser accedido vía web mediante la siguiente dirección: https://www.researchgate.net/

### 1.8.3 Análisis de Resultados

#### 1.8.3.1 Presentación de Resultados

De acuerdo con los documentos e información encontrada, existe información un poco limitada de RPA, existen también un poco más de fuentes de seguridad, sin embargo, siendo un par de temas que son relativamente nuevos, cuesta aún más localizar documentación que incluya los 2, la mayoría que se localizaron corresponden a documentos de investigaciones e información de parte de la herramienta Blue Prism.

#### 1.8.3.2 Comentarios finales

Por medio de la presente investigación, más que una barrera, hallamos una motivación el hecho de que existan pocas fuentes respecto al tema, debido a que este documento podrá ayudar en un campo en el cual para muchas empresas existe falta de información e incertidumbre sobre la seguridad en RPA.

Es un reto que se tomó con mucha motivación, para ayudar a suplir la falta de documentación existente y a la vez ayudar a las empresas que lo necesiten, a pesar de que el documento se está haciendo específicamente para Bridgestone, es altamente probable que podrá ser utilizado por muchas empresas que utilizan software similar, inclusive podría ser presentado en el nivel de CamSCAT (Cámara de Servicios Corporativos de Alta Tecnología) por medio de Bridgestone.

## Capítulo 2. Marco Teórico

En sus inicios, RPA se utilizó como una herramienta para probar la funcionalidad de un usuario de interfaz gráfica mediante la realización de una captura de pantalla. Por ejemplo, antes del código desplegado según la producción, un desarrollador podría crear un robot para probar la funcionalidad de cada pantalla, recopile los resultados de la prueba en un informe, y finalmente envíe el informe al equipo de desarrollo para hacerles saber si la aplicación tiene algún problema. En los últimos años, las herramientas RPA han mejorado con nuevas capacidades que van más allá de las funciones de captura de pantalla (Kappagantula, 2018). Algunas de las nuevas capacidades incluyen la integración con bases de datos, API, hojas de Excel y otros tipos de archivos; trabajar con reconocimiento de imágenes, archivos PDF y PGP (Pretty Good Privacy) para cifrar y descifrar archivos o cualquier información; ejecución de *scripts* externos como Java y *scripts* Visual Basic; integración con operaciones y manipulaciones de correo electrónico y XML.

RPA está siendo utilizado actualmente por muchas industrias, como las telecomunicaciones, tecnología de la información, atención de la salud, seguros, servicios financieros, recursos humanos y muchos otros ("4 Industries that are Killing it With Robotic Process Automation", 2016). Inclusive, la misma industria de la ciberseguridad se está valiendo de la ayuda de RPA para automatizar ciertos procesos.

RPA es utilizado por estas industrias para reducir los costos operativos, mejorar el rendimiento y aumentar la producción de la tasa de trabajo. En los párrafos siguientes, se detallan algunos ejemplos de cómo diferentes industrias pueden emplear herramientas de RPA en sus contextos de negocio específicos.

> Antes de la automatización, los FTE (full-time equivalent por sus siglas en inglés o equivalente a tiempo completo) los humanos tardaban un promedio de 12 minutos en completar el proceso. Los robots pudieron reducir el tiempo total de transacción a cuatro minutos, aunque los análisis revelaron que 45 segundos de este tiempo eran inactivos esperando que uno de los sistemas estuviera disponible. El resultado neto fue tres veces el volumen de transacciones por una décima parte del costo FTE, sin contar los costos iniciales de aumento. El proveedor calculó que logró recuperar su

> inversión inicial en Blue Prism en seis meses simplemente automatizando este proceso. (HfS Research, 2012)

RPA también es útil para la validación de datos. La mayoría de la validación de datos se realiza dentro de una base de datos, pero hay casos en los que los datos tendrán que ser verificados con un sitio web o repositorio de bases de datos disponibles al público.

La robotización de procesos es también una excelente herramienta a la hora de extraer información de muchos diferentes tipos de archivos como Excel, PDF, Word, CSV, etc. Por ejemplo, si un proceso implica extraer información de diferentes tipos de archivos, RPA tiene un conjunto de herramientas y objetos preestablecidos que pueden ayudar a automatizar completamente el proceso. Una herramienta en particular, que puede ser útil para este tipo de tareas, es el Reconocimiento óptico de caracteres (OCR), que se puede utilizar para extraer la información seleccionada de un archivo, como nombre, apellido, número de teléfono, dirección, y así sucesivamente, a pesar de que el archivo no contenga los caracteres originalmente. También, por medio de "scraping" y métodos especiales como *xpath*, se pueden extraer valores específicos de un sitio web.

RPA se puede utilizar para preparar informes complejos que agregan datos de varios orígenes. Algunos informes consumen mucho tiempo, pero un desarrollador podría crear un robot para recopilar información de varios sistemas y luego hacer que el informe se envíe por correo electrónico a las personas que lo han solicitado. El *Bot* se puede programar para entregar el informe diariamente, semanalmente, mensualmente o en otro intervalo, según sea necesario.

RPA también tiene un comando de correo electrónico, que se puede utilizar para enviar correos electrónicos masivos por medio de Outlook. RPA se utiliza ampliamente en la tecnología de la información (TI). En TI, RPA se utiliza para supervisar servidores y comprobar si hay fallos en el sistema. En la misma área de seguridad, es utilizado en tareas repetitivas tales como chequeos de controles.

Para un mejor entendimiento de los conceptos por utilizar en el nivel de seguridad de la información y ciberseguridad, es necesario definir terminología relacionada con el tema en cuestión.

Antes de iniciar a definir terminología en el nivel de seguridad, es de suma importancia abarcar el segmento de amenazas y vulnerabilidades a las que se pueden enfrentar los activos de información en este tipo de ambientes.

## 2.1 Amenazas, vulnerabilidades e impacto

> Una amenaza es cualquier evento que, si se materializa, puede causar daños a un sistema y crear una pérdida de confidencialidad, disponibilidad o integridad. Las amenazas pueden ser malintencionadas, como la modificación intencional de información confidencial, o pueden ser accidentales, como un error en un cálculo de una transacción o la eliminación accidental de un archivo. Se han agrupado las amenazas en varias categorías, y se describen algunos de los elementos de cada categoría. (Krutz & Vines, 2006)

Existen diversos tipos de amenazas, entre ellas:

La pérdida accidental es una pérdida que se produce involuntariamente, ya sea por la falta de capacitación o competencia del operador o por el mal funcionamiento del procedimiento de procesamiento de una aplicación. Los siguientes son algunos ejemplos de los tipos de pérdida accidental:

- Errores y omisiones de entrada del operador. Errores manuales de transacciones de entrada, eliminación de entradas o datos, y modificación defectuosa de datos.
- Errores de procesamiento de transacciones. Errores que se introducen en los datos a través de procedimientos defectuosos de programación o procesamiento de aplicaciones.

También existen actividades inapropiadas tales como:

La actividad inapropiada es un comportamiento informático que, si bien no sube al nivel de actividad criminal, puede ser motivo de acción laboral o despido.

- Contenido inapropiado. Uso de los sistemas de la empresa para almacenar pornografía, entretenimiento, contenido político o violento.

- Desperdicio de Recursos Corporativos. Uso personal de hardware o software, como llevar a cabo un negocio privado con el sistema informático de una empresa.
- Acoso sexual o racial. Uso de correo electrónico u otros recursos informáticos para distribuir material inapropiado.
- Abuso de Privilegios o Derechos. Uso de niveles de acceso no autorizados para violar la confidencialidad de la información confidencial de la empresa.

Continuando con el tema de amenazas, las operaciones informáticas ilegales y ataques intencionales son muy comunes, entre ellas destacan:

Bajo este epígrafe, se han agrupado las áreas de actividades informáticas que se consideran como acciones intencionales e ilegales con fines de lucro financiero personal para su destrucción:

- Escucha activa. El barrido de datos, el análisis de tráfico o tendencias, la ingeniería social, el espionaje económico o político, el olfato, el buceo en contenedores, el monitoreo de pulsaciones de teclas y el surf de hombros son todo tipo de espionaje para obtener información o para crear una base para un ataque. El espionaje es la causa principal del fracaso de la confidencialidad.
- Fraude. Ejemplos de los tipos de fraude son la colusión, las transacciones falsificadas, la manipulación de datos y otras alteraciones de la integridad de los datos para obtener beneficios.
- Robo. Ejemplos de los tipos de robo son el robo de información o secretos comerciales con fines de lucro o divulgación no autorizada, y el robo físico de hardware o software.
- Sabotaje. El sabotaje incluye la denegación de servicio (DoS), los retrasos en la producción y los ataques a la integridad de los datos.
- Ataque externo. Ejemplos de ataques externos son el agrietamiento malicioso, el escaneo y el sondeo para obtener información de infraestructura, marcar para localizar una línea de módem no segura y la inserción de un código o virus malicioso. (Krutz & Vines, 2006)

De la mano de las amenazas, el término vulnerabilidad debe ser mencionado dado que sin una vulnerabilidad existente la amenaza no podría tomar ventaja de esta y causar un impacto.

> Una vulnerabilidad es una debilidad en un sistema que puede ser explotada por una amenaza. La reducción de los aspectos vulnerables de un sistema puede reducir el riesgo y el impacto de las amenazas en el sistema. Por ejemplo, una herramienta de generación de contraseñas que ayuda a los usuarios a elegir contraseñas robustas reduce la posibilidad de que los usuarios seleccionen contraseñas deficientes (la vulnerabilidad) y hace que la contraseña sea más difícil de descifrar (la amenaza de ataque externo). (Walker, 2019)

Entrando en detalles acerca de las amenazas, una de las más comunes y que generan más impacto son los hackers.

> Como cualquier otro campo profesional, el hacking (puede o no ser hackeo ético) tiene su propia jerga y una infinidad de términos que conocer. Los propios hackers, por ejemplo, tienen varios términos y clasificaciones. Por ejemplo, un script kiddle es una persona sin educación en técnicas de hacking que simplemente hace uso de herramientas y técnicas disponibles libremente (pero a menudo viejas y anticuadas) en Internet, y un phreaker es alguien que manipula los sistemas de telecomunicaciones para hacer llamadas gratuitas. (Walker, 2019)

Los hackers se pueden clasificar por sombreros o en inglés como “hats”. Se puede categorizar a un hacker de innumerables maneras, pero el sistema "hat" parece haber resistido la prueba del tiempo. La comunidad de hackers en general se puede clasificar en tres divisiones separadas: lo bueno, lo malo y lo indeciso. En el mundo de la seguridad de TI, esta designación se da como un color de sombrero:

- White hat o Sombrero blanco. Considerados los buenos, estos son los *hackers* éticos, contratados por un cliente con el objetivo específico de probar y mejorar la seguridad o para otros fines defensivos. Los de sombrero blanco son muy respetados y no usan sus conocimientos y habilidades sin el consentimiento previo.
- Black hat o Sombrero negro. Considerados los malos, estos son los *crackers*, trabajan ilegalmente al utilizar sus habilidades para beneficio personal o intención maliciosa.

Buscan robar (copiar) o destruir datos y denegar el acceso a recursos y sistemas. Los sombreros negros no piden permiso ni consentimiento.

- Gray hat o Sombrero gris. El grupo más difícil de categorizar, estos *hackers* no son buenos ni malos. En términos generales, hay dos subconjuntos de sombreros grises: aquellos que simplemente tienen curiosidad por las herramientas y técnicas de *hacking* y aquellos que sienten que es su deber, con o sin el permiso del cliente, para demostrar fallas de seguridad en los sistemas. (Walker, 2019)

Luego de que se materializa una vulnerabilidad por parte de una amenaza, causa un impacto y por ende un incidente el cual se debe reportar y resolver según corresponda la situación.

Un incidente de seguridad de la información puede afectar a más de un activo o solo a una parte de un activo. El impacto está relacionado con el grado de éxito del incidente. Como consecuencia, hay una diferencia importante entre el valor del activo y el impacto resultante del incidente. Se considera que el impacto tiene un efecto inmediato (operativo) o un efecto futuro (negocio) que incluye las consecuencias financieras y del mercado.

El impacto inmediato (operativo) es directo o indirecto.

- Directo

a. el valor de sustitución financiera del activo perdido (parte de);
b. el costo de adquisición, configuración e instalación del nuevo activo o respaldo;
c. el costo de las operaciones suspendidas debido al incidente hasta que se restablezca el servicio prestado por los activos; Y
d. el impacto da lugar a una violación de la seguridad de la información.

- Indirecto

a. costo de oportunidad (los recursos financieros necesarios para reemplazar o reparar un activo se habrían utilizado en otro lugar);
b. el costo de las operaciones interrumpidas;
c. posible uso indebido de la información obtenida a través de una violación de seguridad;
d. violación de las obligaciones legales o reglamentarias; Y
e. violación de los códigos de conducta éticos.

> Como tal, la primera evaluación (sin controles de ningún tipo) estima un impacto muy cercano a la (combinación del valor o valores de activos afectados). Para cualquier siguiente iteración para este (estos) activos, el impacto es diferente (normalmente mucho menor) debido a la presencia y la eficacia de los controles implementados. (ISO,2018)

Gregory (2018) afirma que “un incidente en el nivel general se puede definir como cualquier evento que no forme parte del funcionamiento estándar de un servicio y que cause, o pueda causar, interrupción o reducción en la calidad de dicho servicio “.

Gregory (2018) asegura que, a nivel de seguridad, “un incidente de seguridad es un evento en el que la confidencialidad, integridad o disponibilidad de información (o un sistema de información) se ha visto comprometida. “

## 2.2 Marcos de seguridad de la información y buenas prácticas

Es importante mencionar los marcos de seguridad más utilizados, respetados y reconocidos de la industria de la seguridad de la información y de la ciberseguridad. Para este caso en específico se van a utilizar marcos de referencia en la industria, así como marcos que deben ser utilizados por Bridgestone debido a cumplimiento interno, legal y empresarial. El objetivo es mezclar controles de diferentes marcos y unirlos bajo un solo y único control que abarque dichos marcos, así evitando duplicar evaluaciones y auditorías duplicadas para cada marco.

> ISO/IEC 27004:2016. Proporciona directrices destinadas a ayudar a las organizaciones a evaluar el rendimiento de la seguridad de la información y la eficacia de un sistema de gestión de la seguridad de la información con el fin de cumplir con los requisitos de ISO/IEC 27001:2013, 9.1. Establece:
>
> a. la supervisión y medición del rendimiento de la seguridad de la información;
>
> b. el seguimiento y la medición de la eficacia de un sistema de gestión de la seguridad de la información (ISMS), incluidos sus procesos y controles;
>
> c. el análisis y evaluación de los resultados de la monitorización y medición. (ISO,2016)

ISO/IEC 27005:2018. Este documento proporciona directrices para la gestión de riesgos de seguridad de la información. Adicionalmente, apoya los conceptos generales especificados en ISO/IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

> Este documento es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar riesgos que pueden comprometer la seguridad de la información de la organización. (ISO,2018)

> NIST CSF v1. El marco es un enfoque basado en el riesgo para gestionar el riesgo de ciberseguridad y se compone de tres partes: el núcleo, los niveles de implementación del marco y los perfiles de marco. Cada componente del marco refuerza la conexión entre los impulsores empresariales y las actividades de ciberseguridad. (NIST, 2014)

> ISO/IEC 27001:2013. Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información en el contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ISO, 2013)

ISO/IEC 27002:2013. Proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.

Está diseñado para ser utilizado por organizaciones que tienen la intención de:

1. Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información basado en ISO/IEC 27001;
2. Implementar controles de seguridad de la información comúnmente aceptados;
3. Desarrollar sus propias pautas de gestión de la seguridad de la información. (ISO, 2013)

> PCI DSS v3.2. Los estándares de seguridad PCI son requisitos técnicos y operativos establecidos por el PCI Security Standards Council (PCI SSC) para proteger los datos del titular de la tarjeta. Las normas se aplican a todas las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta, con requisitos para los desarrolladores de software y los fabricantes de aplicaciones y dispositivos utilizados en esas transacciones. El Consejo es responsable de la gestión de las normas de seguridad, mientras que el cumplimiento del conjunto de normas PCI es aplicado por los miembros fundadores del Consejo: American Express, Discover Financial Services, JCB, MasterCard y Visa Inc. (PCI Security Standards Council, 2018)

NIST SP 800-53 Rev. 4. Esta publicación proporciona un catálogo de controles de seguridad y privacidad para los sistemas y organizaciones federales de información y un proceso para seleccionar controles para proteger las operaciones organizativas (incluyendo misiones, funciones, imagen y reputación), activos organizaciones, individuos, otras organizaciones y la nación de un conjunto diverso de amenazas, incluidos ataques cibernéticos hostiles, desastres naturales, fallas estructurales y errores humanos (tanto intencionales como no intencionales). Los controles de seguridad y privacidad son personalizables e implementados como parte de un proceso de toda la organización que administra la seguridad de la información y el riesgo de privacidad. Los controles abordan un conjunto diverso de requisitos de seguridad y privacidad en todo el gobierno federal y la infraestructura crítica, derivados de la legislación, las órdenes ejecutivas, las políticas, las directivas, las regulaciones, los estándares o las necesidades de misión/negocio. La publicación también describe cómo desarrollar conjuntos especializados de controles, o superposiciones, adaptados para tipos específicos de misiones/funciones empresariales, tecnologías o entornos de operación. Por último, el catálogo de controles de seguridad aborda la seguridad desde una perspectiva de funcionalidad (la fuerza de las funciones y mecanismos de seguridad proporcionados) y una perspectiva de garantía (las medidas de confianza en la capacidad de seguridad implementada). Abordar tanto la funcionalidad de seguridad como la garantía ayuda a garantizar que los productos de componentes de tecnología de la información y los sistemas de información creados a partir de esos productos que utilizan principios de ingeniería de seguridad y sistemas de sonido sean suficientemente fiables.

COBIT 5. Es un marco para la gobernanza y gestión de la información y la tecnología, dirigido a toda la empresa. Enterprise I&T significa toda la tecnología y el procesamiento de

información que la empresa pone en marcha para lograr sus objetivos, independientemente de dónde ocurra esto en la empresa.

General Data Protection Regulation (GDPR)

1. Este reglamento establece normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a las normas relativas a la libre circulación de datos personales.

2. Protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de datos personales dentro de la Unión Europea no estará restringida ni prohibida por razones relacionadas con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. (GDPR, s.f.)

OWASP SKF. Security Knowledge Framework es un activo vital para el conjunto de herramientas de programación de un equipo de desarrollo. Se utiliza SKF para aprender e integrar la seguridad por diseño en una aplicación web.

SKF es una base de conocimientos de seguridad de código abierto que incluye proyectos manejables con listas de comprobación y ejemplos de código de prácticas recomendadas en varios lenguajes de programación que muestran cómo evitar que los piratas informáticos obtengan acceso y ejecuten exploits en su aplicación. (OWASP, s.f.)

SANS CSC 20. Los controles críticos de seguridad son un conjunto recomendado de acciones para la defensa cibernética que proporcionan formas específicas y procesables para detener los ataques más generalizados y peligrosos de hoy en día. Una de las principales ventajas de los controles es que priorizan y enfocan un número menor de acciones con resultados de pago elevados. Los controles son eficaces porque se derivan de los patrones de ataque más comunes resaltados en los principales informes de amenazas y examinados a través de una comunidad muy amplia de profesionales gubernamentales y de la industria. Fueron creados por la gente que sabe cómo funcionan los ataques -los equipos rojos y azules de la NSA, los laboratorios de energía nuclear del Departamento de Energía de los Estados Unidos, las organizaciones policiales y algunas de las principales organizaciones forenses y de respuesta a incidentes del

país- para responder a la pregunta", "qué tenemos que hacer para detener los ataques conocidos". Ese grupo de expertos llegó a un consenso y hoy tenemos los controles más actuales. La clave del valor continuado es que los controles se actualizan en función de los nuevos ataques identificados y analizados por grupos desde Verizon hasta Symantec para que los controles puedan detener o mitigar esos ataques. (SANS, s.f.)

## 2.3 Gestión de la seguridad de la información

Gregory (2018) menciona que el término de gestión en seguridad de la información se entiende por “la agregación de directivas, procesos, procedimientos y actividades para garantizar que la política de seguridad de una organización sea eficaz. “

Gregory (2018) establece en el nivel de gobernanza, “es indispensable contar con políticas, las cuales son instrucciones que definen cómo una organización clasificará y protegerá sus activos importantes. “

> Las buenas prácticas son esenciales en la gestión, por ejemplo, la segregación de tareas que se refiere al concepto que garantiza que los individuos no poseen privilegios excesivos que podrían resultar en actividades no autorizadas como el fraude, la manipulación o exposición de datos confidenciales. (Gregory, 2018)

## 2.4 Herramienta de gobernanza, riesgo y cumplimiento (GRC)

> El término GRC se refiere a Gobierno, Riesgo y Cumplimiento. El mismo es clave para una buena gestión de un sistema de seguridad de la información. Se pueden utilizar programas de software para rastrear aspectos claves del programa de riesgo de información de una organización. (Gregory, 2018)

Parafraseado del marco de TI de riesgo de ISACA, es el riesgo empresarial asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de información dentro de una empresa.

Según Gregory (2018), “la gestión de riesgos empresariales (ERM) son los métodos y procesos utilizados por una organización para identificar y gestionar los riesgos empresariales”.

> El riesgo es generalmente, el hecho de que puedan ocurrir eventos no deseados que puedan dañar la propiedad o interrumpir las operaciones; específicamente, un escenario de evento que puede resultar en daños a la propiedad o interrupción. (Gregory, 2018)

El riesgo puede tener varios estados durante su ciclo de vida, por ejemplo:

- El riesgo residual es el que queda después de ser reducido a través de otras opciones de tratamiento de riesgo.
- El riesgo inherente de que haya debilidades materiales en los procesos empresariales existentes y no hay controles de compensación para detectarlos y prevenirlos. (Gregory, 2018)

Antes de iniciar la gestión de riesgos, es importante conocer el nivel de riesgo que una organización está dispuesta a aceptar mientras se persigue su misión, estrategia y objetivos, y antes de que se necesite la acción para tratar el riesgo. (Gregory, 2018). Además de la cantidad objetiva de pérdida que una organización puede tolerar sin que se cuestione su existencia continua. (Gregory, 2018)

Una vez definido el riesgo y sus tipos, es importante resaltar el tema de la gestión de riesgos de seguridad en las organizaciones. Según Gregory (2018) “La gestión se define como todas aquellas actividades utilizadas para identificar, analizar y tratar riesgos. “

En la siguiente imagen se encuentra el ciclo de vida de gestión de riesgos basado en la norma ISO 27005, el cual incluye una evaluación de riesgos con actividades como identificar, analizar y evaluar. Una vez realizadas estas 3 actividades se debe tomar una decisión de cómo tratar ese riesgo en el nivel empresarial. La comunicación y consulta deben ir de la mano en todas las etapas, así como una revisión y un monitoreo luego de tratar el riesgo.




Imagen 11 - Manejo de riesgos

Fuente: ISO 27005:2018

El análisis de riesgos es el proceso de identificación y estudio de riesgos en una organización.

La evaluación de riesgos es un proceso en el que se identifican riesgos, en forma de amenazas y vulnerabilidades, para cada activo.

Según Gregory (2018), “el tratamiento de riesgo es la decisión de gestionar un riesgo identificado. Las opciones disponibles son mitigar el riesgo, evitar el riesgo, transferir el riesgo o aceptar el riesgo”.

- Evitar riesgos

La opción de tratamiento de riesgo que implica el cese de la actividad que introduce el riesgo identificado.

- Transferencia de riesgos

La opción de tratamiento de riesgos que implica el acto de transferir el riesgo a otra parte, como una compañía de seguros.

- Mitigación de riesgos

La opción de tratamiento de riesgos que implica la implementación de una solución que reducirá un riesgo identificado.

- Aceptación de riesgos

La opción de tratamiento de riesgos cuando la dirección decide aceptar el riesgo tal como está.

**2.5 Cumplimiento**

> Se define cumplimiento como todas aquellas actividades relacionadas con el examen de sistemas y procesos para garantizar que se ajusten a las políticas, normas, controles, requisitos y reglamentos aplicables; también, el estado de conformidad con las políticas, normas, controles, requisitos y regulaciones aplicables.
>
> El riesgo de cumplimiento es el riesgo asociado con las consecuencias generales o específicas de no cumplir con una ley, reglamento u obligación legal privada. identidad y gestión de acceso (IAM). Las actividades y sistemas de apoyo que se utilizan para gestionar las identidades de los trabajadores, sus accesos a los sistemas de información y los datos. (Gregory, 2018)

**2.6 Gestión de identidades**

Dicha gestión es la actividad de administrar la identidad de cada empleado, contratista, trabajador temporal y, opcionalmente, cliente, para su uso en un único entorno o en varios entornos.

Según Gregory (2018), “el término usuario se refiere a una empresa o cliente que utiliza un sistema de información”.

## 2.7 Auditoría

A grandes rasgos es una revisión formal de uno o más procesos, controles o sistemas para determinar su estado contra un estándar.

Existen varios tipos de auditorías, entre ellas destacan la auditoría de cumplimiento que se utiliza para determinar el nivel y el grado de cumplimiento de una ley, regulación, norma, disposición de contratos o control interno.

La auditoría de seguridad es una revisión formal de los controles de seguridad, procesos o sistemas para determinar su estado. (Gregory, 2018)

## 2.8 Robótica

RPA es el término que se utiliza hoy en día para describir los programas que se encargan de automatizar tareas de humanos al manipular ecosistemas de software específicos de software de una empresa. Por medio de RPA, en lugar de utilizar una API que permita interconectar los programas, como se daba en el pasado por medio de BPM, el software de RPA se encarga de realizar las operaciones que realiza normalmente un humano. Tiene la ventaja que no depende de humanos por lo que los robots no necesitan descanso, y si de repente se reducen las cargas de trabajo, tampoco hay que despedir a nadie. El término fue creado por la empresa Blue Prism, la cual es una compañía de desarrollo de Reino Unido, enfocada al campo de Robotic Process Automation. Este grupo facilita robots de software que ayudan a automatizar procesos de back office que trabajan exactamente como un humano. Varias empresas compiten en el mismo campo, dentro de estas podemos incluir las siguientes:

- **Automation Anywhere**

Otro software de RPA el cual tiene la fama de ser muy utilizado en el campo. Una de sus cualidades es la grabación de *stages* (etapas), así como que también tiene su versión "community", de uso libre. Suele ser bastante ágil y eficaz.

- **PEGA Robotics**

Software de RPA que tiene la cualidad de interactuar con Visual Studio, por lo que se puede desarrollar por capas, a su vez también se puede convertir en código para ser utilizado

dentro de .Net, Por lo que por medio de esto se puede ejecutar más rápidamente. Tiene una interesante característica de auto creación de los SDDs y otros tipos de documentación, con base en los datos de proyectos ya existentes.

- **UIPath**

  Es una compañía global de software que desarrolla una plataforma de RPA. Seguida de la adquisición de Process Gold y StepShot en el 2019, UIPath se ha convertido en el primer vendedor de escala que brinda juntos la minería de procesos y Robot Process Automation. De acuerdo con el área de Gartner, la combinación de RPA con minería de procesos, AI y *machine learning* y *analytics* es mejor describida como *hiper automation*. (Agarwal ,2018)

- **Blue Prism**

El término Robotic Process Automation, conocido en corto como RPA, fue inventado por Blue Prism. Esto por sí mismo muestra que la compañía es pionera en el campo de desarrollo de RPA. (Blue Prism, 2016). En las siguientes páginas se detalla cómo se utiliza esta herramienta.

A pesar del potencial de RPA, nos hemos dado cuenta de que un robot de estos, implementando inadecuadamente, puede disparar los riesgos de seguridad de una empresa. Afortunadamente existen herramientas que han logrado identificar estas falencias, y se han especializado en brindar soluciones para minimizar los riesgos. Dentro de estas podemos encontrar las siguientes:

**CyberArk**

Empresa líder mundial especializada en la gestión de acceso privilegiado. Dentro de sus muchas soluciones, se encuentra un software diseñado para el almacenamiento y manipulación segura de credenciales, y el cual se puede utilizar en conjunto con Blue Prism y UIPath. Dentro de sus clientes, se encuentra más de la mitad de la lista de Fortune 500 (Cyberark, 2020)

Dentro de sus soluciones, se encuentra una solución gratuita para el diagnóstico de la situación actual de la empresa respecto al acceso privilegiado, llamada CyberArk DNA.

> *CyberArk Discovery & Audit (DNA) es una herramienta poderosa, disponible sin cargo, que escanea sistemas en su red para descubrir cuentas, credenciales y configuraciones erróneas que pueden crear riesgos. Después de un escaneo, CyberArk DNA genera un informe detallado que los auditores de TI y los encargados de tomar decisiones pueden usar para evaluar el estado de las cuentas privilegiadas en la organización e identificar áreas de riesgo. La herramienta es un ejecutable ligero y sin agentes, diseñado para exponer la magnitud del desafío de administración de acceso privilegiado en entornos locales y basados en la nube. (CyberArk, 2020).*

Para la presente investigación se incluye un análisis de un robot que se está trabajando actualmente dentro de Bridgestone. Este robot fue implementado con la herramienta Blue Prism, por lo que se considera importantes detalles acerca de las funciones y características que este contiene. Para comenzar, se explicarán características de la herramienta por utilizar, “Blue Prism”

Al abrir el programa, iniciamos viendo el ¨Dashboard¨




Imagen 12 - Media Center

Fuente: www.blueprism.com

- **Dashboard.** Área de inicio de BP, también llamada home, en la cual se ven estadísticas básicas de los robots, y desde la cual se puede acceder a la mayoría de las opciones y pestaña (Blue Prism, 2016)

El principio básico de RPA es poder manipular programas que los trabajadores de una empresa suelen utilizar. Tomando esto en este momento, ya existen ciertas utilidades de los programas de automatización, enfocadas a los programas típicos de sus empresas clientes. Por brindar un ejemplo, existe un¨objeto¨de Blue Prism que se encarga de manipular Microsoft Excel, otro que manipula Outlook, también existen objetos que manipulan las funciones básicas del sistema de Windows, y dentro de varias, podemos incluir el que se encarga de manipular los directorios y archivos de este.

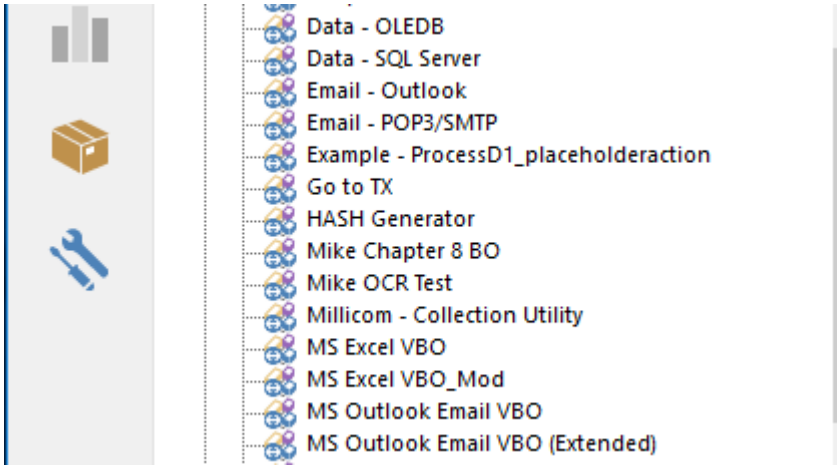



Imagen 13 - Captura de pantalla de BluePrism

Fuente: www.blueprism.com

Existen ocasiones en las cuales no hay un objeto existente para una operación que realiza el negocio. Si no hay un objeto, la herramienta de RPA no sabe cómo manipular al mismo. Debido a esto, y para facilitar la creación de nuevos objetos, las herramientas suelen incluir utilidades que le permiten al programador poder crear nuevos objetos. Dentro de Blue Prism tenemos el **Application Modeller.** Es donde los elementos de las aplicaciones por manipular son identificados por medio de Blue Prism. (Blue Prism, 2016). Por medio de este, Blue Prism nos permite¨espiar¨un objeto específico y poder definir su interfaz, botones, textbox, textbox, mensajes informativos, para luego ser utilizados como insumo por la herramienta. O sea que esto es un mapeo de un software específico, para que el programa de Blue Prism reconozca cómo manipularlo. En otras palabras, por medio del Application Modeller, creamos un controlador para nuevas aplicaciones con las que Blue Prism interactuará.

Luego de ser definidos los objetos correspondientes, también es necesario definir las acciones relacionadas, y para eso la misma herramienta brinda un espacio llamado **Object Layer** para poder incluir el flujo de acciones que se realizan dentro de la aplicación. Dentro de estos se pueden incluir Inputs y Outputs, así como también ¨Code Stages¨ de C#. Un code stage, es una acción que se incluye dentro del software de RPA, para que realice un código específico de C·, el cual se incluye tipificado dentro de esta.

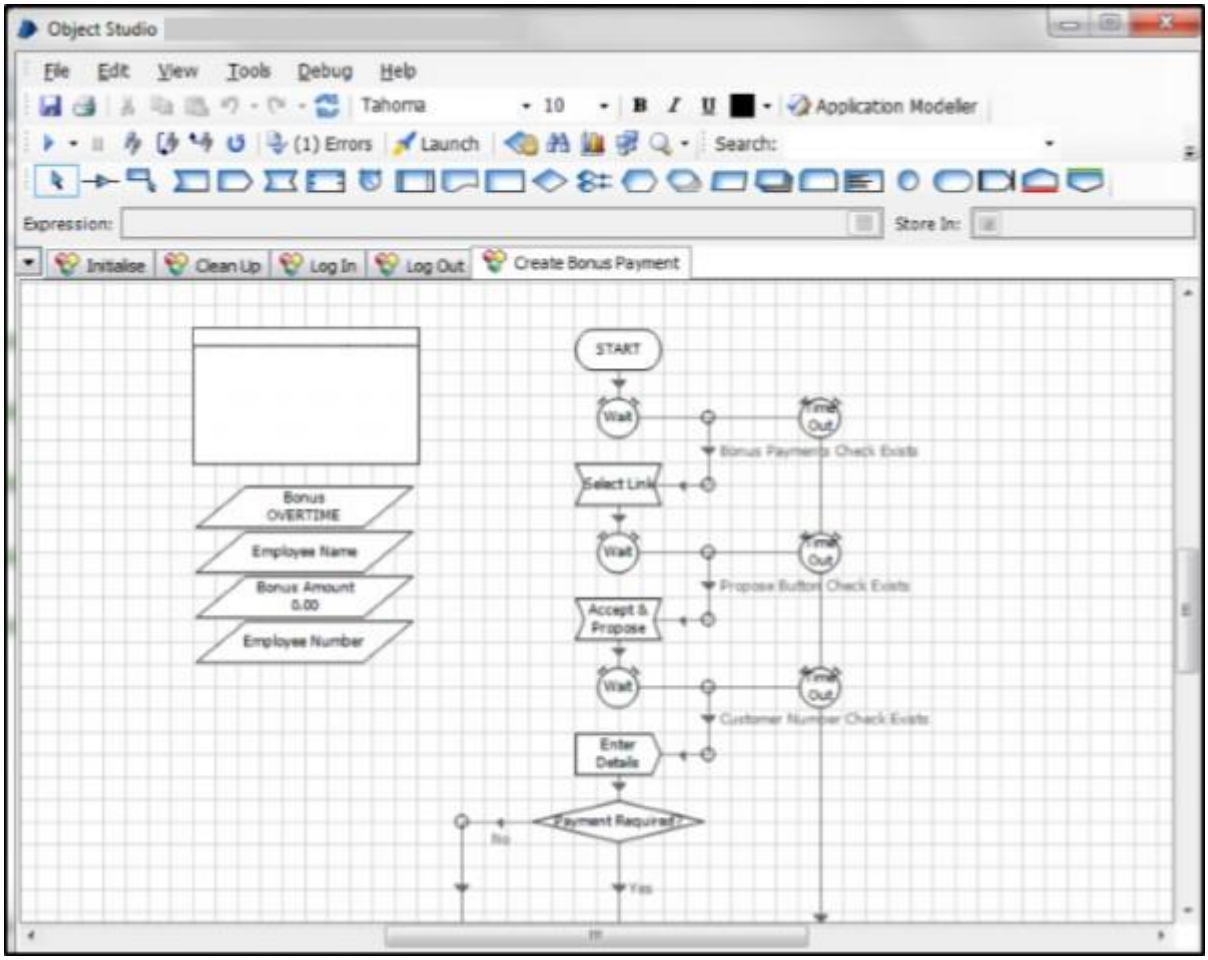



Imagen 14 - Captura de Object Studio del software Blue Prism

Fuente: www.blueprism.com

Cuando un objeto ya ha sido creado, brinda nueva funcionalidad a la herramienta de Blue Prism. Sin embargo, un objeto por sí solo no suele funcionar. Para que este se ejecute, es necesario que sea "invocado" desde otro lugar. Es por esto por lo que existe el "Control **Room",** así como también el O**bject Studio**.

- **Object Studio.** Área de Blue Prism en la cual se accede a los procesos y a los objetos (Blue Prism, 2016). Es el área en donde se diseña el diagrama de flujo funcional, y dentro del mismo se incluyen llamadas a procesos y acciones de objetos.

Cuando un objeto ha sido creado y testado, y también se ha creado un proceso que lo utilice, se suele enviar al control room, en donde se realizan pruebas para asegurarse de que funcione adecuadamente. El control room es una interfaz dentro de la cual se programan corridas

de robots, y se puede analizar por medio de logs todo el proceso que realiza el mismo. Área en la cual se controlan los procesos que están en producción, podemos ver schedules, robots que están corriendo y sus logs. Además, incluye el "scheduler", por medio del cual se programan las corridas de los robots por horario. (Blue Prism, 2016)

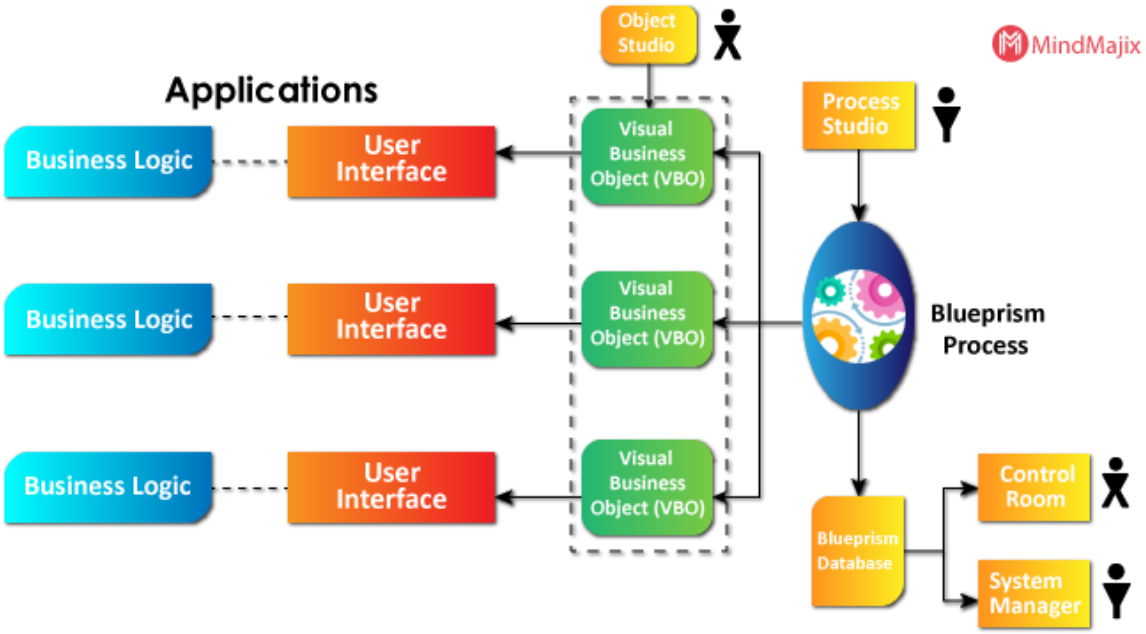



Imagen 15 - Aplicaciones de Blue Prism

Fuente: https://mindmajix.com/blue-prism-tutorial-for-beginners

- **Process Layer**. Las acciones creadas en el (Business) Object Layer se juntan en el Process Layer para formar un proceso completo. (Blue Prism, 2016)

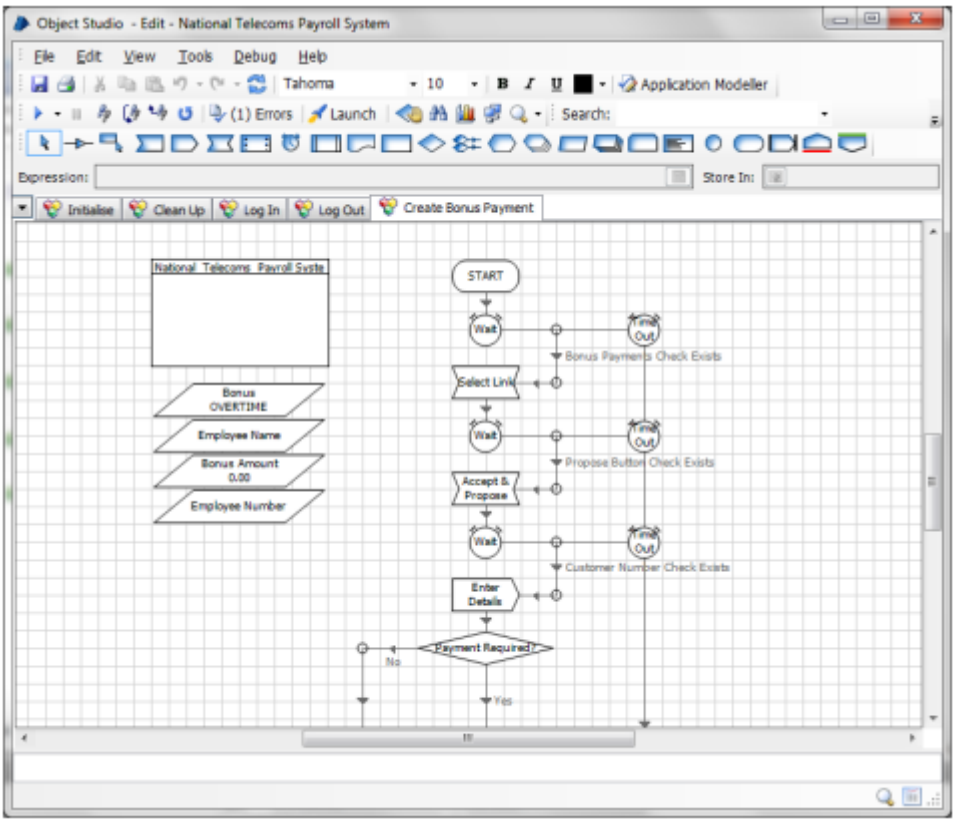



Imagen 16 - Diagrama de Flujo en Object Studio

Fuente: www.blueprism.com

- **Release Manager.** Es donde se une todo un proceso y sus componentes (business objects, work queues, schedules y más) en un solo paquete. Estos procesos pueden ser modificados, convertidos en un "release" y siendo exportados en un archivo XML. Este release puede luego ser importado en otra base de datos de Blue Prism. (Blue Prism, 2016) Es el proceso recomendado por Blue Prism para enviar un proceso a QA y producción, de manera que, lo que es analizado en QA, así como en producción no es el "código" más reciente, sino más bien el paquete que se les envía, junto con las dependencias que también deben de ser incluidas ahí mismo.
- **System Manager.** Incluye muchas opciones importantes y de seguridad, como editar roles de usuario, agregar nuevas licencias y modificar las Work Queues. (BluePrism, 2016)

SO es un proceso usado para combinar funcionalidad de la aplicación, con reglas de negocio para crear flujos de trabajo muy útiles.

Múltiples procesos pueden usar las mismas business object actions. (Blue Prism, 2016)

**Funciones**

- **Attach**

Por medio de attach logramos conectar la aplicación de BluePrism al programa que deseamos automatizar. (Blue Prism, 2016)

- **Global Wait Stages**

El campo de Timeout en BluePrism permite referenciar a data items globales. De esta manera, por medio de un data item global podemos cambiarle el valor de tiempo de espera a muchos ítems a la vez. (Blue Prism, 2016)

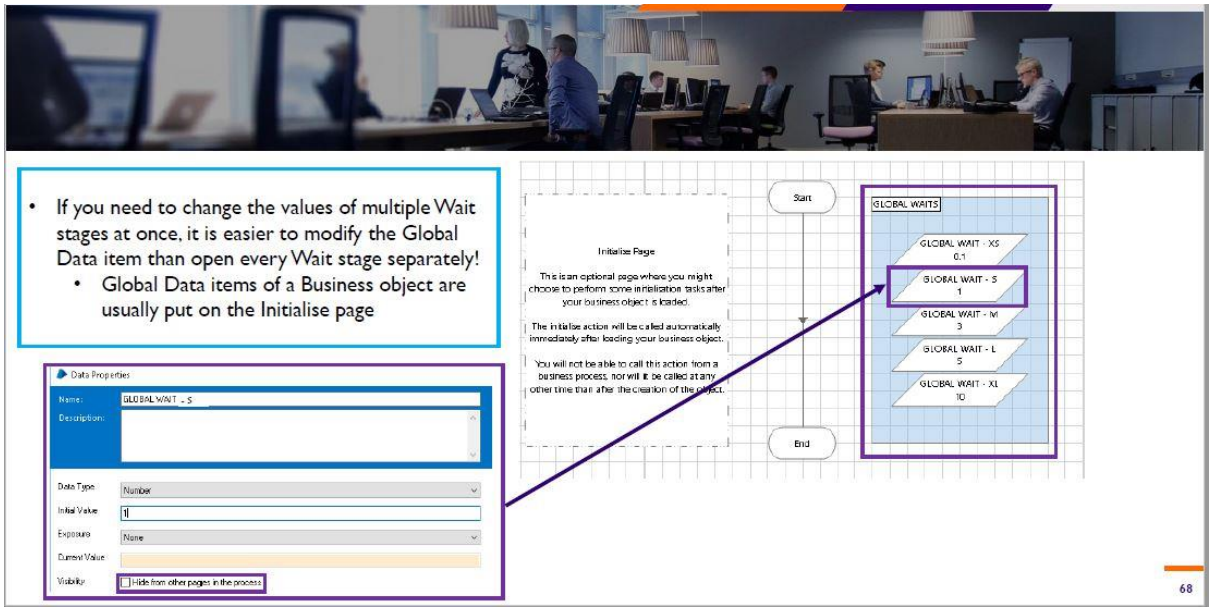



Imagen 17 - Esperas Globales

Fuente: Digital Learning Academy

- **Escalabilidad**

Al igual que en los desarrollos por medio de código, Blue Prism tiene la capacidad que los procesos se vuelvan escalables, esto por medio de diferentes procesos que se adhieren a un queue. (Blue Prism, 2016)

- **Reusabilidad**

Un adecuado desarrollo por medio del modelador de objetos permite que los objetos de negocio no gasten mucha memoria.

# Capítulo 3. Marco Metodológico

## 3.1 Tipo de Investigación.

Siguiendo la línea de la investigación en curso, el estudio se centra en el uso de la metodología de investigación aplicada, puesto que no se genera conocimiento per se, sino más bien se basa en el existente de la investigación básica. El aprovechamiento del conocimiento en el área de RPA y seguridad de la información por parte del investigador, y el reconocimiento en la necesidad de una empresa que utiliza RPA para optimizar procesos, hacen que se aprovechen de las diferentes piezas para crear marco de controles de seguridad y así justificar la escogencia de este tipo de investigación. El siguiente diagrama tomado del sitio douc.cl ejemplifica de forma clara la idea.




Imagen 18 - Investigación aplicada

Fuente (UC,2019)

En este proyecto el problema se establece en la falta de una evaluación de controles para verificar la seguridad de la información en los robots creados con la tecnología RPA que deben ser reguladas; que a su vez se convierte en un modelo específico para realizar auditorías o inspecciones de oficio en un entorno dentro de protección de los datos de la empresa , en donde sus características particulares dificultan la aplicación de modelos construidos con un enfoque empresarial de seguridad de la información.

## 3.2 Alcance investigativo.

El alcance investigativo de este proyecto es de carácter exploratorio. La investigación exploratoria se efectúa sobre un tema poco estudiado, en donde los alcances se limitan a la observación y al registro objetivo de lo encontrado (Barrantes, 1999, p. 131). Este proyecto considera las fuentes primarias, los casos aplicados de guías de control de riesgo sobre RPA y los

estudios teóricos sobre RPA y seguridad de los datos para crear una herramienta que permita evaluar cualquier robot que sea creado al utilizar BluePrism como software de RPA

Por otra parte, y de acuerdo con lo establecido en el tipo de investigación, se propone una solución aplicada, en donde los modelos observados y documentados, serán utilizados para generar marco de controles de seguridad con los requerimientos de cumplimiento y riesgo de la empresa Bridgestone.

**3.3 Enfoque.**

El enfoque de la investigación es mixto, cualitativo y cuantitativo. Cuantitativo porque según Hernández Sampieri consiste "en utilizar la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población". Pero también cualitativo porque según Hernández Sampieri "consiste en utilizar la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación".

**3.4 Diseño.**

El diseño de la investigación define las estrategias básicas para generar información confiable e interpretable (Bautista, 2011, p. 150). La investigación-acción permite el diagnóstico de problemáticas sociales, políticas, laborales, económicas, etc., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones, algunas de sus características según Hernández Sampieri "Cuando una problemática de una comunidad necesita resolverse y se pretende lograr el cambio." (Sampieri, 2014, p. 471) y además es relevante mencionar que las personas tomen conciencia de su papel en ese proceso de transformación. Por ello, implica la total colaboración de los participantes en: la detección de necesidades, el involucramiento con la estructura por modificar, el proceso por mejorar.

Las estrategias estarán dirigidas a resolver un problema puntual, en este caso, generar un marco de controles de seguridad de la información enfocada a la protección de datos contenidos en los robots creados por Bridgestone al utilizar RPA, esto para salvaguardar el cumplimiento y minimizar los riesgos de un potencial compromiso de datos por parte de personas maliciosas.

### 3.5 Población y muestreo.

La población se conforma por robots creados en el software Blue Prism de RPA.

| | **Valor absoluto** | **Valor relativo** |
|---|---|---|
| **Población** | **9** | **100%** |
| **Muestra** | **6** | **66%** |

Tabla 1- Población y muestreo

### 3.6 Instrumento recolección de datos.

Para efectos de esta investigación se cuenta con el conocimiento necesario del negocio para poder dar marcha con el desarrollo de este. Dentro de esto, tiene un papel muy importante el Arquitecto de RPA, ya que es una de las personas que más interactúa y conoce de la totalidad de los robots que se encuentra funcionando en producción.

### 3.7 Técnicas de análisis de información.

La gestión de problemas apunta a resolver problemas a través de la investigación y un análisis en profundidad de incidentes. Una de las metodologías estándar es realizar un diagrama Ishikawa (o diagrama de causa-efecto) a través de una tormenta de ideas de las partes afectadas. Ya que en este caso conocemos con profundidad el problema, la condición se convierte en un "error conocido". Entonces se puede desarrollar un proceso para resolver el problema en cuestión.

El diagrama de Ishikawa, conocido también como causa-efecto o diagrama de espina de pez, es una forma de organizar y representar las diferentes teorías propuestas sobre las causas de un problema. Nos permite, por tanto, representar gráficamente el conjunto de causas que dan lugar a una consecuencia, o bien el conjunto de factores y subfactores (en las “espinas”) que contribuyen a generar un efecto común (en la “cabeza” del diagrama).

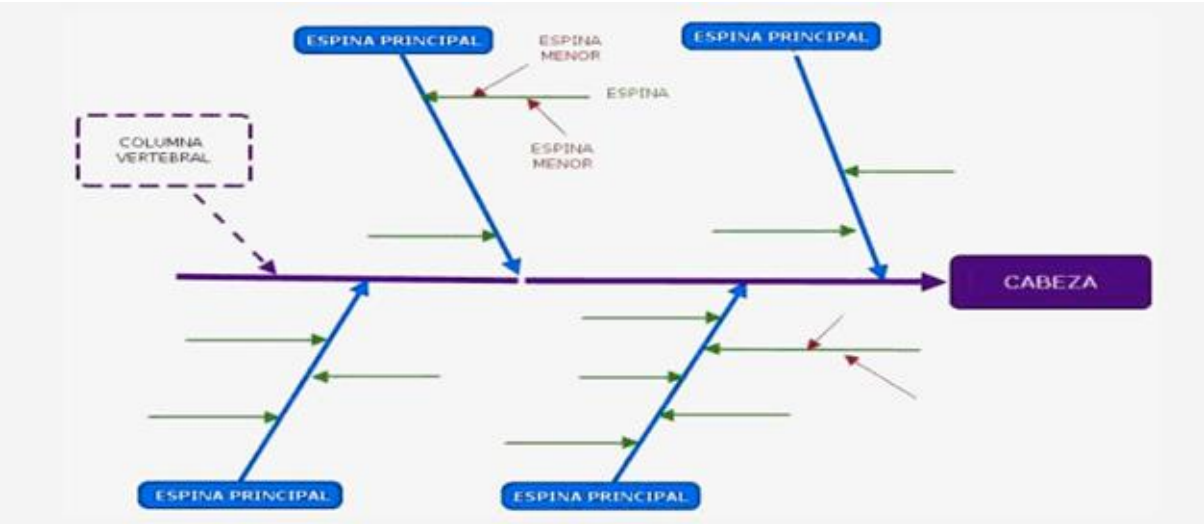



Imagen 19 - Diagrama de Ishikawa: Análisis causa-efecto de los problemas

Fuente: http://www.pdcahome.com/diagrama-de-ishikawa-2

## Capítulo 4. Desarrollo de la solución.

Después de investigar en libros, papers, consultas en Bridgestone, análisis de tesis y libros, análisis de casos de uso de Shared Services, estado de la situación actual en Bridgestone, se decidió priorizar 5 dominios para el proyecto del *framework*.

Estos son:

1. Identidad y Manejo de Acceso (Identity and Access management)
2. Protección de Acceso e Información (Information and Access Protection)
3. Estrategia, Gobierno y Administración (Strategy, governance and management)
4. Inteligencia de Amenazas y Vulnerabilidades (Threat Intelligence and Vulnerability)
5. Riesgo, Cumplimiento y Manejo de Políticas (Risk, Compliance and Policy Manager)

Se seleccionaron estos ya que se consideran los más altos riesgos que se ven en el departamento de RPA.

Adicionalmente los marcos de la industria que se tomaron en consideración fueron seleccionados según las necesidades de cumplimiento, aspectos legales y contractuales de Bridgestone junto con marcos universalmente reconocidos en la industria de la seguridad.

> "Identity and Access management" se define como la prioritaria, debido a que los robots amplifican los riesgos que ya existen con los humanos. Así como un humano puede no manejar adecuadamente unas credenciales, un robot también, e incluye más riesgos, ya que estos siempre deben de ser manipulados por otras personas, por lo que su información no es estrictamente confidencial. No en vano, Cyberark suele llamarle "las llaves del reino" a las credenciales con derechos de administrador que puedan utilizar robots (Cyberark, 2019).

Existe una herramienta gratuita de CyberArk, la cual puede brindar una especie de "radiografía" de la situación actual, esta se llama CyberArk DNA. Por medio de esta podemos crear informes detallados y visualizar amenazas. Dentro de los informes tenemos hallazgos tan importantes como cantidad de llaves, cumplimiento, ¿Qué máquinas tienen llaves que conducen a otras máquinas, credenciales únicas, accesos privilegiados?

Recomendaciones de CyberArk acerca de la seguridad:

1. Quitar credenciales quemadas, y acceder a ellas por medio de un API
2. Rotación frecuente de contraseñas únicas, que tengan cierto grado de complejidad. Implementar suspensión de credenciales en caso de actividades no deseadas
3. Principio de menor acceso.
4. Asegurar el acceso a la consola de administración de RPA. Los administradores deben de ser considerados usuarios privilegiados.

**Marco de controles de seguridad**

Este marco fue desarrollado tomando en cuenta las necesidades específicas de la empresa Bridgestone tales como cumplimiento, riesgo y gobierno. Como parte de este proceso se revisaron políticas, estándares, metodologías de riesgo, inventario de controles, proceso de auditoría interna, registro de riesgos, entre otros.

El marco contiene procesos correlacionados, riesgos, objetivos de control y requerimientos, políticas, estándares y KPIs. Al tener una librería centralizada de controles permite realizar las siguientes actividades:

- Desarrollar o mejorar políticas y estándares
- Capturar responsables o dueños de los controles
- Documentar controles y verificar su estado de implementación
- Realizar pruebas en los controles
- Evaluar y priorizar riesgos y problemas
- Desarrollar KPIs y KRIs para los niveles de la organización
- Reportar madurez en la gestión de riesgos
- Guiar certificación de controles
- Evaluar a la empresa contra marcos de la industria
- Compilar reportes de riesgos
- Mejorar riesgos asociados a un riesgo de negocio

**Uso del marco de controles de seguridad**

Este marco refleja un inventario de riesgos de seguridad y sus controles específicos. A tal punto que continuará siendo revisado con los dueños de los controles y el desarrollo de políticas y estándares. Asimismo, será actualizado, revisado y aprobado de acuerdo con los cambios de los procesos dentro de Bridgestone.

El marco fue diseñado tomando en cuenta su taxonomía de riesgos empresariales y sus posibles riesgos de seguridad y de TI, también se tomaron eventos de riesgo.

El diseño del marco fue realizado en Microsoft Excel dado que se requería un software para ingresar y ordenar gran cantidad de datos provenientes de distintas fuentes como marcos de seguridad de la industria, normas y estándares de la gestión del riesgo, entre otros.

El marco tiene 5 pestañas, las cuales fueron creadas para guiar al usuario en su uso y para documentar distintos conceptos relacionados con el riesgo de la empresa Bridgestone.

A continuación, se detallan las pestañas y la función que cumplen:

- Cover Page. Esta pestaña contiene un resumen del porqué se creó el marco, la estructura del documento de Excel, las ventajas de contar con dicho marco, la definición de cada uno de los campos de la pestaña donde se encuentra la librería de controles de seguridad, los marcos de la industria que se usaron como referencia y la definición de vectores de ataque.
- Risk Categories. Contiene la taxonomía de riesgos de la información, entre ellos las categorías de riesgo, la definición de cada categoría, las subcategorías de riesgo y sus definiciones. Adicionalmente, los eventos de riesgo e impacto asociados a las categorías y definiciones.
- Risk Control Library Framework. Esta pestaña contiene el insumo de trabajo principal, la misma contiene diversos campos que simulan una librería de controles de seguridad con sus respectivos objetivos de control, ejemplos de indicadores de rendimiento o KPIs, procedimientos de prueba, ejemplos de evidencia por recolectar y la referencia al marco del cual provienen.
- Risk Events. Lista de todos los posibles eventos o causas con sus definiciones, impacto y probabilidad. Se define por prioridad según apetito de riesgo y se refiere a la triada de la seguridad de la información. (Confidencialidad, Integridad y Disponibilidad).

- Threat Vectors. Se listan los vectores de las amenazas, sus definiciones y temas incluidos en cada uno. Cada vector está asociado a un control si estos ayudan a prevenir directamente que una amenaza sea explotada, de lo contrario si el control reduce el impacto después que la amenaza fue explotada, entonces el control no será asociado al vector.

**Librería de controles de Seguridad**

En esta hoja de Excel se utilizaron varios tipos de identificadores numéricos y alfanuméricos, en algunos casos con caracteres especiales con el fin de reconocer la diferencia entre los controles de seguridad y para que puedan ser identificados de una manera sencilla y rápida.

**Lista de columnas**

- ID del Ciclo. Es el identificador del nombre del ciclo.
    1. ID. Identity and Access Management
    2. IA. Information and Asset Protection
    3. RC. Risk, Compliance and Policy Manager
    4. SG. Strategy, Governance and Management
    5. TV. Threat Intelligence and Vulnerability Management
- Ciclo - El ciclo de pruebas de control de alto nivel de los procesos.
- ID del Proceso - Se compone del ID del ciclo más las iniciales de las palabras contenidas en el nombre del proceso, por ejemplo:

  **IA-DCIP-DRT:** Data Inventory, Classification and Protection - Data Retention

- Proceso. Lista de nombres de procesos y subprocesos para los que se asignan los riesgos y controles a alto nivel.
- Categoría de riesgo - Riesgo de nivel 1 según se define en la taxonomía de riesgo ERM (limitada a los riesgos de información). Esta es la convención de nomenclatura corta, la definición completa se puede encontrar en la pestaña "Categorías de riesgo".

- Sub-Categoría de Riesgo - Riesgo de Nivel 2 según se define en la taxonomía de riesgo ERM (limitada a los riesgos de información). Esta es la convención de nomenclatura corta, la definición completa se puede encontrar en la pestaña "Categorías de riesgo".
- Evento de riesgo. Campo desplegable de 12 eventos que afectan la capacidad del negocio para alcanzar sus objetivos al impactar en la confidencialidad, integridad o disponibilidad de la información. Esta es la convención de nomenclatura corta, la definición completa se puede encontrar en la pestaña "Eventos de riesgo".
- Escenario de riesgo - Una situación o escenario en el que se manifiesta el evento de riesgo, al describir los actores, métodos y evento negativo. El comentario de riesgo es un campo de forma libre, es la declaración de riesgo más granular en esta biblioteca.
- Vector de amenaza. Rutas o herramientas comunes que un actor de amenazas utiliza para realizar un escenario de riesgo.
- Objetivo de control - Declaración de un resultado deseado o propósito de un control.
- Requisito de control racionalizado - Los requisitos de control se racionalizan a partir de la industria y fuentes regulatorias como NIST CSF, ISO 27001/2, FFIEC, PCI DSS, NIST 800-53 y COBIT.
- Actividad de Control de Bridgestone- Un conjunto de actividades que la organización debe realizar para cumplir con el objetivo de control. Los requisitos de control específicos derivados de la industria y las fuentes reguladoras (muchas a una relación con los objetivos de control).
- Propietario del control. El propietario del control es el delegado del propietario estándar responsable de comprender el diseño del control y supervisar la eficacia operativa. Serán el principal punto de contacto para investigar y corregir problemas relacionados con los controles, incluso si el control está siendo realizado por otros.
- Estándar. El estándar relacionado con el riesgo de información que incluye este requisito de control. La asignación de cada requisito de control a un estándar garantiza que cada requisito de control se asigne a un único estándar.
- Política - La política relacionada con el riesgo de información que incluye el objetivo de control. La asignación de cada requisito de control a una directiva garantiza que cada requisito de control se asigne a una única directiva.
- Métricas - Una medida numérica de la implementación, eficacia o impacto de los controles relacionados con el riesgo de información.

- Tipo de control. Distingue si el control solo pertenece a activos PCI en el ámbito o en el nivel de aplicación.
- Framework Mapping - La asignación de cada control a requisitos específicos / directrices de los marcos de la industria.
- Tipo de medida. El tipo de medida definido en NIST 800-55 Revisión 1 - Guía de medición del rendimiento para la seguridad de la información.

**Cómo utilizar la matriz para asegurar o evaluar un robot o arquitectura de RPA**

Antes de utilizar la matriz de controles se deben tener en cuenta los siguientes aspectos del robot a evaluar:

1. Alcance. Establecer de manera clara los límites del robot en términos de operación. Esto incluye con cuáles sistemas se comunica, en cuáles redes interactúa o segmentos de red y hasta donde puede operar.
2. Función. Entender el resultado y entregable final del robot.
3. Disponibilidad. La criticidad del robot para la operación en caso de que deje de operar por cierta cantidad de tiempo.
4. Impacto. Posible consecuencia en caso de que el robot falle o deba ser detenido por razones propias de la operación o un incidente interno/externo.
5. Riesgo. Determinar los datos que serán utilizados por el robot y si hay legislaciones u otros estándares por cumplir, ya sea en el nivel de privacidad o seguridad de la información.

Una vez determinados estos cinco aspectos, se procede con un barrido manual de los posibles controles de seguridad que puedan aplicar para dicho robot en específico.

Primeramente, el barrido puede ser visual dependiendo de la experiencia del usuario con el robot y sus conocimientos en controles. Sin embargo, la idea es ir descartando los controles uno a uno para asegurar que no se están evaluando controles que no aplican al ambiente y función del robot.

El objetivo es verificar si el control de seguridad se está aplicando en el robot o bien está siendo tomado en cuenta en el ciclo de vida de desarrollo del robot. Asimismo, algunos de estos controles pueden ser aplicados en el nivel de arquitectura o infraestructura del ambiente de RPA.

La matriz de controles de seguridad puede ser encontrada en la sección de Anexos en el final de este documento como el Anexo #2.

**Caso de uso**

El robot que se utiliza para análisis se llama Invoice Copies, y consta de una serie de procesos similares que se están ejecutando dentro de Bridgestone, por diferentes unidades de negocio. Este se encarga de realizar la descarga de facturas especificadas por los agentes de la empresa, a partir de solicitudes de los clientes.

Este robot se ha desarrollado por uno de los autores de esta investigación (Luis Matamoros) como desarrollador principal, contando con la ayuda del equipo de RPA en caso de cualquier inconveniente, especialmente el equipo “MI6” con el cual se le da seguimiento al proyecto por medio de la metodología scrum, así como también la ayuda de otras empresas que colaboran en el proceso de outsourcing respecto a RPA siempre que sea necesario. (“Proceso de Shadowing”).

Dentro de la creación del primer robot, el equipo de análisis y recomendaciones, incluyendo al desarrollador Carlos Mora como líder, se da cuenta que, a pesar de que se van a realizar diferentes robots para las áreas de negocio, la mayoría de estos tienen una misma función para ¨popular¨ los datos de SQL al queue. Es por esta razón que se decide crear un robot independiente, llamado “Queue Populator”, el cual carga los datos de SQL server, de todas las unidades de negocio (BO) al “queue” de BluePrism.

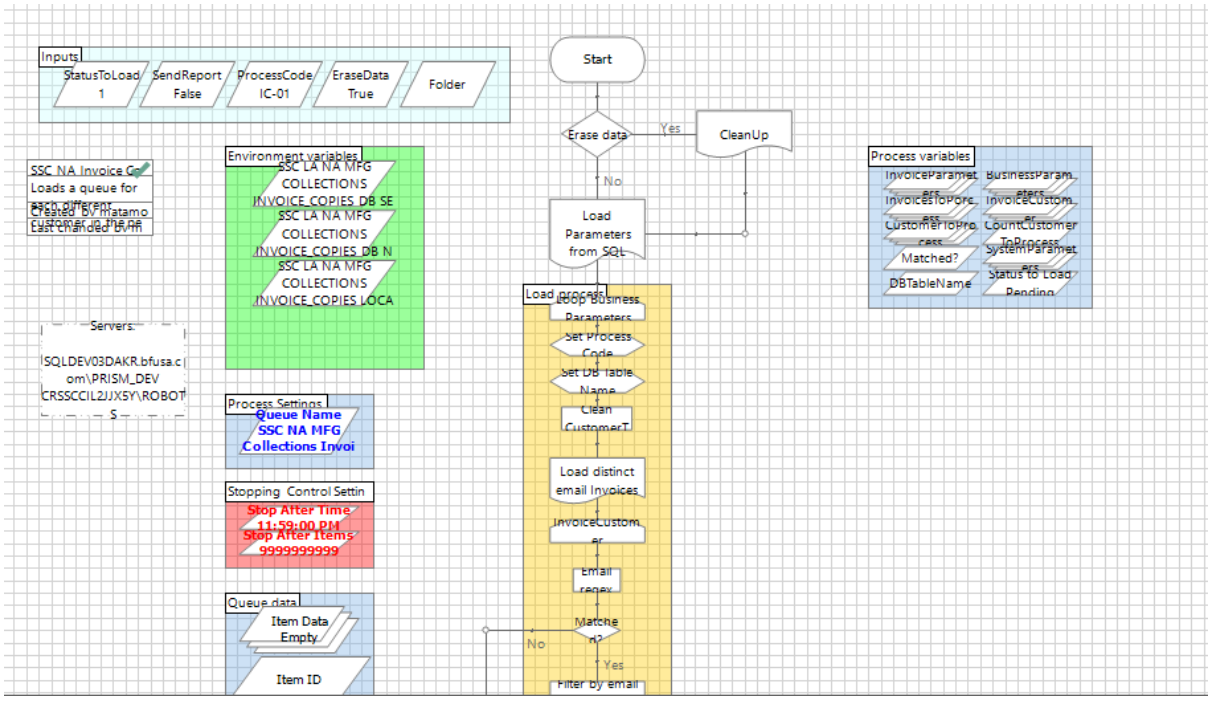



Imagen 20 - Queue Populator

Fuente: Captura de pantalla de Invoice Copies Populator Robot

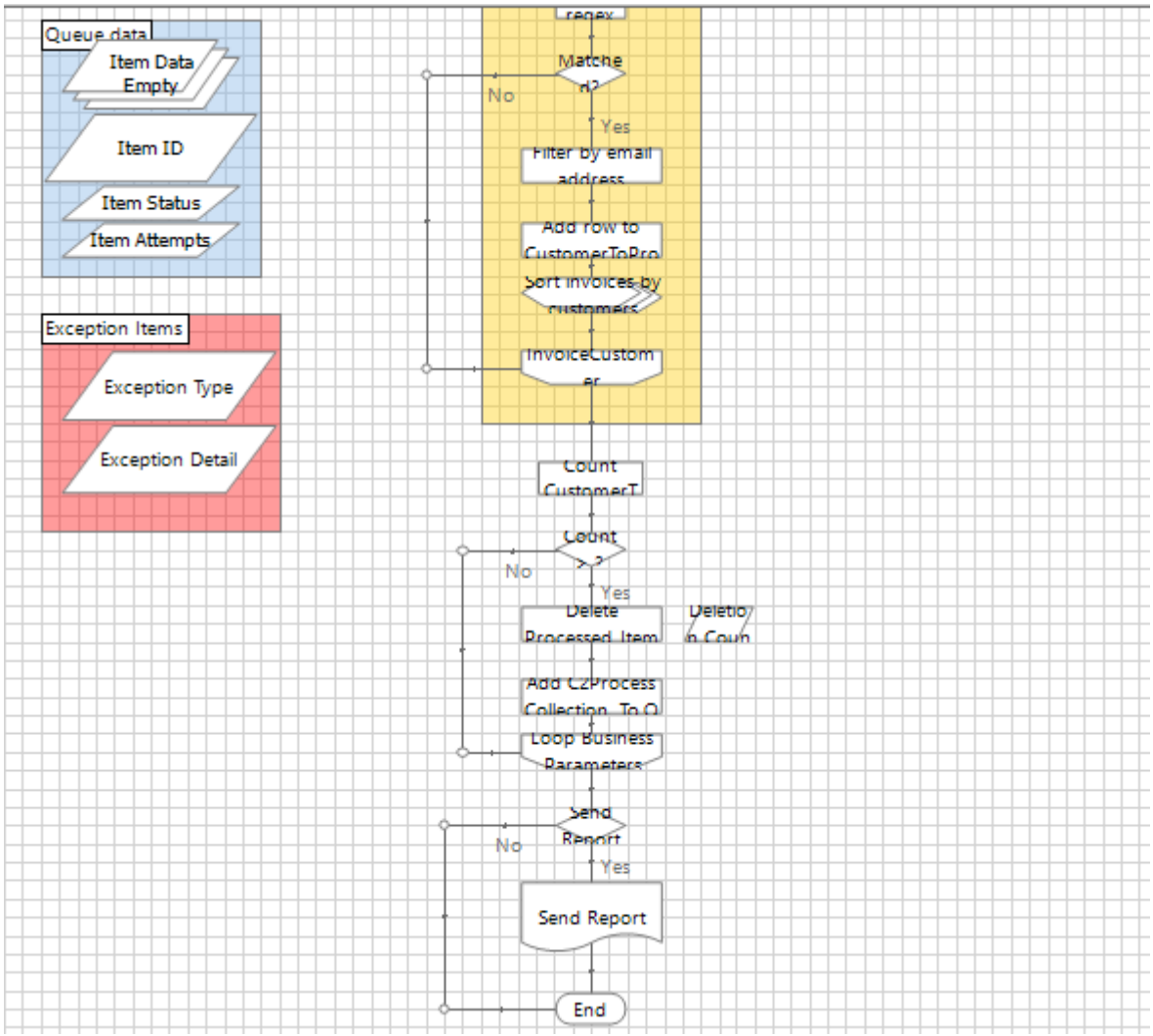



Imagen 21 - Queue Populator

Fuente: Captura de pantalla de Robot de Invoice Copies

Es importante recalcar que para que los datos sean cargados dentro de la base de datos, fue creada una macro por parte del equipo de automatización, sin embargo, esta no se tomará dentro del análisis del documento actual.

Luego que el queue populator se encarga de cargar los datos de la base de datos, el robot encargado de procesar la información es “Invoice Copies BATO downloader”, o “Invoice Copies FSIP downloader”, al depender de la unidad de negocio.

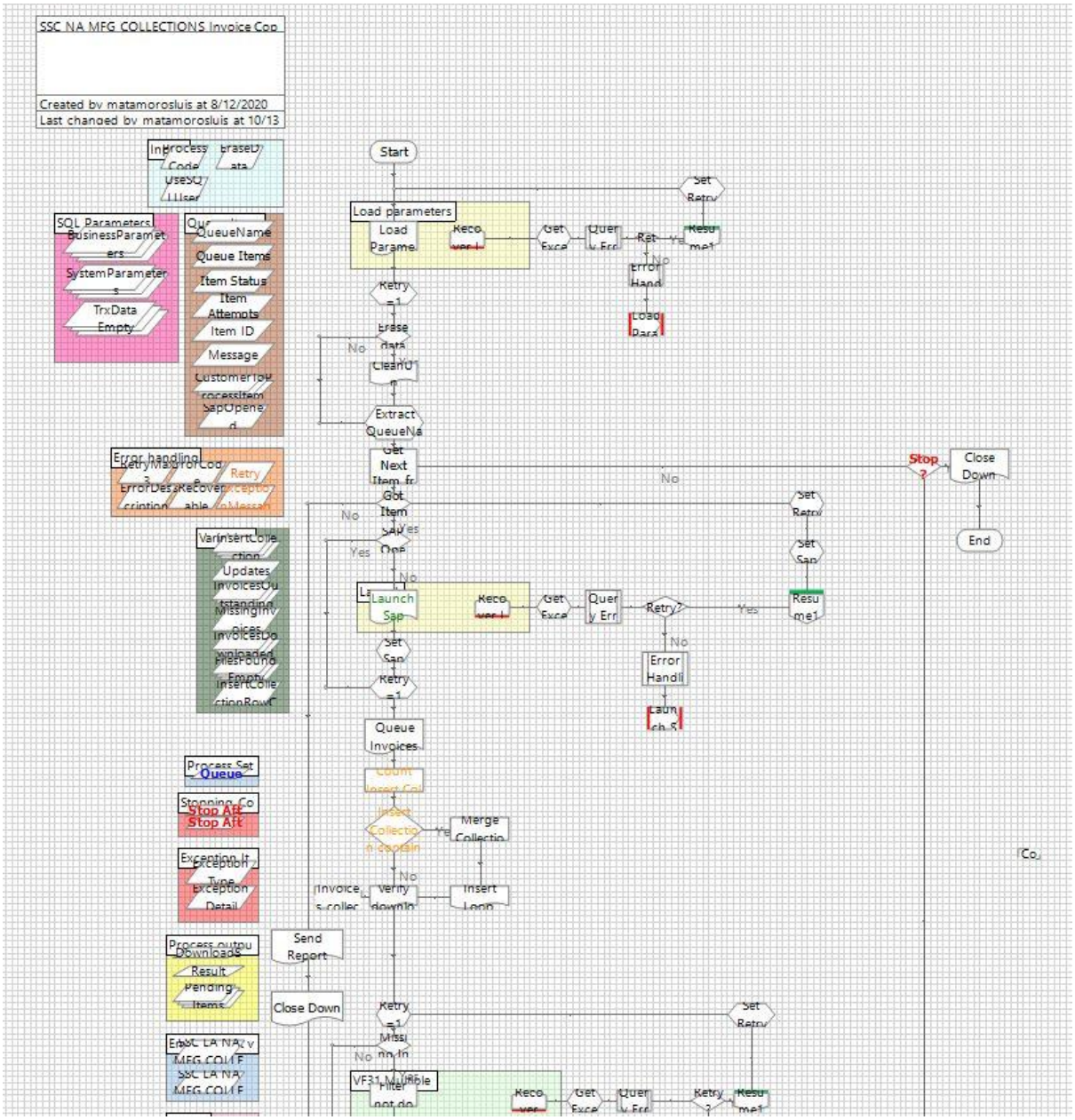



Imagen 22 - Invoice Copies FSIP SAP Downloader

Fuente: Captura de pantalla de robot Invoice Copies

Fuente: Captura de pantalla de robot Invoice Copies

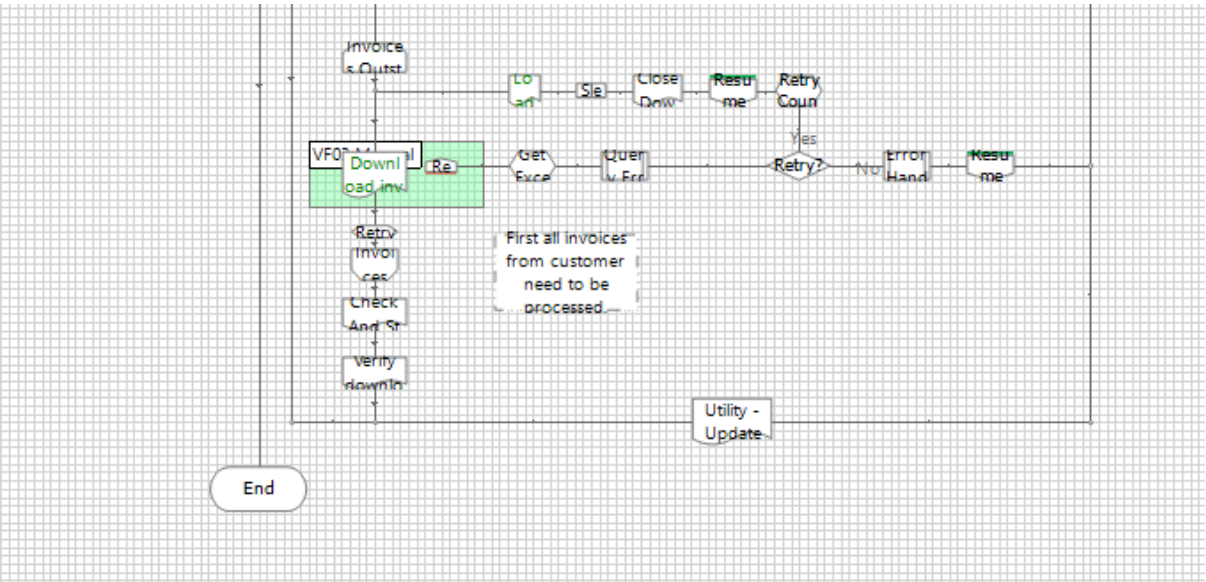



Imagen 23 - Invoice Copies SAP Downloader

Fuente: Captura de pantalla de robot Invoice Copies

En el caso de Invoice Copies FSIP SAP Downloader, uno de los requerimientos es que después de hacer ciertas consultas se inserten nuevos datos dependiendo de los resultados, y se detectó, de acuerdo con las prácticas que debe de utilizar un CoE, que esta parte no se encontraba adecuadamente programada, ya que un robot debe de seguir las características de separación correcta de layers, a pesar de no tener un modelo MVC o similar:

> Cuando se separa la automatización basada en diferentes tipos de lógica y funcionalidad, el equipo se puede asignar para trabajar en las secciones y partes que se ajusten a sus puntos fuertes. Esta lógica se podría desarrollar junto con un arquitecto de procesos de negocio -alguien que esté bien versado en crear y optimizar los elementos de toma de decisiones dentro de una automatización. Mientras tanto, en paralelo, un configurador más junior podría construir las capas para interactuar con la pantalla elementos y para crear objetos que serían utilizados por el arquitecto de procesos de negocio. Esta delineación de tareas y capas permite mayor eficiencia, pero, lo que es más importante,

proporciona un marco de desarrollo donde cada elemento en la configuración funciona por separado, lo que hace es más fácil identificar una falla, hacer un cambio o compartir la configuración entre los miembros del equipo. (HfS & Symphony, 2017, p17)

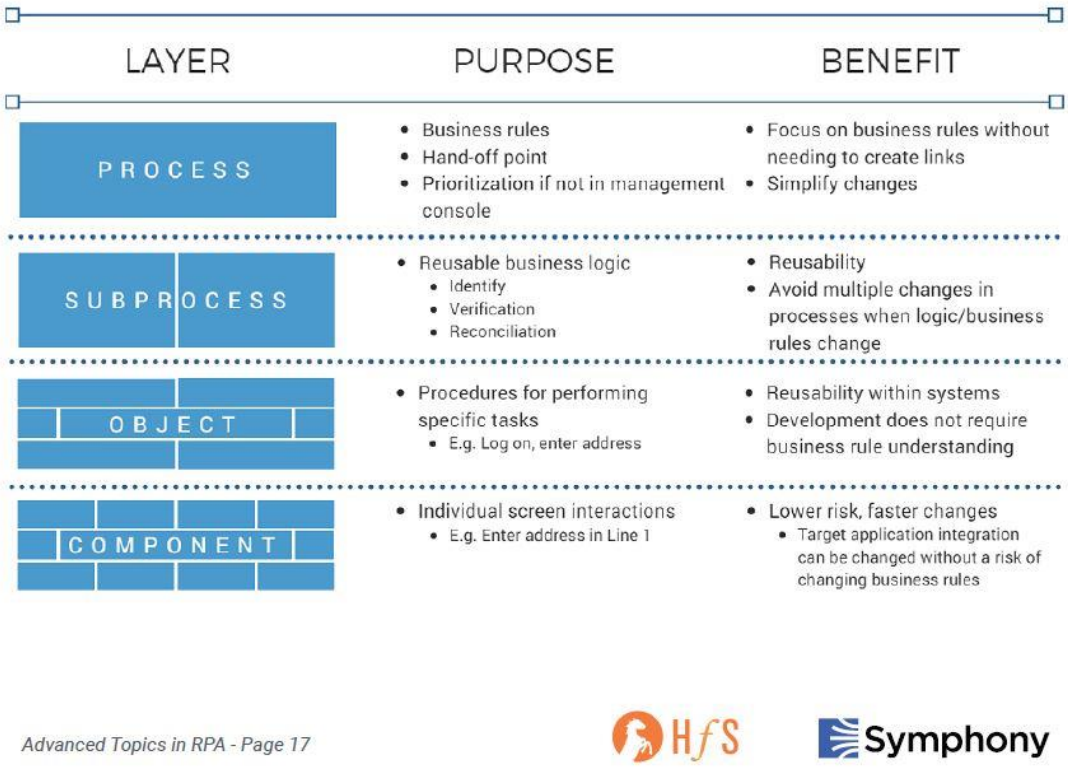



Imagen 24 - Diseño por capas

Fuente: “The RPA Bible: Advanced Topics”

Este robot está compartiendo la capa de negocio y de datos en la misma página, por lo que fue corregido, mediante extracción de los datos por insertar dentro de una colección, para luego en una parte exclusiva dedicarse a la inserción de información en la base de datos.

El tercer robot se encarga de enviar por medio de email las facturas correspondientes a cada cliente. Dentro de los requerimientos se especificó que el cliente puede seleccionar si algunas facturas se envían juntas en un mismo archivo PDF.

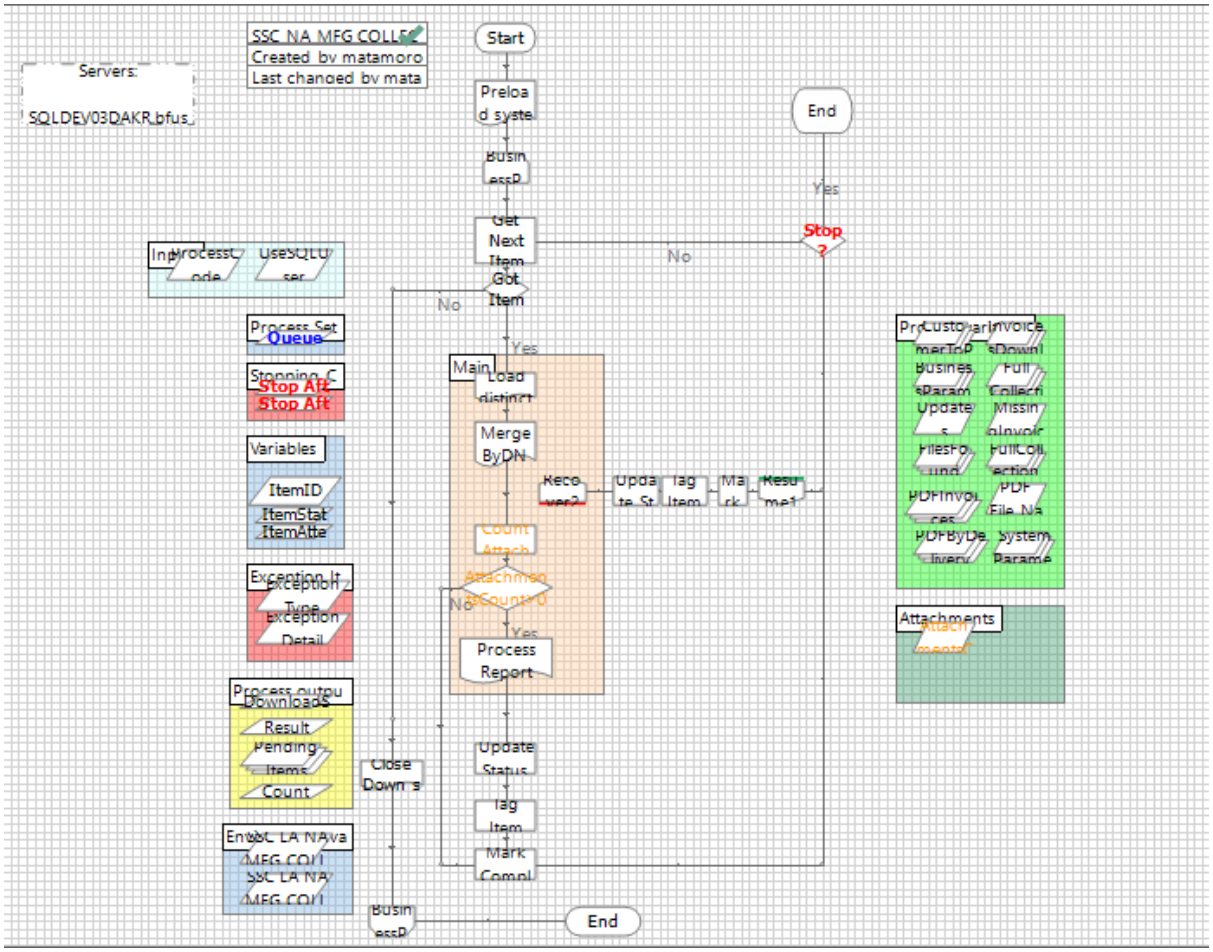



Imagen 25 - Captura de pantalla de Invoice Copies Report

Fuente: Captura de pantalla de robot Invoice Copies

# Capítulo 5. Conclusiones y Recomendaciones.

## 5.1 Conclusiones.

Una vez analizados los datos que se recaban con la investigación, se tienen como conclusiones:

1. Con una investigación previa del sistema de seguridad de información de Bridgestone y conociendo sus necesidades en el nivel de riesgo y cumplimiento, se definen una serie de controles por medio de una matriz integrada para satisfacer requisitos y necesidades del negocio relacionados con RPA, la cual será critica para el crecimiento y madurez del equipo de RPA Costa Rica.
2. Se logra establecer una guía rápida y concisa de cómo usar la matriz con el fin de informar a los encargados de aplicar el marco de controles de seguridad a los robots, ya sea nuevos o existentes.
3. Se soporta el ciclo de vida de desarrollo actual de RPA en la empresa y cualquier otro tipo de metodología de desarrollo o herramientas de automatización. Además, se diseña el marco para que se adapte a distintas situaciones independientemente del método utilizado, los controles siempre pueden llegar a ser aplicados o valorados.
4. Se detectan riesgos al utilizar RPA y herramientas de automatización, de la mano el impacto al no contar con controles de seguridad apropiados en la empresa Bridgestone. Gracias a la aplicación de marcos reconocidos de la industria se pueden detectar y solventar vulnerabilidades asociadas al uso de esta tecnología.
5. Existen riesgos en el nivel de las herramientas de RPA que siguen latentes. Podría ser por la falta de madurez en el campo o bien por la falta de involucramiento del área de Seguridad en las operaciones de RPA, sin embargo, al analizar el sistema de seguridad de información de Bridgestone se aseguró una compatibilidad con su gobierno de seguridad, al dar como resultado un marco de controles holístico que comprendiera las áreas de cumplimiento, requerimientos legales e internos.

6. Dado que este trabajo es pionero en el campo de la seguridad, además es pilar en la revolución industrial 4.0, es una tecnología emergente y que existen muy pocos esfuerzos de investigación, se logra consolidar un entregable muy importante en el área de la

seguridad en RPA, el cual se espera sea utilizado como referencia por diferentes empresas relacionadas al campo.

A pesar de que el equipo de RPA no tiene actualmente un equipo de CoE como tal, es de admirar las muchas buenas prácticas que siguen actualmente, y dentro de esto podemos citar:

- Un proceso de revisión de código estricto, mediante el cual el mismo programador desarrolla el pensamiento de mejores prácticas.
- Utilización de la metodología scrum para el manejo de todos sus proyectos, al utilizar todos sus "artefactos"
- Capacitación y liderazgo continuo de los trabajadores

7. Existen muchos trabajadores que por desconocimiento le tienen temor a la introducción de robots en la empresa, ya que les preocupa que les quiten su puesto. Hasta el momento no existe inteligencia artificial que tenga la creatividad humana. RPA nos puede ayudar a quitarnos de tareas repetitivas, tediosas, e inclusive si le agregamos a la receta un poco de Inteligencia Artificial hasta nos podría ayudar conciertas decisiones basados en lo que hemos hecho anteriormente, pero jamás tendrá la creatividad, las ideas, la inspiración de un humano. Cualquier automatización existente hasta el momento, inclusive machine learning, puede aprender a partir de experiencias anteriores, pero justo ahí está la diferencia:

   No tienen el alma humana. No tienen capacidad de pensar por sí mismos, de tener conciencia. Al final, todo está basado en las indicaciones que se les dan. Mientras más robots se desarrollen, más oportunidad de crear tendremos, más espectro para la creatividad.

   El problema, eso sí, está en las personas que se sienten amenazadas por estas tecnologías, se deprimen, pierden la creatividad, las ideas, la inspiración…. En esos estados, cercanos a la depresión, se pierde hasta en cierto punto hasta la conciencia. En ese caso, definitivamente un robot les aventaja. Esas son las personas por las cuales, si debemos de preocuparnos, y, porque no, implementar planes con cierto porcentaje de los gigantescos ahorros que produce RPA, para sacar adelante a esas personas. Seria valioso

agregarle un punto ético y responsable al sector del RPA. Esto en definitiva le dará más confianza a las personas que se sienten amenazadas.

**5.2 Recomendaciones.**

El hecho de contar con una mayor experiencia en el área de seguridad de la información y a su vez en RPA, facilitará de una mejor manera la forma en que se desarrolla la matriz en el nivel de funcionalidad y adaptación a las necesidades de la empresa.

Es recomendable adquirir una solución de Identidad y Manejo de Accesos adicional al módulo que tenga la plataforma de RPA, en el caso de Blue Prism, el tema de IAM es manejado de manera decente, pero hay varias falencias que pueden ser automatizadas y remediadas utilizando un software que administre credenciales de administrador de manera segura, que utilice *hashes* en vez de contraseñas, que segregue los permisos para asegurar que solo tengan acceso las personas que deberían , que se encargue de aprovisionamiento y des aprovisionamiento de usuarios de manera automática. Agregar una plataforma de ese tipo en RPA puede darles una mayor seguridad y confianza a los dueños de esta para incorporar datos un poco más sensibles y potenciar el uso de la herramienta.

La creación de un centro de excelencia conocido por sus siglas como CoE, es vital para asegurar la participación oportuna y continua de seguridad en las operaciones de RPA. Con esto, se integran la gestión de riesgo empresarial e incluso empezar a auditar de manera frecuente el uso de la tecnología. Este centro también sería una gran base de apoyo para el equipo estadounidense de RPA (El CoE se propondría para Costa Rica)

Por último, se sugiere analizar y mejorar el sistema de seguridad de información de la empresa Bridgestone, así como la forma en cómo gestionan sus riesgos en el nivel de metodología. La falta de una gobernanza clara en el nivel de RPA, lleva a qué áreas como la seguridad, sean pasadas por alto o aplicando controles mínimos que no disminuye la superficie de ataque hacia la tecnología ni las últimas amenazas a las que pueda verse expuesta.

## Capítulo 6. Trabajos de futuro.

La creación y diseño de la matriz de controles en este proyecto es apenas la fase inicial en el nivel de madurez.

Existen varios puntos de mejora, que pueden ser incorporados en versiones futuras, entre ellos destacan:

- Automatizar la matriz de controles de forma que se integre con un sistema de GRC para dar seguimiento a riesgos y velar el estricto cumplimiento.
- Asociar estos controles con un modelo de madurez tales como CMMI, NIST o CIS con el fin de medir progreso y etapas de madurez de la tecnología.
- Alinear esta matriz con la estrategia de ciberseguridad de la empresa, para que contribuya directamente a los objetivos globales de seguridad y a mejorar la postura de la empresa en dicho aspecto.
- Hay que asegurar que dicha matriz de controles pueda integrarse en el proceso de creación y diseño de los robots. Con la creación de un centro de excelencia, la gobernanza a dichos niveles puede facilitar el ciclo de vida de desarrollo y puesta en producción de los robots.

- El Coe es apenas el inicio de un nuevo nivel de mejora continua, después de esto se recomienda comenzar con la certificación del CoE por medio de un ente debidamente autorizado.

**Tabla de Acrónimos**

| Acrónimo | Significado |
|---|---|
| **API** | Application Programming Interface |
| **RPA** | Robotic Process Automation |
| **NIST** | National Institute of Standards and Technology |
| **ISO** | International Organization for Standardization |
| **IA o AI** | Inteligencia Artificial o Artificial Intelligence |
| **CoE** | Centro de Excelencia o Center of Excellence |
| **ISACA** | Information Systems Audit and Control Association |
| **IRPAAI** | Institute for Robotic Process Automation & AI |
| **SQL** | Structured Query Language |
| **FTE** | Fixed Time Employee |
| **SAP** | Systems, Applications, and Products |
| **OPEX** | Operational Expense |
| **POC** | Proof of Concept |
| **TI o IT** | Tecnologías de la Información o Information Technology |
| **ROI** | Return of Investment |

| | |
|---|---|
| **OWASP** | Open Web Application Security Project |
| **GRC** | Governance, Risk and Compliance |
| **RPO** | Recovery Point Objective |
| **RTO** | Recovery Time Objective |
| **BIA** | Business Impact Analysis |
| **AES** | Advanced Encryption Standard |
| **HTTP** | Hypertext Transfer Protocol |
| **SSL** | Secure Socket Layer |
| **SSH** | Secure Shell |
| **VPN** | Virtual Private Network |
| **PKI** | Public Key Infrastructure |
| **PGP** | Pretty Good Privacy |
| **PCI DSS** | Payment Card Industry Data Security Standard |
| **OCR** | Optical character recognition |
| **ISMS** | Information Security Management System |
| **GDPR** | General Data Protection Regulation |
| **IAM** | Identity and Access Management |

| | |
|---|---|
| **BPM** | Business Process Modeler |

**Bibliografía**

Agarwal, M. (18 de septiembre de 2018). *With India Focus, Global Robotics Company UiPath Raises $225 Mn.* Recuperado de https://inc42.com/buzz/with-india-focus-global-robotics-company-uipath-raises-225-mn/

Ayehu (2016). Industries that are Killing it With Robotic Process Automation. https://ayehu.com/4-industries-that-are-killing-it-with-robotic-process-automation/

Bautista, N. (2011). Proceso de la investigación cualitativa: epistemología, metodología y aplicaciones. Bogotá: Manual Moderno.

Blue Prism. (2016). Blue Prism Software Robots. Introducing the Virtual Workforce. Recuperado de https://www.blueprism.com/uploads/resources/white-papers/Blue-Prism-Product-Overview-Enterprise-Edition.pdf

Everest Group Research (2018), Smart RPA Enterprise Playbook

GDPR. (n.d.). *Art. 1 GDPR*. Recuperado de Subject-matter and objectives: https://gdpr-info.eu/art-1-gdpr/

Gregory, P. H. (2018). CISM Certified Information Security Manager All-in-One Exam Guide. McGraw-Hill.

Hfs research (2012) *ROBOTIC AUTOMATION EMERGES AS A THREAT TO TRADITIONAL LOW-COST OUTSOURCING.* Recuperado de https://www.horsesforsources.com/wp-content/uploads/2016/06/RS-1210_Robotic-automation-emerges-as-a-threat-060516.pdf

Hfs research, Symphony Ventures (2017). The RPA Bible. Recuperado de https://sykes-staging.com/campaigns/robotic-process-automation-bible/

Institute for Robotic Process Automation & Artificial Intelligence. (n.d) *Definition and Benefits* . Recuperado de https://irpaai.com/definition-and-benefits/

ISO. (Octubre de 2013). *ISO/IEC 27001:2013*. Recuperado de Information technology — Security techniques — Information security management systems — Requirements: https://www.iso.org/standard/54534.html

ISO. (Octubre de 2013). *ISO/IEC 27002:2013*. Recuperado de Information technology — Security techniques — Code of practice for information security controls: https://www.iso.org/standard/54533.html

ISO. (Dicimebre de 2016). *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. Recuperado de ISO/IEC 27004:2016: https://www.iso.org/standard/64120.html

ISO. (2018). *ISO/IEC 27005:2018*. Recuperado de Information technology — Security techniques — Information security risk management: https://www.iso.org/standard/75281.html

Kalra, P., & Eisnor, M. (2015). Going beyond the call center basics to manage seasonal spikes. Recuperado de https://www.teamhgs.com/blog/going-beyond-the-call-center-basics-to-manage-seasonal-spikes/

Kappagantula, S. (Diciembre de 2018). Robotic Process Automation | *What is Robotic Process Automation*. Recuperado de https://www.edureka.co/blog/robotic-process-automation/#Emergence%20of%20RPA

Krutz, R., & Vines, R. (2006). *The CISSP® and CAP*. Wiley.

Lacity, M. & Willocks L. (2017) Robotic process automation and risk mitigation: the definitive guide" by Ashford, England: SB Publishing

Mindfields (2015) Robotic Process Automation – Driving the next wave of cost rationalization

NIST. (Abril de 2013). *SP 800-53 Rev. 4.* Recuperado de Security and Privacy Controls for Federal Information Systems and Organizations: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

NIST. (Febrero de 2014). *Framework for Improving*. Recuperado de https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

OWASP. (n.d.). *OWASP security Knowledge Framework*. Recuperado de https://owasp.org/www-project-security-knowledge-framework/

PCI Security Standards Council. (Julio de 2018). *PCI DSS Quick Reference Guide*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Roberto Hernández Sampieri, Carlos Fernández Collado, Pilar Baptista Lucio, Metodología de la Investigación, 6ta Edición, México D.F, 2014.

SANS. (n.d.). *CIS Critical Security Controls*. Recuperado de https://www.sans.org/critical-security-controls

Smith, M. (2018). A refresher on robotic process automation. Recuperado de https://medium.com/@_MatthewJSmith/a-refresher-on-robotic-process-automation-97001f1f2025

UC, D. (Marzo de 2019). Duoc.cl. Obtenido de http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

The Federal RPA Community of Practice. (2020). RPA Program Playbook

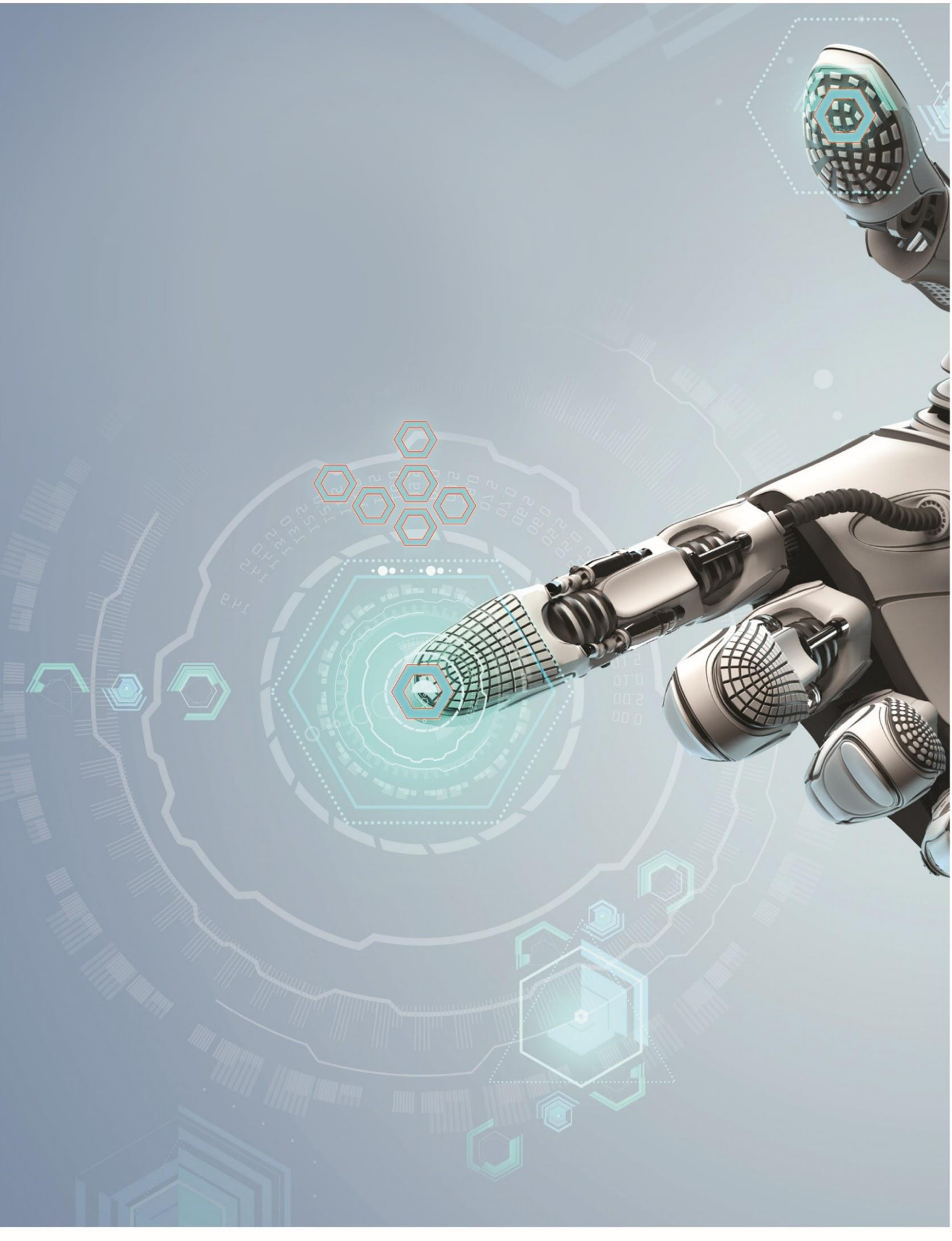
Walker, M. (2019). *CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition, 4th Edition.* McGraw-Hill.

## Anexos

### Anexo 1

PDD Proceso ejemplo

DiRWA
PROCESS AUTOMATION



## Revision Control

| Date | Revision | Description | Author |
|---|---|---|---|
| 04/29/2020 | 1.0 | Solution Design first version | Jorge Palacios<br>Luis Matamoros |

## Design Authority Approval

| Date | Revision | Approver |
|---|---|---|
| | | |

## Customer Approval

| Date | Revision | Approver |
|---|---|---|
| | | |

# 1 Solution Overview

## 1.1 Solution Description

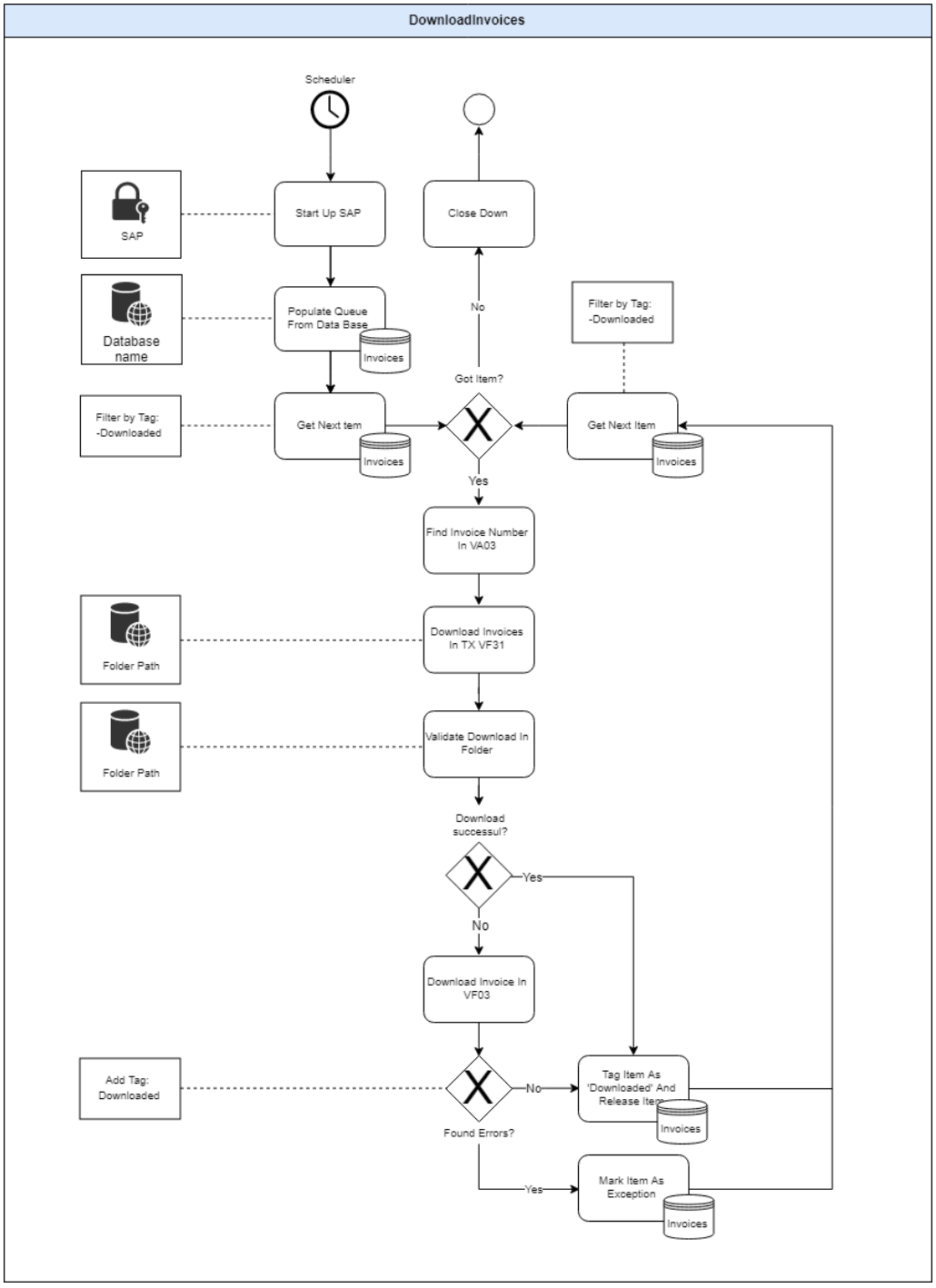
The proposed solution for this process is to build 2 Blue Prism processes using one Work Queue.

The input where the cases will be found will be a SQL Database linked to an Excel spreadsheet, where the SME will enter the cases that they want the bot to process.

The bot will then populate the Work Queue with these cases and proceed to find the Invoice Number in SAP based on the available information provided (it can be either by the PO Number, by the Sales Order Number or the Deliverable Number) in VA03. It will download the invoice in TX VF31 and then validate that it was successfully downloaded, if not, it will download it in VF03. If the invoice was still not successfully downloaded, it will be marked as an exception. If the invoice is downloaded it will be marked with a tag and released for the next process.

The second process will retrieve the cases filtering them by the tag that indicates that the invoices were downloaded and proceed to merge them if required and add to a collection of attachments to be sent by email. If the email is sent all cases will be marked completed.

### 1.1.1 Download Invoices




- Start SAP application using the Blue Prism Start Up standard page and using valid Credentials stored in the Credential Manager. Use an Environment Variable to store the SAP Environment (also known as SAP instance).

- Proceed to populate the Work Queue using the standard Bridgestone Blue Prism page to retrieve Database information.

- The Get Next Item will filter the cases by the ones not containing the tag “Downloaded”.

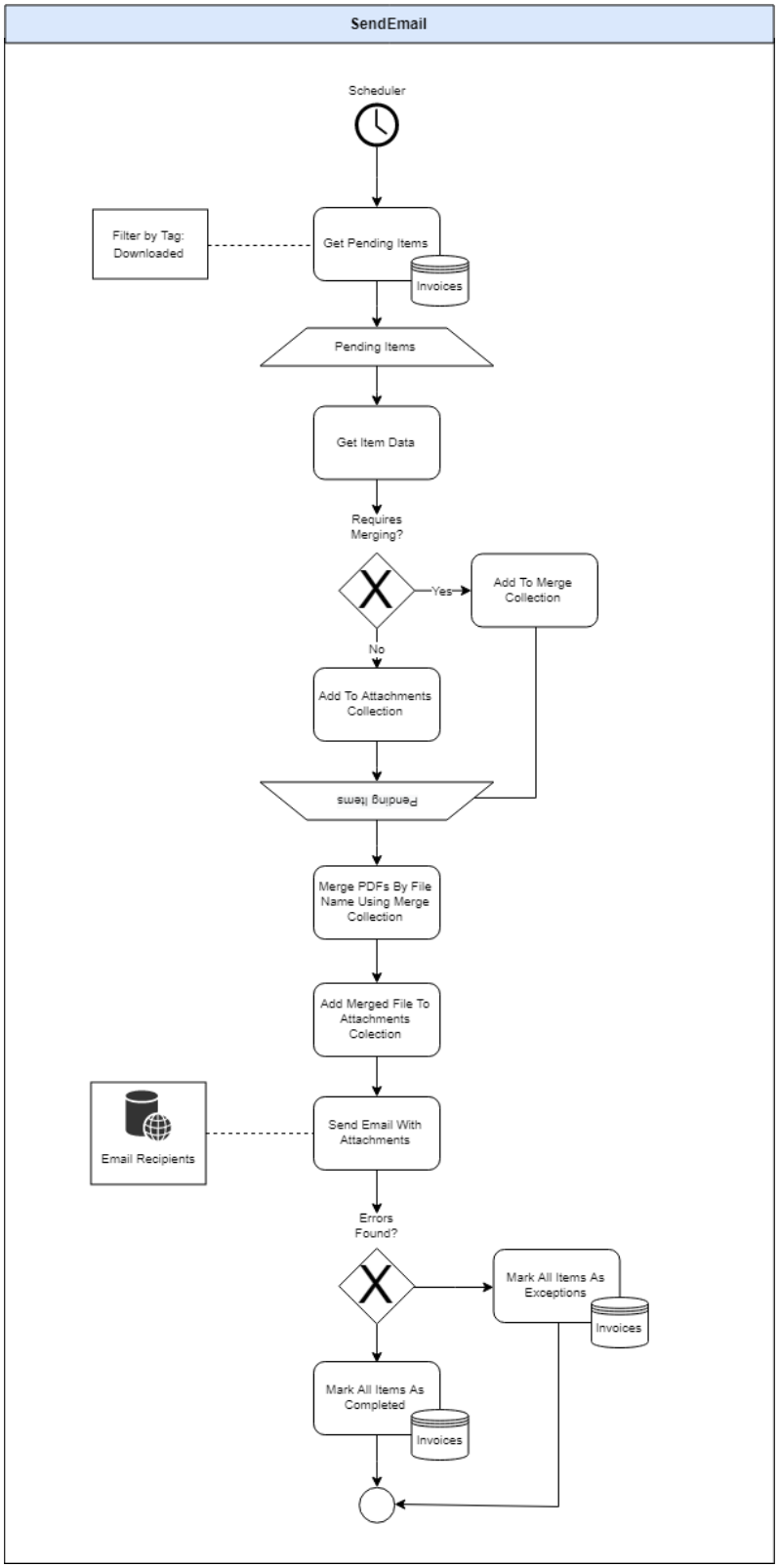
- In the Find Invoice Number page, perform a multiple decision using several decision stages or a choice stage, validating first if the data from the Queue has an Invoice Number, if it does, create a path to search the invoice number with this field. If not, validate if the case has a Sales Order and create a path to search the invoice if it does. Do the same for the Deliverable Number and if the case does not provide any information to search the invoice, send a Business Exception.

- The folder where the invoices will be downloaded is recommended to be stored in an Environment Variable. A subfolder within this folder is also recommended to be created, this can be named after the day of processing.

- Validate that the Invoice was downloaded in the folder, if it was, the case can be moved to the Tag and Release page, if not, perform the steps in the User Stories to download the invoice from VF03. After this, validate if the Invoice was downloaded and if not, Mark the Item as Exception. If downloaded, move the item to the Tag and Release page.

- In the Tag and Release Item page, the item will be tagged as “Downloaded” and released.

### 1.1.2 Send Email




- Use a Get Pending Items action from the Work Queues Object, retrieve the cases filtering by the tag “Downloaded”.

- Loop the collection returned by the Get Pending Items action and inside, a Get Item Data action to retrieve the information of the cases. Validate if the case requires merging the pdf, and if it does, add a row to a new collection (Merge Collection) and save the path of this invoice. If a merge is not required for the invoice, add the path of the invoice to a new collection, Attachments.

- After the loop and with the Merge Collection filled, use the action Merge PDFs by file name of the PDF Manipulation object, to merge all files from the collection into a single file, add this file to the Attachments collection.

- Send the email with the addresses stored in an Environment Variable. Use the Attachments collection to send the PDF files in the action.

- Use the flag of the Send Email action to validate if sending the email was successful. If not, mark all ítems as exceptions.

- If successful, mark all items as Completed and delete the PDF files.

# 2 Process Data

## 3.1 Triggers

The trigger of the process will be a specific scheduler.

The input of the process is the file “Macro Invoice Copies IP” Excel, which the user will produce.

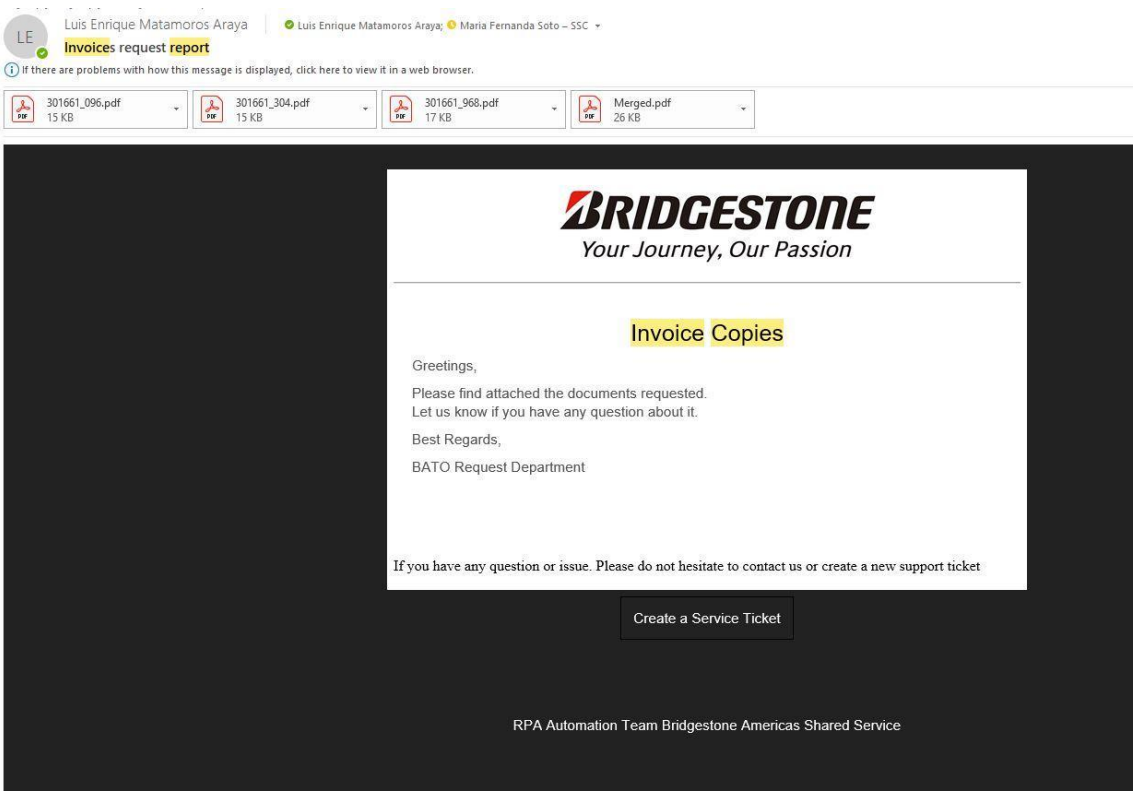


INSERT TABLE TO DB

| BU | Customer Number | Email Address | Invoice # | PO # | Order # | Delivery Order | Ou |
|---|---|---|---|---|---|---|---|
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492258096 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492474304 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492198968 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6491488034 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492059601 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492349929 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6491883288 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6488679668 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6491757750 | | | | |
| PRUEBA | | sotofernanda@la-bridgestone.com | 6492147715 | | | | |

## 2.1 Output

The result will be the email with the processed items, with the suggested format shown below:



## 2.2 Scheduler

The Scheduler will run every day at a suggested time of <Execution time>, considering the business requirements and SLAs.

Will it run on weekends?

NO

Will it run on holidays?

NO

Are there any system requirements that would prevent the process to be executed at a certain time or day (system maintenance)?

## 2.3 Work Queues

### 2.3.1 Invoices

This work queue will contain the information shown in the Database. The item key of the Queue will be the <Case Number>. The data of the queue will be:

- (Item Key)

The item will have the tag “Downloaded”.

## 2.4 Additional Controls

### 2.4.1 Environment Variables.

- **SAP Environment.** Name of the instance to select as it appears in the initial screen of SAP.
- **Downloaded Invoices Folder Path.** Path of the folder where the downloaded will be stored.
- **Email Recipients.** List of email addresses to which all the PDF files will be send to.

### 2.4.2 Credentials.

- **SAP Credential.**

# 3 Assumptions

## 3.1 Technical

Resource PC will have Outlook installed, email inbox configured, Microsoft Excel installed and access to instances of SAP.

**Windows OS Language should be ENGLISH**

**SAP Layout:**

## 3.2 Business

The Business area will fill the input file with sufficient time before the execution of the bot. The format of this file should not be changed.

## Anexo 2

### Hoja de cálculo de matriz de controles de seguridad



RPA Security Controls Framework.xlsx

**Nota: Las siguientes tablas representan un resumen de la hoja de cálculo de la matriz de controles de seguridad y no contienen todas las columnas disponibles por razones del formato de impresión.**

**La hoja de cálculo en versión digital es la fuente completa de este anexo 2.**

**Portada**

| Security Controls Framework (Information Risk [IT and IS] Risks and Controls) | |
|---|---|
| This framework reflects the current inventory of information risks and control objectives. As this framework continues to get reviewed with control owners and as Bridgestone continues to develop their policies and standards, this framework will get updated, reviewed, and approved in line with the formal change process. | |
| **Version:** | v1 |
| **Last Update Date:** | 6/19/2020 |

| **Document Structure** |
|---|
| **Risk Categories**<br>This worksheet lists the information risk categories and sub-categories from the enterprise risk management risk taxonomy. The worksheet also provides a summary of how information risk events roll up to risk sub-categories and risk categories in the taxonomy. These risks are defined at an altitude that can be aggregated across the organization. |
| **Security Controls Framework**<br>This worksheet contains a mapping of processes, risks, controls objectives and requirements, policies and standards, and KPIs. This centralized library is meant to be leveraged to perform the following activities:<br>• Developing policies and standards<br>• Capturing accountability / ownership of controls<br>• Documenting controls and implementation status<br>• Performing control testing<br>• Assessing and prioritizing new risks and issues<br>• Developing KPIs and KRIs for all levels of management<br>• Reporting on risk management maturity and the health of control environment<br>• Guiding RCSA and controls certification<br>• Assessing organization against industry frameworks<br>• Compiling risk reports across the organization in a consistent manner<br>• Strengthening related controls after a business risk event |

**Field Listing:**

- **Cycle** - The high-level control testing cycle which the processes roll up to.
- **Process -** List of processes and subprocesses for which the risks and controls are mapped to.
- **Risk Category** - Level 1 risk as defined in the ERM risk taxonomy (limited to Information Risks). This is the short naming convention; the full definition can be found in the "Risk Categories" tab.
- **Risk Sub-Category** - Level 2 risk as defined in the ERM risk taxonomy (limited to Information Risks). This is the short naming convention, the full definition can be found in the "Risk Categories" tab.
- **Risk Event** - Drop down field of 12 events that impact the business's ability to achieve its objectives by impacting the confidentiality, integrity, or availability of information.
- **Risk Scenario** - A situation or scenario in which the risk event is manifested, describing the actors, methods and negative event. The risk comment is a free-form field, it is the most granular risk statement in this library.
- **Threat Vector** - Common paths or tools that a threat actor uses to realize a risk scenario.
- **Control Objective** - Statement of a desired outcome or purpose of a control.
- **Rationalized Control Requirement** - The control requirements are rationalized from industry and regulatory sources such as NIST CSF, ISO 27001/2, FFIEC, PCI DSS, NIST 800-53 and COBIT.
- **Bridgestone Control Activity-** A set of activities that the organization must perform in order to meet the control objective. The specific control requirements derived from industry and regulatory sources (many to one relationship to control objectives).
- **Control Owner** - The Control Owner is the standard owner's delegate accountable for understanding the control design and monitoring operating effectiveness. They will be the primary point of contact for investigating and remediating issues related to the controls, even if the control is being performed by others.
- **Standard** - The information risk related standard which includes this control requirement. Mapping each control requirement to a standard ensures each control requirement is mapped to a single standard.
- **Policy** - The information risk related policy which includes the control objective. Mapping each control requirement to a policy ensures each control requirement is mapped to a single policy.
- **Metrics -** A numeric measure of the implementation, effectiveness or impact of information risk related controls.
- **Control Type** - Distinguishes whether the control only pertains to PCI in-scope assets or at the application-level.
- **Framework Mapping** - The mapping of each control to specific requirements / guidelines from industry frameworks.
- **Measure Type** - The measurement type as defined in NIST 800-55 Revision 1 - Performance Measurement Guide for Information Security.

**Industry Framework Flags**:

- ***Control Type*** -
- ***NIST CSF*** - Reference ID
- ***ISO 27001*** - Reference ID
- ***ISO 27002*** - Reference ID
- ***FFIEC*** - Reference ID
- ***PCI DSS*** - Reference ID
- ***NIST 800-53 (MOD)*** - Reference ID
- **COBIT** - Reference ID

**Threat Vectors**

This worksheet provides general guidelines on how the threat vectors were mapped.

## Categorías de riesgo

**Information Risk Taxonomy**

| Risk Category | Risk Category Definition | Risk Sub-Category | Risk Sub-Category Definition |
|---|---|---|---|
| Technology Risk | Risk arising from IT systems service disruptions, misconfigurations, aging systems or failure of governance. | System Outage | Risk arising from unexpected natural hazards or technology disruptions, including service level availability issues to systems, platforms, applications, and devices. |
| | | System Misconfiguration | Risks arising from errors, flaws, or misconfigurations in IT infrastructure or applications (e.g., failure of SDLC, change management). |
| | | IT Infrastructure Failure | Risks arising from not maintaining and supporting IT infrastructure including aging and legacy systems. |
| | | IT Governance Failure | Risks arising from failure of governance and IT related processes (e.g., change, capacity, incident, problem management). |
| Cybersecurity Risk | Risk of unprotected systems impacting confidentiality, availability or integrity of IT systems. | Security Breach or Disruption | Risk arising from attack or breach of Bridgestone's data, systems or other information assets due to inadequate |

| | | | |
|---|---|---|---|
| | | | protection, detection, response, and recovery processes. |
| | | Access & Authentication | Risk arising from inadvertent unauthorized access (internal and external) to Bridgestone's systems and information assets. |
| Data and Privacy Risk | Risk arising from the improper use or disclosure of sensitive data. | Data Lifecycle | Risk arising from improper collection, acceptable use, transfer, sovereignty, governance, storage, retention, and disposition of data. |
| | | Data Access Governance | Risk arising from inadequate access restrictions to data allowing unauthorized use, treatment or release of information (i.e., employing principal of least privilege). |
| | | Privacy | Risk arising from improper use, treatment, or release of sensitive consumer data resulting in reputational or financial damagers (e.g., inadequate consumer notice, consumer consent to use or sell information, access to personal data). |

**Risk Event to Risk Category Rollup Overview**

| | Risk Category | Risk Events / Impacts | Definitions |
|---|---|---|---|
| Information Risk | Technology Risk | Business Outage / Service Disruption | Extended outage or disruption of critical business processes |

| | | | |
|---|---|---|---|
| | | IT Related Third Party Support Failure | Failure to identify, measure or manage risks associated with vendors, suppliers or outsourced third parties that support critical IT systems or services |
| | Cybersecurity Risk | Cyber Attack | Disclosure of sensitive data due to a cyber attack |
| | | Client Dissatisfaction Due to Cyber Event | Loss of customer loyalty as a result of cyber attacks |
| | | Brand Reputational Damage Due to Cyber Event | Significant decline in Bridgestone's shareholder value following a cyber attack |
| | | Loss of Competitive Advantage Due to Cyber Event | Intellectual property is disclosed to a competitor and Bridgestone loses its market differentiation, thereby causing a loss in revenues |
| | *Maps to Security and Data & Privacy Risks* | Legal / Regulatory Non-Compliance Due to Cyber Event | Breach of legal / regulatory obligations in conjunction with a cyber incident which leads to fines, sanctions, heightened regulatory scrutiny, or legal proceedings filed against Bridgestone |
| | | Data Manipulation / Corruption | Malicious or inadvertent manipulation / corruption of critical business data |
| | | Negligent Employee | Inadvertent disclosure of sensitive data by an employee |
| | Data and Privacy Risk | Insider Threat | Malicious disclosure of sensitive data by an employee to an |

| | | | |
|---|---|---|---|
| | | | unauthorized recipient |
| | | IT Related Third Party Data Breach / Misuse | Vendors, suppliers, resellers or other third parties fail to adequately protect Bridgestone data |
| | *Can roll up to Technology, Security or Data & Privacy Risk* | Governance Failure | Failure to provide the necessary leadership, organizational structure and supporting processes that enable IT Security |

**Eventos de Riesgo**

| | Risk Event (Cause) | Definition | Impact | Likelihood | Confidentiality | Integrity | Availability | Priority |
|---|---|---|---|---|---|---|---|---|
| R1A | Cyber Attack | Malicious or inadvertent disclosure of sensitive data due to a cyber attack | Data Confidentiality | Likely | x | | | 1 |
| R1B | Insider Threat | Non-public information is disclosed to an unauthorized recipient who uses it for financial gain | Data Confidentiality | Infrequent | x | | | 2 |
| R1C | Negligent Employee | Inadvertent disclosure of sensitive data by an employee | Data Confidentiality | Infrequent | x | | | 2 |
| R2A | Data Manipulation / Corruption | Malicious or inadvertent manipulation / corruption of critical business data | Data Integrity | Infrequent | | x | | 3 |
| R3A | Client Dissatisfaction Due to Cyber Event | Loss of customer loyalty as a result of cyber attacks (e.g., loss of confidence in security controls or dissatisfaction resulting in missing SLAs) | Client / Revenue | Likely | x | x | x | 1 |
| R3B | Loss of Competitive Advantage Due to Cyber Event | Intellectual property is disclosed to a competitor and Bridgestone loses its market differentiation and thereby | Client / Revenue | Likely | x | | x | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | causing a loss in revenues | | | | | | |
| R3C | Brand Reputational Damage Due to Cyber Event | Significant decline in Bridgestone's shareholder value following repeated cyber attacks (e.g., media coverage asserts that Bridgestone's was negligent with confidential issuer data over an extended period of time – causing a major decline in stock value) | Client / Revenue | Infrequent | x | | | 2 |
| R4A | Business Outage / Service Disruption | Extended outage or disruption of critical business processes following a cyber incident (e.g., Missed SLA) | Operational | Frequent | | | x | 2 |
| R5A | IT Related Third Party Support Failure | Failure to identify, measure or manage risks associated with vendors, suppliers or outsourced third parties that support critical IT systems or services | External | Infrequent | x | x | x | 3 |
| R5B | IT Related Third Party Data | Vendors, suppliers, resellers or other third parties fail to | External | Infrequent | x | x | | 3 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Breach / Misuse | adequately protect Bridgestone data | | | | | | |
| R6A | Legal / Regulatory Non-Compliance | Breach of legal / regulatory obligations following a cyber incident which leads to fines, sanctions, heightened regulatory scrutiny, or legal proceedings filed against Bridgestone (e.g., a cyber examination identifies multiple risk and control gaps – resulting in MRA and MRIAs) | Regulatory / Legal | Likely | x | x | | 2 |
| R7A | IT Governance Failure | Failure to provide the necessary leadership, organizational structure | Governance | Frequent | x | x | x | 2 |

## Vectores de amenazas

### General Guidelines for Mapping Threat Vectors to Controls

**General Mapping Guideline**: Controls are mapped to threat vectors if they directly prevent the threat from being exploited. If the control reduces the impact after a threat has been exploited, the control is not mapped to the threat vector.

| Threat Vector | Proposed Definition | Topics Included | Topics Excluded |
|---|---|---|---|
| **Phishing** | Threats arising from a perpetrator masquerading as a legitimate business or reputable person to acquire sensitive data from internal employees, such as credit card information, through a fraudulent solicitation in email or on a web site. | - email communication standards<br>- DLP for outbound traffic | |
| **DDoS** | Threats arising from an attacker using numerous hosts to prevent authorized access to information assets or delay time-critical operations. | - Network controls related to traffic<br>- Network infrastructure, web servers are securely hardened<br>- Router configurations<br>- DNS verification<br>- "denial of service attacks", "DDOS"<br>- Controls about backup information, alternative storage, capacity and availability<br>- Firewall controls<br>- IPS controls | - Environmental controls<br>- BCP training for BCP personnel<br>- BCP Plans<br>- Business impact analysis |
| **Web Vulnerability Exploit** | Threats arising from an attacker taking advantage of a system flaw or weakness in a web-based application to abuse information assets. | - DMZ / externally facing<br>- Patching / EoL<br>- Monitoring unusual traffic<br>- Remote access for employees and non-employees<br>- Network infrastructure, web servers are securely hardened<br>- App security assessments | |
| **Insider Attacks** | Threats arising from the malicious intent of individuals who have internal access to the Bridgestone network which may manipulate, disclose or damage Bridgestone information data or systems. | - Most access management controls (passwords, priv accounts, admin/logical access, physical access)<br>- Alerts regarding | - Firewall for incoming traffic, DMZ / externally facing<br>- antivirus |

| | | | |
|---|---|---|---|
| | | personnel activity<br>- Separation of duties / least privilege<br>- sanitization of media<br>- application blacklisting / whitelisting, least functionality<br>- remote access controls for employees<br>- compliance enforcement<br>- Logging and monitoring | tools<br>- SDLC, security advisement process<br>- network segmentation<br>- include controls about encrypted data transfer or management of cryptographic keys |
| **Patch Exploits** | Threats arising from a malicious individual attacking system that are vulnerable due to a lack of inherent security or effective controls. | - Patching, vulnerability scanning | |
| **Third Party Connectivity** | Threats arising from malicious abuse of company information assets by third parties (vendors, contractors, consultants, service providers etc.) or failure to adhere to company policies and standards. | - Remote third-party access controls<br>- Keywords: non-employees, vendor, third parties/ third party, contractors, supplier, guest<br>- service agreements | |
| **compromise End Points** | Threats arising from an unprotected end point that can exchange digital information or services among other individuals, groups, or institutions from within the Bridgestone network. | - Patching, antivirus<br>- Security hardening<br>- Remote access for employees<br>- Password-related controls<br>- Intrusion prevention and detection controls<br>- alerts<br>- access related controls<br>- sanitization, data disposal<br>- physical access controls, unattended devices<br>- encrypted data transmission, encrypted connection<br>- firewall<br>- cryptographic controls<br>- scanning<br>- identity management | - router, dmz, network segmentation<br>- Secure SDLC |

| | | | |
|---|---|---|---|
| | | - separation of duties, least privilege<br>- wireless access point controls<br>- key management<br>- Covers workstations, servers, phones, etc. | |
| **Cloud Security** | Threats arising from the use of cloud-based applications/infrastructure where security of the service is not under the complete control of Bridgestone. | - Any reference to virtual servers (hypervisor)<br>- Remote administrative access and third-party access<br>- service level agreements with external parties<br>- network infrastructure, web servers on hardened configurations<br>- external connection<br>- outsource | |
| **Mobile Device Exploit** | Threats associated with malicious data manipulation/disclosure or damage to information systems by internal employees while accessing company networks using personal or work mobile devices (smartphones and tablets). | - Reference to personal devices, phones, mobile storage,<br>- Remote access<br>- Password related controls | - General SLDC controls<br>- antivirus on endpoints<br>- malware tools on endpoints<br>- mobile code |
| ***N/A - Topics Not Mapped*** | | | *- Controls related to hiring employees with the right skillset*<br>*- Having policies / procedures / methodology reviewed periodically*<br>*- Auditing*<br>*- Testing of controls*<br>*- Inventory creation / cataloging*<br>*- Training and awareness*<br>*- Data lifecycle* |

**Lista de controles con detalles de objetivos y actividades**

| Cycle | Process | Control Objective ID | Control Objective | Rationalized Control Requirement | Control Activity |
|---|---|---|---|---|---|
| Information and Asset Protection | Asset Management - Inventory | IA-ASMT-INV-010 | Establish and maintain an asset inventory. | An asset lifecycle management program exists. An inventory of all information assets (hardware, software) and assets that internal and external to the organization is developed and updated on a periodic basis. Cardholder data media inventories are conducted on an annual basis. Each information asset has an owner who is accountable for protecting the information asset. The asset inventory captures details such as asset name, type, owner, unique identifier, etc. inventory of assets is reviewed on a periodic basis to ensure accuracy and alignment with business needs and also to determine ways to optimize costs. | Company's asset lifecycle management program is formally governed with established roles and responsibilities. Formal tools, processes, and methodology exist for asset management. Decisions such as sourcing, use, decommissioning or removal of, and all other aspects related to the life cycle of a technology asset, are formally reviewed, approved, documented, and reflected in the asset inventories. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Asset Management - Inventory | IA-ASMT-INV-010 | Establish and maintain an asset inventory. | An asset lifecycle management program exists. An inventory of all information assets (hardware, software) and assets that internal and external to the organization is developed and updated on a periodic basis. Cardholder data media inventories are conducted on an annual basis. Each information asset has an owner who is accountable for protecting the information asset. The asset inventory captures details such as asset name, type, owner, unique identifier, etc. inventory of assets is reviewed on a periodic basis to ensure accuracy and alignment with business needs and also to determine ways to optimize costs. | Each information asset must have an Infrastructure Owner or Enterprise BU/COE Architect that is assigned various responsibilities, including security and data protection for the asset. Each Owner has the following responsibilities:• Assignment of the application, Infrastructure platform to the asset• Assignment of operational responsibility for the asset, including identifying resources or designates who will perform operational tasks such as:o Coordinating security tasks such as patching;o Participating in risk assessments; |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | ando Reviewing periodic reports of the status of security controls for the asset.• Following the Self-Reporting Attestation process by certifying all applications and supporting hardware and software under their management are accounted for and being used according to applicable contract terms and conditions. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Asset Management - Inventory | IA-ASMT-INV-010 | Establish and maintain an asset inventory. | An asset lifecycle management program exists. An inventory of all information assets (hardware, software) and assets that internal and external to the organization is developed and updated on a periodic basis. Cardholder data media inventories are conducted on an annual basis. Each information asset has an owner who is accountable for protecting the information asset. The asset inventory captures details such as asset name, type, owner, unique identifier, etc. inventory of assets is reviewed on a periodic basis to ensure accuracy and alignment with business needs and also to determine ways to optimize costs. | Cardholder data media inventories are conducted on an annual basis. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Asset Management - Inventory | IA-ASMT-INV-010 | Establish and maintain an asset inventory. | An asset lifecycle management program exists. An inventory of all information assets (hardware, software) and assets that internal and external to the organization is developed and updated on a periodic basis. Cardholder data media inventories are conducted on an annual basis. Each information asset has an owner who is accountable for protecting the information asset. The asset inventory captures details such as asset name, type, owner, unique identifier, etc. inventory of assets is reviewed on a periodic basis to ensure accuracy and alignment with business needs and also to determine ways to optimize costs. | A current inventory of all backup media, whether stored on-site or at a remote location, must be maintained and reviewed for accuracy and completeness at least annually. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Asset Management - Inventory | IA-ASMT-INV-010 | Establish and maintain an asset inventory. | A current inventory of all software platforms and applications including license keys is documented and maintained. | A current inventory of all software platforms and applications including license keys is documented and maintained. Software licenses are reviewed periodically to prevent the inclusion of unauthorized software, or any software instances in excess of current license agreements, in the technology environment. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Data Inventory, Classification and Protection - Data Retention | IA-DICP-DRT-020 | Sensitive authentication data only is stored by issuers and companies that support issuing services when there is a business justification, and the data is stored securely. | Sensitive authentication data or other personally identifiable information is not stored (even if encrypted) after authorization. Sensitive authentication data or other personally identifiable information is rendered unrecoverable upon completion of the authorization process. For the cardholder data environment, the following sensitive authentication data is not stored: - Full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)- Card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions - Personal | Sensitive authenticatio n data or other personally identifiable information is not stored (even if encrypted) after authorizatio n. Sensitive authenticatio n data or other personally identifiable information is rendered unrecoverab le upon completion of the authorizatio n process. For the cardholder data environment , the following sensitive authenticatio n data is not stored: - Full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere)- Card verification code or |

| | | | | | |
|---|---|---|---|---|---|
| | | | | identification number (PIN) or the encrypted PIN block. | value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions - Personal identification number (PIN) or the encrypted PIN block. |

| | | | | | |
|---|---|---|---|---|---|
| Information and Asset Protection | Privacy Processes and Controls - Data Leakage | IA-PPCO-DLK-010 | Protections against data leaks are implemented. | Unauthorized leaks of data, specifically PII and PHI, are prevented or detected. The processor prevents or monitors for unauthorized leakage of data or enables the capability for its customers to prevent or monitor for the unauthorized leakage of data. DLP tools monitor outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at interior points within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information. | Unauthorized leaks of data, specifically PII and PHI, are prevented or detected. The processor prevents or monitors for unauthorized leakage of data or enables the capability for its customers to prevent or monitor for the unauthorized leakage of data. DLP tools monitor outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at interior points within the system (e.g., subsystems, subnetworks) to detect covert exfiltration of information. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Administrative Access | ID-IDAM-ADA-010 | Privileged user roles and responsibilities are managed and tracked. | Privileged user access is administered on a controlled basis and approved by an authorized individual. Administrative responsibilities for user accounts, such as additions, deletions, and modifications, are assigned to the appropriate personnel. | Privileged user access is administered on a controlled basis, approved by an authorized individual, and assigned to appropriate personnel. All privileged user access requests must be recorded and retained in accordance with the Record Retention Schedule. Only authorized administrators shall have Superuser access to server operating systems. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Segregation of Duties | ID-IDAM-NIL-010 | Segregation of Duties is maintained and enforced for critical business processes and in production environments. | Segregation of duties is achieved by organizing personnel into relevant and defined functional groups, to reduce opportunities for unauthorized or unintentional modification or misuse of organization's assets and to prevent unauthorized changes to production environments. | Personnel are organized into relevant and defined groups to provide segregation of duties and prevent misuse of organizational assets.Separate access requests must be used to gain access to production, development, user acceptance testing, quality assurance and any additional environment, to ensure separation of duties and protection of credentials is maintained. A separate request must be made and authorized for each User ID. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Provisioning | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | A formal access registration and provisioning process is in place to assign access rights for all user types to all systems and services, in alignment with the access control policy. | A formal access registration and provisioning process exists and is in alignment with access control policy. Every request for a new or amended ID must be appropriately documented and be validated by an authorized business manager prior to being set up or amended. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Authorization | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | Logical access to information and system resources requires authorization from a designated authority in accordance with applicable access control policies. | Logical access to information and system resources requires authorization from a designated authority in accordance with applicable access control policies. Company users must only be provided with access to the information systems, services, and applications that they have been specifically authorized to use. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Least Privilege | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Non-privileged users are prevented from executing privileged functions. Access is limited to the types of transactions and functions that authorized users are permitted to execute. | Access to applications and systems by Company users must be based on a principle of least privilege – a user's access must be limited to the functions and menus needed to perform the user's job responsibilities. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Least Privilege | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Non-privileged users are prevented from executing privileged functions. Access is limited to the types of transactions and functions that authorized users are permitted to execute. | Non-privileged users are prevented from executing privileged functions. Access is limited to the types of transactions and functions that authorized users are permitted to execute. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access control systems | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | An access control system is in place to support information system account management and to restrict access unless access is specifically granted. This access control system includes the following:- Coverage of all system components- Assignment of privileges to individuals based on job classification and function- Default “deny-all” setting. | The Company Access Management Tool is used as an access control system to support information system account management and to restrict access unless access is specifically granted. All new systems (operating systems, applications, databases, firewalls, and network devices) must be fully integrated with the tool. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Identity and Access Management | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | Access to database is restricted. For databases in the CDE, the access (including access by applications, administrators, and all other users) is restricted as follows:- All user access to, user queries of, and user actions on databases are through programmatic methods.- Only database administrators have the ability to directly access or query databases.- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | For PCI systems access to database is restricted. For databases in the CDE, the access (including access by applications, administrators, and all other users) is restricted as follows:- All user access to, user queries of, and user actions on databases are through programmatic methods.- Only database administrators have the ability to directly access or query databases.- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Identity and Access Management - ID Management | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | The organization requires that users of privileged information system accounts or roles with access to organization-defined security functions or sensitive security-relevant information use non-privileged accounts or roles when accessing non security functions. | Privileged users must use their non-privileged User ID for non-privileged functions. A separate User ID must be issued for all privileged access assigned to a given user and that account used only for the designated elevated processes or actions. |
| Identity and Access Management | Identity and Access Management - ID Management | ID-IDAM-NIL-020 | Access to systems and assets is controlled by incorporating the principle of least privilege. | Shared/group accounts are managed per the organizational guidelines. For the CDE, the following guidelines are followed:- Generic user IDs are disabled or removed. - Shared user IDs do not exist for system administration and other critical functions. - Shared and generic user IDs are not used to administer any system components. | For PCI systems, shared or group accounts/passwords are prohibited from use.For the CDE (Cardholder data environments), generic user IDs are disabled or removed and are not used to administer any system components. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Identity and Access Management - ID Management | ID-UAPD-NIL-010 | Unique identities and credentials are managed for authorized devices and users. | Individual user accounts (for system users, processes acting on behalf of users, or devices) are assigned unique identifiers (User ID) to manage access to information systems and devices. Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms are assigned as follows: 1. Authentication mechanisms are assigned to an individual account and not shared among multiple accounts 2. Physical and/or logical controls are in place to ensure only the intended account can use that mechanism to gain access. | Unique user IDs must be assigned to each user (and processes acting on behalf of users or devices) to manage access to information systems and devices. Users must not share their IDs or passwords. Company controlled User ID accounts may not utilize PII data elements as part of their username. This applies to both internal and external facing applications. Account names are static per recipient and must not change once assigned unless the user requests such change.Addition, deletion, and modification of user IDs, credentials, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | and other identifier objects requires authorizatio n. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Identity and Access Management - ID Management | ID-UAPD-NIL-010 | Unique identities and credentials are managed for authorized devices and users. | Individual user accounts (for system users, processes acting on behalf of users, or devices) are assigned unique identifiers (User ID) to manage access to information systems and devices. Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms are assigned as follows: 1. Authentication mechanisms are assigned to an individual account and not shared among multiple accounts 2. Physical and/or logical controls are in place to ensure only the intended account can use that mechanism to gain access. | Where nonuser ID authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms are assigned as follows: 1. Authentication mechanisms are assigned to an individual account and not shared among multiple accounts 2. Physical and/or logical controls are in place to ensure only the intended account can use that mechanism to gain access. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Identity and Access Management - ID Management | ID-UAPD-NIL-010 | Unique identities and credentials are managed for authorized devices and users. | Processes for managing and controlling user identifiers are defined and implemented. Addition, deletion, and modification of user IDs, credentials, and other identifier objects requires authorization. User identifiers are not re-used for a defined time period and are disabled after a period of inactivity. | All User IDs shall have the associated privileges suspended after thirty (30) days of non-use and the User ID deleted after ninety (90) days of non-use.System access for consultants and temporary personnel must automatically expire at the end of the current contract term. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Transfers | ID-UAPD-NIL-030 | Access permissions are revoked based upon access reviews and/or user terminations. | The organization has a defined process for reviewing and authorizing access permissions for employee transfers/change of roles. | The organization has a defined process for reviewing and authorizing access permissions for employee transfers/change of roles. When a user's access requirements warrant removal from a particular system (i.e., the user changes departments or job roles and should not have access to previous systems) a user de-registration process must be carried out. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Deprovisioning | ID-UAPD-NIL-030 | Access permissions are revoked based upon access reviews and/or user terminations. | A formal user deprovisioning process is in place. Timely revocation of logical access to information and system resources is enforced as a result of a termination of a user's account. Access for temporary, emergency accounts, and inactive accounts are revoked after a defined period of time. Anonymous accounts which cannot be linked to a unique user or accounts associated with users who may be a significant risk to the system are revoked upon detection. | A formal user deregistration process is in place. Timely revocation of logical access to information and system resources is enforced as a result of a termination of a user's account. Access to critical systems and applications must be removed within twenty-four (24) hours of the termination date. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Deprovisioning | ID-UAPD-NIL-030 | Access permissions are revoked based upon access reviews and/or user terminations. | A formal user deprovisioning process is in place. Timely revocation of logical access to information and system resources is enforced as a result of a termination of a user's account. Access for temporary, emergency accounts, and inactive accounts are revoked after a defined period of time. Anonymous accounts which cannot be linked to a unique user or accounts associated with users who may be a significant risk to the system are revoked upon detection. | Access for temporary, emergency accounts, and inactive accounts are revoked after a defined period of time. Anonymous accounts which cannot be linked to a unique user or accounts associated with users who may be a significant risk to the system are revoked upon detection. |
| Identity and Access Management | Access Deprovisioning | ID-UAPD-NIL-030 | Access permissions are revoked based upon access reviews and/or user terminations. | The organization employs mechanisms to notify individuals and teams responsible for disabling access upon termination of an individual or for modifying access when there is a change in the role. | The organization employs mechanisms to notify individuals and teams responsible for disabling access upon termination of an individual or for modifying access when there is a |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | change in the role. |
| Identity and Access Management | Access Recertification | ID-UAPD-NIL-050 | Access permissions are reviewed periodically for appropriateness. | Access privileges assigned to users are reviewed and validated periodically. Modifications or removal of privileges is performed as necessary. An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained. | All users' access rights shall be reviewed at a minimum of quarterly and after any significant changes. Modifications or removal of privileges is performed as necessary. |

| | | | | | |
|---|---|---|---|---|---|
| Identity and Access Management | Access Recertification | ID-UAPD-NIL-050 | Access permissions are reviewed periodically for appropriateness. | Access privileges assigned to users are reviewed and validated periodically. Modifications or removal of privileges is performed as necessary. An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained. | Privileged user access certifications, to include access rights and authorization rights, are to be reviewed at least every ninety (90) days and after any significant changes. |
| Identity and Access Management | Access Recertification | ID-UAPD-NIL-050 | Access permissions are reviewed periodically for appropriateness. | Access privileges assigned to users are reviewed and validated periodically. Modifications or removal of privileges is performed as necessary. An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained. | An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained. |

| | | | | | |
|---|---|---|---|---|---|
| Risk, Compliance and Policy Management | Regulatory Compliance Management | RC-COMP-NIL-010 | Legal and regulatory requirements regarding intellectual property rights, use of proprietary software, and cybersecurity, including privacy and civil liberties obligations, are understood and managed. | All relevant legislative, statutory, regulatory, contractual obligations and intellectual property rights, along with the organization's approach to meet these requirements, should be explicitly identified, documented and kept up to date for each information system and the organization. Appropriate procedures should be implemented to maintain ongoing awareness and incorporation of legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products to the organization's processes. | Security compliance assessments are conducted based on the scope of security compliance program. |

| | | | | | |
|---|---|---|---|---|---|
| Risk, Compliance and Policy Management | Regulatory Compliance Management | RC-COMP-NIL-010 | Legal and regulatory requirements regarding intellectual property rights, use of proprietary software, and cybersecurity, including privacy and civil liberties obligations, are understood and managed. | All relevant legislative, statutory, regulatory, contractual obligations and intellectual property rights, along with the organization's approach to meet these requirements, should be explicitly identified, documented and kept up to date for each information system and the organization. Appropriate procedures should be implemented to maintain ongoing awareness and incorporation of legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products to the organization's processes. | Appropriate procedures are implemented to maintain ongoing awareness and incorporation of legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products to the organization's processes. |

| | | | | | |
|---|---|---|---|---|---|
| Risk, Compliance and Policy Management | Policies, Standards, and Guidelines Management - Acceptable Use Policies | RC-PSGM-AUP-010 | Policies are established for the acceptable use of information assets which are internally accessible by the business. | The information systems display notification message requiring consent on usage prior to granting access to the system. Privacy and security notices consistent with applicable rules and regulations are provided to users accessing systems. | The information systems display notification message requiring consent on usage prior to granting access to the system. Privacy and security notices consistent with applicable rules and regulations are provided to users accessing systems. |

| | | | | | |
|---|---|---|---|---|---|
| Risk, Compliance and Policy Management | Risk Identification and Assessment | RC-RIAT-NIL-010 | Threats, both internal and external, are identified and documented | a. Organization has a formally documented risk assessment methodology that is reviewed and maintained. A criteria for risk acceptance is established.b. Security threats and vulnerabilities have been identified and documented. Periodic information security risk assessments (at least annually or upon changes to the environment) are conducted identify, quantify, and prioritize relevant threats and vulnerabilities based on their likelihood and impact to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.c. Risk owners are determined as part of the risk assessment process. Results of risk assessment are communicated | Security threats and vulnerabilities have been identified and documented. Periodic information security risk assessments (at least annually or upon changes to the environment ) are conducted identify, quantify, and prioritize relevant threats and vulnerabilities based on their likelihood and impact to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | and reported to Senior Management for review and approval. | |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-010 | The organization enforces a standard approach for program / project management to enable project governance, manage stakeholder engagement, and achievement of desired outcomes. | A formal, approved integrated plan is established and maintained to guide program and project execution and control throughout the life of the program and project. The program/project scope, associated deliverables, milestones, and acceptance criteria are clearly defined and tied to the strategic objectives of the program/project. | A formal, approved integrated plan is established and maintained to guide program and project execution and control throughout the life of the program and project. The program/project scope, associated deliverables, milestones, and acceptance criteria are clearly defined and tied to the strategic objectives of the program/project. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-010 | The organization enforces a standard approach for program / project management to enable project governance, manage stakeholder engagement, and achievement of desired outcomes. | Formal project and program management approach and standards that align with enterprise's culture and operating environment have been established. The approach and standards enable project governance and achievement of desired outcomes. | Formal project and program management approach and standards that align with enterprise's culture and operating environment have been established. The approach and standards enable project governance and achievement of desired outcomes. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-010 | The organization enforces a standard approach for program / project management to enable project governance, manage stakeholder engagement, and achievement of desired outcomes. | A business case, which is reviewed and approved by program sponsors, is established and maintained for projects and programs. The business case outlines expected benefits, feasibility analysis, a benefits realization and measurement plan, the full scope of initiatives required, the risk involved and the impact. Commitment and participation from the sponsors and impacted stakeholders is obtained during the definition and execution of the project. | A business case, which is reviewed and approved by program sponsors, is established and maintained for projects and programs. The business case outlines expected benefits, feasibility analysis, a benefits realization and measurement plan, the full scope of initiatives required, the risk involved and the impact. Commitment and participation from the sponsors and impacted stakeholders is obtained during the definition and execution of the project. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-020 | The organization's investment portfolio supports organization goals, needs, and strategy. | The organization determines the investment mix based on cost, alignment with strategy, and financial measures such as cost and expected return of investment over the full economic life cycle, degree of risk, and type of benefit for the programs in the portfolio. A formal process exists to evaluate and prioritize program business cases, and decide on investment proposals, including the allocation of funds and initiation of programs. | The organization determines the investment mix based on cost, alignment with strategy, and financial measures such as cost and expected return of investment over the full economic life cycle, degree of risk, and type of benefit for the programs in the portfolio. A formal process exists to evaluate and prioritize program business cases, and decide on investment proposals, including the allocation of funds and initiation of programs. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-030 | The organization monitors and optimizes its investment portfolio regularly throughout the entire investment life cycle and actively engages with stakeholders. | Project stakeholders, including program steering committee and sponsors, are apprised of the program's and project's scope, progress, schedule, quality, benefits realization, costs, and risks on a regular basis and also during stage-gate reviews. Stakeholder expectations are continuously reviewed and addressed throughout the lifecycle of the project and program. | Project stakeholders, including program steering committee and sponsors, are apprised of the program's and project's scope, progress, schedule, quality, benefits realization, costs, and risks on a regular basis and also during stage-gate reviews. Stakeholder expectations are continuously reviewed and addressed throughout the lifecycle of the project and program. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-040 | The organization allocates appropriate resources to information security and risk management. | The organization establishes a plan for the allocation of appropriate resources to projects and programs based on assessing organizational, operational, and strategic considerations | The organization establishes a plan for the allocation of appropriate resources to projects and programs based on assessing organizational, operational, and strategic considerations |
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-040 | The organization allocates appropriate resources to information security and risk management. | Resources (human, technology, finance) required to achieve security objectives are allocated for the establishment, implementation, maintenance and continual improvement of the information security management system. | A formal budgeting process exists to fund security capital and operational expenditures |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Finance and Portfolio Management - Portfolio and Program Management | SG-FIPM-PPM-060 | Implement security controls in projects. | Information security is addressed in project management, regardless of the type of the project. | Information security is addressed in project management, regardless of the type of the project. |
| Strategy, Governance and Management | Personnel Strategy - Roles and Responsibilities | SG-PERS-RRS-010 | Employees understand their responsibilities outlined in the code of conduct. | The organization notifies individuals of legally binding post-employment requirements for protection of organizational information and requires individuals to sign an acknowledgment of these requirements as part of granting initial access to covered information. Non-employees are provided the organization's data privacy and security policy prior to accessing system resources and data. | Contractors and Contingent workers (Non-employees) are provided the organization's data privacy and security policy prior to accessing system resources and data. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Personnel Strategy - Roles and Responsibilities | SG-PERS-RRS-020 | All applicable personnel understand their roles and responsibilities. | The organization has established and communicated roles and responsibilities for IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability. | The organization has established and communicated roles and responsibilities for IT personnel, as well as other stakeholders with responsibilities for enterprise IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability. |
| Strategy, Governance and Management | Personnel Strategy - Roles and Responsibilities | SG-PERS-RRS-030 | All employees acknowledge their security responsibilities. | Employees acknowledge that they have read and understood their responsibilities outlined in the Code of Conduct Handbook and in information security policies. | Employees acknowledge that they have read and understood their responsibilities outlined in the Code of Conduct Handbook and in information security policies. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Project Management | SG-PM-NIL-060 | Active risk management practices are incorporated throughout project lifecycle. | Project managers practice active risk management and quality assurance throughout the project lifecycle. Risks faced by the project are established and centrally recorded. Specific risks associated with projects are eliminated or minimized through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. | Project managers practice active risk management and quality assurance throughout the project lifecycle. Risks faced by the project are established and centrally recorded. Specific risks associated with projects are eliminated or minimized through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Project Management | SG-PRMT-NIL-020 | Projects are completed and deliver the planned results and benefits. | At the end of each project, post implementation reviews are performed to ascertain whether the project delivered the planned results and benefits. Any outstanding activities are identified and communicated. | At the end of each project, post implementation reviews are performed to ascertain whether the project delivered the planned results and benefits. Any outstanding activities are identified and communicated. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Project Management - Quality Management | SG-PRMT-QMT-010 | Quality of processes, projects, programs, organizational units, products or services is managed continuously. | A quality management system (QMS) is established and maintained that provides a formal and continuous approach for quality management. An overall quality plan is maintained and regularly communicated to promote continuous improvement. The QMS data is analyzed for effectiveness and opportunities for improvement, including corrective and preventive actions, are taken to eliminate the cause of identified and potential nonconformities. | A quality management system (QMS) is established and maintained that provides a formal and continuous approach for quality management. An overall quality plan is maintained and regularly communicated to promote continuous improvement. The QMS data is analyzed for effectiveness and opportunities for improvement, including corrective and preventive actions, are taken to eliminate the cause of identified and potential nonconformities. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Project Management - Quality Management | SG-PRMT-QMT-010 | Quality of processes, projects, programs, organizational units, products or services is managed continuously. | 1. The organization has established QMS standards, practices, and procedures and incorporate relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings.2. The organization performs periodic quality monitoring and certification of key IT processes, projects, programs, organizational units, products or services. | The organization has established QMS standards, practices, and procedures and incorporate relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings. |
| Strategy, Governance and Management | Strategy and Direction - Organizational Strategy and Direction | SG-STRT-OSD-050 | Risk tolerance and corresponding strategies have been defined and communicated to different stakeholders | Organization's risk tolerance is considered while designing business processes. The business processes are updated until the organization's level of risk tolerance is achieved. | Organization's risk tolerance is considered while designing business processes. The business processes are updated until the organization's level of risk tolerance is achieved. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Strategy and Direction - Organizational Strategy and Direction | SG-STRT-OSD-050 | Risk tolerance and corresponding strategies have been defined and communicated to different stakeholders | The organization has developed and implemented a comprehensive strategy to manage enterprise risk in alignment with its established level of risk tolerance. The risk strategies are updated as needed. The information security strategy outlines the initiatives required to achieve security objectives, resources and budget required, associated roles and responsibilities, timelines for completion, and key metrics for evaluation of success of the security strategy. The strategy will be aligned with the security objectives, take into account results of risk assessment, will be periodically updated and is communicated to relevant key stakeholders. | The strategy will be aligned with the security objectives, take into account results of risk assessment, will be periodically updated and is communicated to relevant key stakeholders. |

| | | | | | |
|---|---|---|---|---|---|
| Strategy, Governance and Management | Strategy and Direction - Organizational Strategy and Direction | SG-STRT-OSD-050 | Risk tolerance and corresponding strategies have been defined and communicated to different stakeholders | Organizational risk tolerance is determined and clearly expressed. Organization evaluates the external environment, internal environment, its role in the critical Infrastructure, business objectives, and sector specific risks, while determining risk tolerance. | Organizational risk tolerance is determined and clearly expressed. Organization evaluates the external environment, internal environment, its role in the critical Infrastructure, business objectives, and sector specific risks, while determining risk tolerance. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-010 | Logging mechanisms and the ability to track activity is established, tracked, and monitored. | Logging mechanisms are configured to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity: The following events are tracked:- General user access and activities- Privileged / Super user (root, admin etc.) access and activities- Access to audit logs - Invalid access attempts- Changes to identification and authentication mechanisms- Changes to or elevation of privilege access rights- Initialization, stopping, or pausing of the audit logs- Creation and deletion of system - level objects- Exceptions- System faults- Information security events- System/network eventsFor each event, the following | Logging mechanisms are configured to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity: The following events are tracked:- General user access and activities- Use of system utilities- Root access and activities- Access to audit logs- Invalid access attempts- Changes to identification and authentication mechanisms - Creation, deletion, or changes to a privileged user account- Initialization, stopping, or pausing of the audit logs- |

| | | | | | |
|---|---|---|---|---|---|
| | | | | details are captured:- Type of event- Timestamp- Where the event occurred (Destination IP address, hostname etc.)- Source of the event (Source IP address, hostname etc.)- Outcome of the event (success/failure) - Unique identity of individuals associated with the event- Identity or name of affected data, system component, or resource. | Creation and deletion of system-level objects- exceptions- system faults- information security events- system/network events- Application of patches- Change in all user rights (person, system, regular and privileged)For each event, the following details are captured:- Type of event - User Identification - Source and Destination IP address - Port and Protocol used - Terminal address and location - Date and time stamp - Activity type attempted (login, login help, update, delete, insert, create, file upload/download, etc.) - |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Activity success/fail - Before and after values- Identity or name of affected data, system component, or resource. |
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-010 | Logging mechanisms and the ability to track activity is established, tracked, and monitored. | The types of events that are logged are reviewed and updated on a periodic basis. Inputs from multiple stakeholders across different functions and entities are obtained while determining the types of events to be logged. | The types of events that are logged are reviewed and updated on a periodic basis. Inputs from multiple stakeholders across different functions and entities are obtained while determining the types of |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | events to be logged. |
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-020 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Audit logs from multiple sources are captured and are correlated and reviewed using automated mechanisms in accordance with formal information security policies. Procedures are in place to take follow-up actions for anomalies and indications of inappropriate, suspicious, or unusual activity detected during log reviews. Capabilities are in place to provide audit reduction and report generation to support on-demand analysis and reporting. | Audit logs from multiple sources are captured and are correlated and reviewed using automated mechanisms in accordance with formal information security policies. The security alert monitoring tools employed by the central facility receives, aggregates, and normalize all forwarded alerts. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-020 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Audit logs from multiple sources are captured and are correlated and reviewed using automated mechanisms in accordance with formal information security policies. Procedures are in place to take follow-up actions for anomalies and indications of inappropriate, suspicious, or unusual activity detected during log reviews. Capabilities are in place to provide audit reduction and report generation to support on-demand analysis and reporting. | The administrator's of Company Systems periodically review logs to identify any anomalous activity and contact Security in a timely manner, upon identification of any anomalous activity. Procedures are in place to take follow-up actions for anomalies and indications of inappropriate, suspicious, or unusual activity detected during log reviews. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-020 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Audit logs are stored securely. Logs for external-facing technologies are written onto a secure, centralized, internal log server or media device. Access to audit log files are provided only on a 'need to know' basis. The audit log files are secured and protected against unauthorized access, alterations, deletion, or modifications. Management of audit functionality is limited to a subset of privileged users. | Audit logs are stored securely. Logs for external-facing technologies are written onto a secure, centralized, internal log server or media device. Access to audit log files are provided only on a 'need to know' basis. The audit log files are secured and protected against unauthorized access, alterations, deletion, or modifications. Management of audit functionality is limited to a subset of privileged users. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-020 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Audit records are retained for an appropriate time period to provide support for subsequent investigations of security incidents and to meet both the organization's security policies and all applicable regulatory requirements. | Audit records are retained for an appropriate time period to provide support for subsequent investigations of security incidents and to meet both the organization's security policies and all applicable regulatory requirements. |
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-030 | Logs are configured to capture all actions taken specifically by individuals with administrative privileges. | Logs are configured to capture all actions taken specifically by individuals with administrative privileges. | Logs are configured to capture all actions taken specifically by individuals with administrative privileges. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Audit Logging | TV-SIEM-AUL-040 | Track and record events and activities performed by users with privileged access. | An audit of privileged accounts is conducted periodically to detect any accounts which have been misused. Any discrepancies are remediated. | An audit of privileged accounts is conducted periodically to detect any accounts which have been misused. Any discrepancies are remediated. |
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Network Monitoring | TV-SIEM-NMO-010 | The network is monitored to detect potential cybersecurity events<br><br>The organization relies on third party sources for the monitoring and detection of potential cybersecurity events | External alerts and advisories are monitored on an ongoing basis and actions are taken as necessary. | External alerts and advisories are monitored on an ongoing basis and actions are taken as necessary. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Network Monitoring | TV-SIEM-NMO-020 | Intrusion and Detection techniques are established and implemented | Communications traffic posing a threat to networks, systems, and internal sub-networks is detected, logged, analyzed and denied using both networks based and host-based intrusion detection and prevention systems (IDS/IPS). Traffic is monitored at the perimeter of the cardholder data environment, and personnel are alerted to suspected compromises. IDS/IPS engines, baselines and signatures are kept up to date. | Intrusion Prevention Systems are configured to provide the following capabilities: Real-time management of security threats, intrusions and policy violations; Provision of solutions for the historical analysis of intrusion detection/prevention logs enabling queries and analysis of logs from a central location; Capturing of the IP addresses of the source and destination of the activity, timestamps, alert names, event data, as well as the names of the related files and objects that were grounds for the alert are mandatory. Capturing of User IDs, |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | MAC addresses, process IDs, event IDs and other appropriate information are also required it this data is available for capture; Mitigation of high-risk threats through the automation of processes and alerts defined by Security; Prevention of unauthorized disclosure of Company information. |

| | | | | | |
|---|---|---|---|---|---|
| Threat Intelligence and Vulnerability Management | Security Information and Event Monitoring - Network Monitoring | TV-SIEM-NMO-020 | Intrusion and Detection techniques are established and implemented | Communications traffic posing a threat to networks, systems, and internal sub-networks is detected, logged, analyzed and denied using both networks based and host-based intrusion detection and prevention systems (IDS/IPS). Traffic is monitored at the perimeter of the cardholder data environment, and personnel are alerted to suspected compromises. IDS/IPS engines, baselines and signatures are kept up to date. | Traffic is monitored at the perimeter of the cardholder data environment, and personnel are alerted to suspected compromises. |

**Lista de controles con procedimientos de prueba y ejemplos de requerimientos de evidencia**

| Control Objective ID | Baseline Test Procedures | Additional Framework Specific Test Procedures | Sample Evidence Requirements |
|---|---|---|---|
| IA-ASMT-INV-010 | 1. Inquire of the control owner and validate the following:<br>- whether the organization documents and maintains a current inventory of all information components (systems (every system that has an Internet protocol (IP) address on the network), applications, databases, media, data centers, hard copy files, etc.)<br>- whether the organization uses an automated asset inventory discovery tool to build a preliminary inventory of systems connected to its public and private networks.<br>- whether equipment acquisitions are automatically updated in the organization's inventory system as new and approved devices are connected to the network. | [PCI]<br><br>1. Inquire with control owner to confirm that the list of devices is updated when devices are added, relocated, decommissioned, etc.<br><br>2. Inspect the list of devices to determine that it includes:<br><br>- Make, model of device<br>- Location of device (for example, the address of the site or facility where the device is located)<br>- Device serial number or other method of unique identification.<br>- Description of function and use.<br><br>3. Inspect that inventory logs are maintained and reviewed at least annually.<br><br>4. Select a sample of devices from the list and inspect devices and device locations to determine that the list is accurate and up to date.<br><br>5. Verify whether an inventory of wireless access points including a | 1. Evidence of current physical inventory of information assets.<br><br>2. Copy of annual asset inventory per data center and information processing facility.<br><br>3. Data Classification and Handling Standard<br><br>4. Records Retention Schedule<br><br>5. Evidence that the organization includes asset owner information in the asset inventory. |

| | | | |
|---|---|---|---|
| | | documented business justification, is maintained. | |

| | | | |
|---|---|---|---|
| IA-ASMT-INV-010 | 1. Obtain and inspect the asset inventory in addition to selecting a sample of assets and comparing those assets to the asset inventory to validate that the organization has each asset is assigned an asset owner 2. Verify the asset owner: - defined the security level for the asset based on the Data Classification and Handling Standard - identified application and Infrastructure platform of the asset - assigned and Infrastructure Owner or Enterprise BU/COE Architect for the asset3. Verify each asset has an Infrastructure owner that: - coordinated security tasks, such as patching - participated in risk assessments - reviewed periodic reports of the status of security controls for the asset - updated Asset Management records to include: - physical location - brand - model number - IP address and/or hostname - serial number - operating system and version | [PCI] 1. Inquire with control owner to confirm that the list of devices is updated when devices are added, relocated, decommissioned, etc. 2. Inspect the list of devices to determine that it includes: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification. - Description of function and use. 3. Inspect that inventory logs are maintained and reviewed at least annually. 4. Select a sample of devices from the list and inspect devices and device locations to determine that the list is accurate and up to date. 5. Verify whether an inventory of wireless access points including a documented business justification, is maintained. | 1. Evidence that the organization includes infrastructure information for each asset owner in the asset inventory. |

| | | | |
|---|---|---|---|
| IA-ASMT-INV-010 | 1. Validate whether cardholder data media inventories is maintained, reviewed, and updated on at least on an annual basis<br><br>2. Verify that removable media:<br>- has documented authorization for all media removed from the organization<br>- has records of all removals from the organization retained as per the Corporate Records Retention Schedule<br>- has procedures developed and maintained by each area for checking out and removing media<br>- is stored in a secure environment<br>- is not shipped to another country without proper controls in place (e.g., encryption) | [PCI]<br><br>1. Inquire with control owner to confirm that the list of devices is updated when devices are added, relocated, decommissioned, etc.<br><br>2. Inspect the list of devices to determine that it includes:<br><br>- Make, model of device<br>- Location of device (for example, the address of the site or facility where the device is located)<br>- Device serial number or other method of unique identification.<br>- Description of function and use.<br><br>3. Inspect that inventory logs are maintained and reviewed at least annually.<br><br>4. Select a sample of devices from the list and inspect devices and device locations to determine that the list is accurate and up to date.<br><br>5. Verify whether an inventory of wireless access points including a documented business justification, is maintained. | [PCI]<br>1. Evidence that assets are tracked from acquisition to decommission.<br><br>2. Evidence that the inventory logs are maintained and reviewed at least annually.<br><br>3. Inventory of wireless access points including a documented business justification. |

| | | | |
|---|---|---|---|
| IA-ASMT-INV-010 | 1. Verify whether or not backup media is reviewed for data integrity on an annual basis in accordance with the backup media procedures | [PCI] 1. Inquire with control owner to confirm that the list of devices is updated when devices are added, relocated, decommissioned, etc. 2. Inspect the list of devices to determine that it includes: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification. - Description of function and use. 3. Inspect that inventory logs are maintained and reviewed at least annually. 4. Select a sample of devices from the list and inspect devices and device locations to determine that the list is accurate and up to date. 5. Verify whether an inventory of wireless access points including a documented business justification, is maintained. | 1. Backup media policies and procedures2. Evidence of annual review of backup media for data integrity and accuracy. |

| | | | |
|---|---|---|---|
| IA-ASMT-INV-010 | 1. Inquiry of the control owner to determine how a current inventory of all software platforms and applications including license keys is documented and maintained. Additionally, inquire of the control owner and obtain evidence to determine whether they periodically conduct an audit to identify all instances of installed licensed software.<br><br>2. Inspect the register of software platforms, applications, and all purchased software licenses and associated license agreements to determine whether current inventory is documented and maintained.<br><br>3. Obtain evidence of the audit performed to identify all instances of installed licensed software, if any discrepancies were identified obtain follow-up evidence. | - | - |

| | | | |
|---|---|---|---|
| IA-DICP-DRT-020 | [PCI Only] 1. Inquire with the control owner to determine if sensitive authentication data or other personally identifiable information is not stored (even if encrypted) after authorization and sensitive authentication data or other personally identifiable information is rendered unrecoverable upon completion of the authorization process. 2. For a sample of system components, examine data sources including but not limited to the following, and verify that the full contents of any track from the magnetic strip on the back of card or equivalent data on chip are not stored after authentication: - Incoming transaction data - All logs (for example, transaction, history, debugging, error) - History files - Trace files - Several database schemas - Database contents. | - | 1. Data source files, for example:- Incoming transaction data- All logs (for example, transaction, history, debugging, error)- History files- Trace files- Several database schemas- Database contents |

| | | | |
|---|---|---|---|
| IA-PPCO-DLK-010 | 1. Inquire of management and obtain evidence to validate whether the organization has capabilities to prevent or monitor data leaks.<br><br>2. Determine if the organization performs activities to analyze potential opportunities for covert channels. If so, determine if testing is performed to identify exploitable channels and the bandwidth associated with those channels.<br><br>3. Inquire with the control owner to determine if the above-mentioned capabilities in test procedure #1 are aligned with legislative, regulatory, or contractual obligations.<br><br>4. Obtain and inspect policies, procedures, and other supporting documentation to validate whether the aforementioned capabilities in test procedure #1 are in place to enable the organization to meet their obligations to customers in accordance with contractual requirements.<br><br>5. Review desktop Data Loss Prevention configuration from a sample of desktops to validate:<br>- DLP is installed<br>- it prevents storage devices (USB, SD, Bluetooth, Thunderbolt, Mobile Phones, etc) from being mounted<br><br>6. Review network Data | [FedRAMP/ NIST 800-53]<br>1. Inquire of management and obtain evidence to validate whether the organization prevents the unauthorized exfiltration of information across managed interfaces.<br><br>2. Inquire of management and obtain evidence to validate whether the organization prevents the covert exfiltration of information (e.g., steganography) | Special Note: Personally identifiable information (""PII"") and Protected Health Information (""PHI"") fall under ""Customer Data"" and is thus subjected to the company's data classification schema and controls.<br><br>1. Data Classification and Protection policies and procedures.<br><br>2. Policies and procedures related to Data Loss Prevention and the handling of customer data.<br><br>3. Evidence of the organizations capabilities to prevent or monitor data leaks.<br><br>4. Evidence that data loss prevention processes and procedures are aligned with legislative, regulatory, or contractual obligations.<br><br>5. Desktop DLP configurations<br><br>6. Network DLP configurations<br><br>7. Performance monitoring evidence |

| | | | |
|---|---|---|---|
| | Loss Prevention configuration to validate:<br>- outbound media and communications are scanned for hidden information<br><br>7. Review performance monitoring evidence to validate system resources are monitored for suspicious behavior | | |

| | | | |
|---|---|---|---|
| ID-IDAM-ADA-010 | 1. Inquire with control owners responsible for assigning access to verify that access to privileged user IDs are: - Assigned only to roles that specifically require such privileged access including authorized administrators with Superuser access to server operating systems; - Restricted to least privileges necessary to perform job responsibilities. 2. Obtain and inspect documentation to determine that privileged access requests are evaluated for appropriateness and follow the principles of least privilege.3. Obtain a population of users with privileged access, including sudoers file (if Unix access is applicable), and select a sample of user IDs and inspect evidence to determine that privileges assigned are: - Necessary for that individual's job function; - Restricted to least privileges necessary to perform job responsibilities;- Approved by the designated authority.4. Validate privileged user access requests are retained in accordance with the Records Retention Schedule. | - | 1. Information Security Policy or Access Provisioning/Deprovisioning Policy2. Population of users with privileged access.3. Evidence for selected samples, indicating the job function(s) or roles requested, access requests along with approval for the access request.4. List of designated approvers.5. Information system configuration settings6. Information system-generated list of privileged user accounts and associated roles7. Information system monitoring records8. Records Retention Schedule |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-010 | 1. Inquire with a sample of control owners to determine if segregation of duties is achieved by organizing personnel into relevant and defined functional groups for processes such as change management, access management, business processes, etc. Validate whether any activity can be performed and approved by the same person.<br><br>2. Obtain and inspect online organization charts to determine if personnel are organized into relevant and defined functional groups.<br><br>3. Inspect employee information within the employee directory for a sample of employees selected from interview procedures to verify responsibilities are segregated from the responsibilities of employees in other defined functional groups.<br><br>4. Inquire of management and inspect relevant documentation to determine if segregation of duties (SOD) is enforced (e.g., development, testing, quality assurance, and production functions, segregation of network operations and computer operations) to prevent unauthorized changes or modification to the organization's assets (e.g., ensure that developers do not have access to migrate changes directly to production). | - | 1. Information Security Policy, SDLC Policy, & Change Management Policy.<br><br>2. Organization charts demonstrating personnel are organized into relevant and defined functional groups.<br><br>3. Population of developers and users with access to an in-scope system with query/parameters used to generate the listing.<br><br>4. System-generated list of users with access to the release management tool.<br><br>5. Access requests for selected samples. |

| | | | |
|---|---|---|---|
| | 5. Obtain the population of users with access to the system, the list of developers, and the parameters associated with each population. Inspect the parameters to validate the completeness and accuracy of the listing.<br><br>6. Compare the list of developers to the system access list to validate whether developers do not have access to the migrate changes to production or otherwise implement changes directly.<br><br>7. Obtain a sample of access requests and validate requests are separate for each ID, and do not request access to multiple environments (e.g., production, development, user acceptance testing, quality assurance, or other environments) | | |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with control owners to determine whether a process is in place to register and provision user access to systems.-Every request for a new or amended ID must be appropriately documented and be validated by an authorized business manager prior to being set up or amended and must be fully integrated with the Company Access Management tool. - Separate access requests must be used to gain access to production, development, user acceptance testing, quality assurance and any additional environment, to ensure separation of duties and protection of credentials is maintained. A separate request must be made and authorized for each User ID.- All privileged user access requests must be recorded and retained in accordance with the Record Retention Schedule2. Verify that access to personal information is restricted by procedures that address: - Authorizing and registering internal personnel and individuals - Identifying and authenticating internal personnel and individuals - Making changes and updating access profiles - Granting system access privileges and permissions - Preventing individuals from accessing other than their own personal or sensitive information 3. Obtain and inspect policies and procedures and verify | - | 1. Policies and procedures related to registering and provisioning user access.2. Evidence that the information system enforces:- access restrictions and supports auditing of the enforcement actions.- [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts]. 3. Evidence of a process for managing emergency access.4. Record retention schedule for validating that privileged access requests are maintained. |

| | | | |
|---|---|---|---|
| | that procedures are in accordance with access requirements as listed in the policies, and cover the management of access to network systems, management networks, and information systems | | |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with the control owners and determine if the organization configures information systems to enforce approved authorizations for users and customers to attain logical access to information and system resources as defined in access control policies and individuals only have access to the information based on their need to access the information as a part of their responsibilities.<br><br>2. Through review of documentation and interview with control owners, confirm that there are a) defined roles for providing authorization for logical access requests and b) processes for authorization of logical access requests<br><br>3. Inspect the automated mechanisms that implement access controls and determine that they enforce only approved authorizations for logical access to information and system resources. | - | 1. Access control policies<br><br>2. Access control automated mechanisms<br><br>3. List of database user privileges<br><br>4. Information system configuration settings<br><br>5. Information system design documentation<br><br>6. Automated mechanisms implementing least privilege<br><br>7. List of authorized approvers for access |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with the control owner(s) and determine that for a select sample of user IDs, management personnel assign privileges based on that individual's job classification and function. 2. Obtain a population of roles and select a sample to test. For the selected sample of roles, inspect the access needs for each role and determine that the necessary access is granted based on system/device/data needs and level of privilege to perform the assigned responsibilities, specifically:- the system components and data resources each role needs to access in order to perform its defined job function- the identification of needed privileges per role in order to perform its defined job function. | [Fed Ramp and ] 1. Inquire with control owners to determine whether the organization: - Identifies and selects the types of roles to support organization's business processes - Assigns account managers for information system accounts; - Establishes conditions for group and role membership; - Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. | 1. Access Control Policy2. Population of roles3. Sample of roles4. Access configurations for the selected sample. |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with the control owner and determine that users with privileged access to security functions or security-relevant information use non-privileged accounts or roles when accessing non-security functions.<br><br>2. Inspect access control policies and determine that the policies define the following:<br>- access assignments for each role including privileged access assignments<br>- access restrictions for privileged users (least privilege)<br>- access assignments based on role, function, and responsibilities<br>- electronic or written access approvals by authorized parties (including specific privileges)<br>- access assignments to all hypervisor management functions or administrative consoles for systems hosting virtualized systems | [Fed Ramp and ]<br><br>1. Inquire with control owners to determine whether the organization:<br>- Identifies and selects the types of roles to support organization's business processes<br>- Assigns account managers for information system accounts;<br>- Establishes conditions for group and role membership;<br>- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account. | 1. Access configurations to show that non-privileged users are prevented from executing privileged functions. |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with the control owners and determine if the organization:- has automated mechanisms in place to support information system account management- establishes an access control system for systems to restrict access unless access is specifically granted.- confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.2. Inspect system settings and vendor documentation and determine that the organization implements access control systems:- that are configured to enforce the specific privileges authorized and assigned to users based on roles and business function.- that have "deny-all" as a default setting.3. Validate all systems on the systems list are configured in the Company Access Management Tool. | - | 1. Access control system privilege configuration2. Vendor Documentation - access control systems3. Information Security Policy4. Systems list (with access controls)5. Company Access Management Tool list of configured systems |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire with management to determine how access to database is restricted.<br><br>2. Inspect database and application configuration settings and determine the following:<br>- that all users are authenticated prior to access<br>- that programmatic methods (i.e., stored procedures) are the only manner by which all database users' access, queries, or conducts actions (i.e., move/copy/delete).<br><br>2. Inspect database access control settings and database application configuration settings and determine that configurations restrict user direct access to, or queries of, databases to database administrators.<br><br>3. Inspect database access control settings, database application configuration settings, and related application IDs to confirm that application IDs can only be used on applications (i.e., not individual users). | - | 1. Database configuration settings.<br><br>2. Application configuration settings.<br><br>3. Database access controls. |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inspect the automated mechanisms that implement least privilege functions and determine whether the authorized access for users allowed is based on user needs to accomplish tasks in accordance with business functions, and that users with privileged accounts use separate non-privileged accounts to access non-security functions.2. Validate that privileged accounts are only used for security functions, and not for standard use (e.g., email, common use items) | - | 1.Evidence that automated mechanisms implement least privilege functions. |

| | | | |
|---|---|---|---|
| ID-IDAM-NIL-020 | 1. Inquire of management and obtain evidence to validate whether the organization only permits the use of shared/group accounts that meet (organization-defined) conditions for establishing shared/group accounts.<br><br>2. Inquire with control owner to determine the following:<br>- Shared/group and generic user IDs are only used in exceptional circumstances where there is a clear business benefit<br>- Additional accountability controls are implemented when shared/group or generic IDs are used<br>- Approval by management for the use of these IDs<br><br>3. Inquire of management to validate whether the information system terminates shared/group account credentials when members leave the group.<br><br>4. Inspect the automated mechanisms that implement account management functions and determine whether the organization:<br>- for shared/group accounts, if the organization only permits the use of shared or group accounts for reasons that meet organization-defined conditions (FedRAMP and HITRUST);<br>- configures the information system to terminate shared/group account credentials when the users leave the group (FedRAMP and | [PCI]<br>1. Inquire with control owner to determine the following:<br>- if group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested<br>- if the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts<br>- if the organization defines the physical and/or logical controls to only allow access to the intended accounts<br><br>2. Examine authentication policies and procedures and determine the following:<br>- that use of group and shared IDs and/or passwords or other authentication methods is explicitly prohibited<br>- that the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts<br>- that the organization defines | 1. Evidence that the organization only permits the use of shared/group accounts that meet (organization-defined) conditions for establishing shared/group accounts.<br><br>2. Evidence that the information system terminates shared/group account credentials when members leave the group.<br><br>3. Evidence of controls in place prohibiting shared use of system IDs.<br><br>4. User List |

| | | | |
|---|---|---|---|
| | HITRUST).<br><br>5. Inspect the user list to verify there are no accounts that are shared by multiple users (not including application accounts to which users cannot authenticate).<br><br>6. Inquire of management and obtain evidence of controls in place that do not allow system IDs (Administrator, SA, root, etc) to be used by multiple people or to affirmatively identify the individual using the account. | the physical and/or logical controls to only allow access to the intended accounts<br><br>3. Obtain a population of system components and select samples to examine user ID lists to verify the following:<br>- Generic user IDs are disabled or removed.<br>- Shared user IDs for system administration activities and other critical functions do not exist.<br>- Shared and generic user IDs are not used to administer any system components. | |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-010 | 1. Inquire with the control owner to determine the following: - if the organization assigns user and administrator accounts unique identifiers in order to access information assets, information systems, databases, and devices;- if the organization tracks unique ID account activity, including creation, modification, deletion of IDs for auditing purposes.2. Inquire with control owner to determine that de-activated or expired user IDs are not granted to other individuals.3. Obtain and inspect the information security policy to validate that the organization requires user accounts to be assigned unique identifiers in order to access information assets.4. Validate user accounts are assigned to a single individual, and do not contain PII.5. Validate that only the individual user is able to use the account-Observe authorization mechanisms (e.g., passwords) are in place on user IDs6. Validate that any account name changes identified have an associated request from the user. | (PCI) 1. Inquire with control owner to determine the following: - if the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts - if the organization defines the physical and/or logical controls to only allow access to the intended accounts 2. Examine authentication policies and procedures and determine the following: - that the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts - that the organization defines the physical and/or logical controls to only allow access to the intended accounts 3. Inspect system configuration settings and determine that the organization implements the controls to only allow access to the intended account | 1. Information Security Policy2. Identity access and authentication procedures3. System configuration settings4. Population of system components5. Sample of system components6. User List with ID and user's name |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-010 | 1. Inquire with the control owner to determine the following:<br>- if the organization assigns user and administrator accounts unique identifiers in order to access information assets, information systems, databases, and devices;<br><br>2. Validate nonuser ID authentication mechanisms (e.g., security tokens, certificates) are assigned to a single individual.<br><br>3. Validate that only the individual user is able to use the authentication mechanism<br>- Observe physical identifiers are controlled to not allow shared use<br>- Validate logical identifiers are implemented correctly to disallow extraction/reuse | (PCI)<br><br>1. Inquire with control owner to determine the following:<br>- if the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts<br>- if the organization defines the physical and/or logical controls to only allow access to the intended accounts<br><br>2. Examine authentication policies and procedures and determine the following:<br>- that the organization manages assigned authentication verification mechanisms of individual accounts to not be shared among multiple accounts<br>- that the organization defines the physical and/or logical controls to only allow access to the intended accounts<br><br>3. Inspect system configuration settings and determine that the organization implements the controls to only | 1. Identifier and user's name for other authentication mechanism's that do not have a User ID (e.g., physical or logical security tokens, smart cards, certificates, etc)<br><br>2. Identity access and authentication procedures<br><br>3. System configuration settings<br><br>4. Population of system components<br><br>5. Sample of system components |

| | | | |
|---|---|---|---|
| | | allow access to the intended account | |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-010 | 1. Validate the are no accounts over 90 days of non-use, and accounts over 30 days of non-use have been suspended/locked.2. Validate all consultant IDs have an expiration date defined | (FedRAMP, NIST 800-53) 1. Inquire with the control owner and determine if the organization requires a registration process to take place for users to receive specific authenticators (Examples: RSA tokens, YubiKey, etc) conducted by specified personnel in person or by a trusted third party prior to the organization registering the authenticator to the user. 2. Inspect policies and procedures outlining identification and authentication and authenticator management and determine the following: - That the organization defines the kinds of authenticators a user can receive; - That the organization defines the authority in charge of maintaining oversight over the authenticator registration process; - That the organization defines the personnel or roles with the ability to authorize registration authority; - That the organization defines if the registration process for authenticators are to be conducted in person or by a trusted | 1. List of users over 90 days of non-use, a separate list of any additional user over 30 days of non-use, and the account status of each (e.g., active, suspended, etc)2. List of consultant IDs with the account expiration date |

| | | | |
|---|---|---|---|
| | | third party. 3. Inquire of management and obtain evidence to validate whether the organization manages information system identifiers (e.g., user ids, MAC addresses, IP addresses) by: - Receiving authorization from organization-defined personnel to assign an individual, group, role, or device identifier; - Selecting an identifier that identifies an individual, group, role, or device; - Assigning the identifier to the intended individual, group, role, or device; - Preventing reuse of identifiers for an (organization-defined) time period; - Disabling the identifier after an (organization-defined) time period of inactivity; - Ensuring that each identifiers is unique. | |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-030 | 1. Inspect policies and procedures addressing personnel security and personnel transfers and determine the following:<br>- that the organization has defined the actions for transfer or reassignment that need to be initiated upon employee transfer or reassignment;<br>- that the organization has defined how long after employee reassignment or transfer actions are required to take place;<br>- that the organization has defined which roles or personnel to notify upon employee reassignment or transfer to other positions internally;<br>- that the organization has defined within what time period it is required to notify specified roles and personnel upon employee reassignment or transfer. .<br><br>2. Inquire with the controls owners and inspect the automated mechanisms to determine that when individuals are reassigned or transferred to other internal positions, the organization reviews and confirms the ongoing operational need for the following:<br>- logical access authorizations to information systems;<br>- physical access authorizations to information system and facilities;<br><br>3. Inquire with the controls owners and inspect the automated mechanisms to determine: | - | 1. Personnel security policies<br><br>2. Personnel transfer procedures<br><br>3. Information Security Technical Standards<br><br>4. Security Account Management Procedures<br><br>5. Database Access Management Procedures<br><br>6. List of users that have changed positions (for sampling)<br><br>7. Access requests for selected samples of users |

| | | | |
|---|---|---|---|
| | - that the organization initiates the transfer or reassignment actions immediately upon an employee transfer or reassignment;<br>- that the organization modifies the corresponding access authorizations as needed against changes in operational needs in result of employee transfer or reassignment;<br>- that the organization notifies the defined personnel or roles within five days of an employee reassignment or transfer to another position.<br><br>4. Review a sample of users that have changed positions to ensure previous access has been revoked. | | |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-030 | 1. Inquire with control owners to determine whether the organization revokes user account access in response to terminations and that all physical authentication methods (smart cards, tokens, etc.) are returned or deactivated. Validate that access to critical systems and applications must be removed within twenty-four (24) hours of the termination date.2. Obtain and inspect policies and procedures to determine that requirements are clearly stated for the removal of logical access as a result of terminations.3. Obtain the population of current users, and a population of terminated users for the time period under review for both local and remote access. 4. Select a sample from the obtained population of current and terminated users, inspect ticket evidence and determine that access is revoked, and IDs are deactivated or removed within the timeframe specified by the access control procedures for the users selected (by end of day) by comparing the current to terminated employees listing. twenty-four (24) hours of the termination date.5. Inquire with the control owner and inspect if the organization, upon termination of individual employment:- Conducts exit interviews that include a discussion of [Assignment: organization-defined information | - | 1. Information Security Policy or Access Provisioning/Deprovisioning Policy.2. Current population of all active users for in scope production network, database servers, application servers, application users, database users (both local and remote access).3. Population of terminated users and evidence that access is revoked, and IDs are deactivated or removed within the timeframe specified by the access control procedures. |

| | | | |
|---|---|---|---|
| | security topics];- Retains access to organizational information and information systems formerly controlled by terminated individual; - Notifies organization-defined personnel or roles within organization-defined time period. | | |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-030 | 1. Inquire with control owners to determine whether the organization revokes access for temporary/ emergency accounts after a defined period of time.<br><br>2. Inquire with control owners to determine whether the organization identifies and revokes access for inactive accounts after a defined period of time.<br><br>3. Inquire with control owners to determine whether the organization identifies and revokes access for anonymous accounts after a defined period of time.<br><br>4. Obtain a population of user access reviews noting whether temporary/emergency, inactive, and/or anonymous accounts were identified. Treat each different account type as a separate population and select a sample from each to validate whether appropriate action was taken as a result of the review. | - | 1. Information Security Policy or Access Provisioning/Deprovisioning Policy.<br><br>2. Current population of all active users for in scope production network, database servers, application servers, application users, database users (both local and remote access).<br><br>3. Population of terminated users and evidence that access is revoked, and IDs are deactivated or removed within the timeframe specified by the access control procedures.<br><br>4. Population of user access reviews to validate whether temporary/emergency, inactive, and/or anonymous accounts exist. |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-030 | 1. Inquire with the control owners to determine if the organization has automated mechanisms in place to notify and alert specified personnel when the organization terminates an employee or when the employee's' role changes.2. Inspect personnel security policies, procedures addressing termination, and information system configuration settings to determine that the organization defines the roles and individuals required to receive notifications upon termination of an employee when the employee's' role changes.3. Observe automated mechanism processes relating to personnel termination and determine that the organization configures mechanisms to send notification alerts to defined personnel upon termination of an employee when the employee's' role changes. | [FedRAMP and ] 1. Inquire with the control owner and determine whether the organization notifies account managers: - When accounts are no longer required; - When users are terminated or transferred; and - When individual information system usage or need-to-know changes. | 1. Personnel security policy2. Personnel termination procedures3. Current Employee Transfer Process |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-050 | 1. Inquire with the control owners and determine whether accounts were reviewed by management on at least a quarterly basis and accounts identified as no longer appropriate were investigated and resolved.<br><br>2. Obtain and inspect policies and procedures to determine that user access to data (inclusive of sensitive data such as PII, PHI) is evaluated for appropriateness (i.e., no terminated users have access, and roles/privileges are appropriately assigned).<br><br>3. Obtain the population of active user accounts for the in-scope systems.<br><br>4. Obtain and inspect evidence indicating that the user accounts were reviewed and validated by the designated reviewer/approver.<br><br>5. If changes were required as a result of the review, obtain evidence and inspect that the requested changes to the user access list were completed.<br><br>6. Inspect the transfer review ticket details for a sample of months and determine whether the review was completed, and any inappropriate users were investigated and resolved. | - | 1. Information Security Technical Standards<br><br>2. Population of active user accounts for the in-scope system<br><br>3. Evidence of user account review by a designated authority<br><br>4. Evidence of any changes to user accounts based on the review<br><br>5. List of designated approvers<br><br>6. Transfer review ticket details<br><br>7. Population and sample of logical accounts.<br><br>8. Population and sample of access logs.<br><br>9. Policies and procedures related to access authorizations. |

| | | | |
|---|---|---|---|
| ID-UAPD-NIL-050 | 1. Inquire with the control owners and determine whether privileged users are reviewed at least every 90 days.2. Obtain the population of active user accounts for the in-scope systems.3. Obtain and inspect evidence indicating that the user accounts were reviewed and validated by the designated reviewer/approver.4. If changes were required as a result of the review, obtain evidence and inspect that the requested changes to the user access list were completed.5. Inspect the transfer review ticket details for a sample of months and determine whether the review was completed, and any inappropriate users were investigated and resolved. | - | 1. Population of active user accounts for the in-scope system2. Evidence of user account review by a designated authority3. Evidence of any changes to user accounts based on the review4. List of designated approvers5. Transfer review ticket details |
| ID-UAPD-NIL-050 | 1. Inquire of control owners and inspect/observe evidence to validate that an up-to-date record of users or profiles of users with authorized access to the information system is maintained. | - | 1. Sample of user access listings. |

| | | | |
|---|---|---|---|
| RC-COMP-NIL-010 | 1. Inquire with the control owner to determine if documented information security policies and procedures are available to personnel on accessible resources (the organization's internal network, shared drive, etc.), and include requirements for identifying and maintaining applicable legislative, statutory, regulatory, contractual obligations and intellectual property rights to the organization. | - | 1. Security compliance program documentation2. Information security compliance assessment (including templates and completed assessments) |

| | | | |
|---|---|---|---|
| RC-COMP-NIL-010 | 1. Obtain and inspect policies and procedures to corroborate that there are requirements for identifying and maintaining applicable legislative, statutory, regulatory, contractual obligations and intellectual property rights to the organization. Confirm that roles and responsibilities have been defined to meet the requirements. | - | 1. Evidence to demonstrate review of procedures are maintained according to changes in legislation, regulatory, or contractual compliance. |

| | | | |
|---|---|---|---|
| RC-PSGM-AUP-010 | 1. Inquire with the control owners and validate whether the organization:- configures the Company information system to display the defined system use notification message/banner to users before granting access (relating to privacy/security notices consistent with laws and regulations), stating that system is the property of Company, access to the system is for Authorized Use Only, that system usage may be monitored, recorded and is auditable (and that user usage indicates consent); - configures the information system to retain notification messages/banners relating to privacy and conditions of Company information system access until users explicitly acknowledge the conditions defined and go forward with log in procedures;- configures publicly accessible systems to display defined conditions prior to granting further access;- configures publicly accessible systems to display references (if any) to the monitoring, recording, or auditing, consistent with privacy practices for cases where systems typically prohibit specific activities;- login banner is displayed using the largest banner possible.2. Inspect access control policies, privacy policies and procedures, and system use procedures and validate whether the organization: - defines that a system usage notification message/banner must be | - | 1. Information Security Policies and Procedures.2. Access Control Policies and Procedures.3. System notification message/banner configuration. |

| | | | |
|---|---|---|---|
| | displayed by the Company information system prior to granting user access;- defines the conditions of system usage and that the conditions are displayed by the information system prior to granting user access; - configures publicly accessible systems to include a description of the authorized uses of the system.3. Inspect system configuration to validate:- the system usage notification message/banner displayed by the Company information system defines conditions of system usage;- the scope of the systems displaying the notification message/banner includes all systems which provide an entry point to the Company network and internal applications. | | |

| | | | |
|---|---|---|---|
| RC-RIAT-NIL-010 | 2. Obtain and examine the risk assessment documentation to determine whether the following were identified:<br>-internal and external threats;<br>-internal and external vulnerabilities;<br>-identification & prioritization of critical assets;<br>-updates to the risk assessment or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.<br><br>3. Obtain and review risk assessment documentation to determine whether the risk assessment process is performed at least annually, and risk owners are determined and assigned formally for each tracking and mitigating each risk. | - | 1. Risk assessment documentation (including the completed assessment)<br><br>2. List of Identified critical assets. |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-010 | 1. Obtain project management methodology or process documentation from control owner.2. Verify that the documentation contains requirements for: - creation of a formal integrated plan to guide program and project execution and control throughout the life of the program and project- maintenance and approval of the plan by management3. Obtain a list of programs/projects from the past 2 years. Select an appropriate sample from the list and inspect the program/project plans for each to verify that it includes the following:- program/project scope- deliverables- milestones- deliverable acceptance criteria- alignment of the above to the strategic objectives of the program/project | - | 1. Project management methodology or process documentation2. Population: System extract or register of projects3. For a sample of program/ projects selected, program/project plan documents |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-010 | 1. Obtain project management methodology or process documentation from control owner.<br><br>2. Verify that the documentation specifies formal project and program management approach that aligns with Company's culture and operating environment. Verify that there are standards in place to enable project governance and achievement of desired outcomes. | - | 1. Project management methodology or process documentation including any standards in place |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-010 | 1. Obtain project management methodology or process documentation from control owner.2. Verify that the documentation specifies the development of a business case for a program or project which outlines the following:- expected benefits with a benefits realization and measurement plan- feasibility analysis- the full scope of initiatives required- the risk involved and the impact- approval by program sponsor- commitment and participation from the sponsors and impacted stakeholders3. Obtain a list of programs/projects from the past 2 years. Select an appropriate sample from the list and inspect the program/project business case for each. Verify if it meets the requirements stated in the project management methodology documentation. | - | 1. Project management methodology or process documentation2. Population: System extract or register of projects3. For a sample of program/ projects selected, business case documents |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-020 | 1. Obtain project management methodology or process documentation from control owner.<br><br>2. Verify that the documentation specifies the approach for determining investment mix (project/program/portfolio) based on:<br>- alignment with strategy<br>- financial measures such as cost, expected return of investment over the full economic life cycle<br>- degree of risk<br>- type of benefit for the programs in the portfolio<br><br>3. Verify if the documentation also specifies a formal process to evaluate and prioritize program business cases, and decide on investment proposals, including the allocation of funds and initiation of programs.<br><br>4. Obtain a list of programs/projects from the past 2 years. Select an appropriate sample from the list and obtain program/project business cases, investment proposals, documents including the allocation of funds and initiation of programs. Inspect the documents to verify that the requirements as part of the project management methodology documentation are met. | - | 1. Project management methodology or process documentation<br><br>2. Population: System extract or register of projects<br><br>3. For a sample of program/ projects selected, business case documents, investment proposals, documents including the allocation of funds and initiation of programs |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-030 | 1. Obtain a list of programs/projects from the past 2 years. Select an appropriate sample from the list and obtain project progress or status reports. Verify if the project progress reports highlight the following:- project scope- project progress- project schedule- quality & benefits realization- costs and risks- stage-gate reviews by stakeholders2. Discuss with control owner and inquire if there is a periodic review of such reports with stakeholders including project steering committee and sponsors throughout the lifecycle of the project. Also, inquire if stakeholder expectations are considered and addressed in this process. | - | 1. Project management methodology or process documentation2. Population: System extract or register of projects3. For a sample of program/ projects selected, project progress/status reports |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-040 | 1. Obtain a copy of the organizations process and/or plans for allocating resources and verify it takes the following factors into consideration:<br>– people, skills, experience and competence;<br>– resources needed for each step of the risk management process;<br>– the organization's risk processes, methods and tools to be used for managing risk;<br>– documented processes and procedures;<br>– information and knowledge management systems;<br>– training programmers. | - | - |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-040 | 1. Inquire with the control owner and confirm if Company has processes in place to identify additional expertise needed to improve information security defenses. | - | 1. Documentation for the most recent annual budget planning exercise.2. Evidence that the organization has processes in place to identify additional expertise needed to improve information security defenses.3. Provide a strategic roadmap for technology implementations. |

| | | | |
|---|---|---|---|
| SG-FIPM-PPM-060 | 1. Inquire with senior leadership and control owners how security is embedded in the organizational wide project management process/lifecycle.<br><br>2. Obtain organizational wide project methodology or process documentation and validate that it considers security risks as part of the process.<br><br>3. Obtain a list of current projects from functional units outside of Security and inspect a selected sample of project management considerations to determine whether or not security is addressed and incorporated into the project management guidelines and processes. | - | 1. Project management methodology or process documentation.<br><br>2. Population: System extract or register of projects<br><br>3. For a sample of projects selected, evidence of risk assessment activities being performed as part of the project management lifecycle.<br><br>4. ISMS manual - Description of the security requirements department managers are to include in projects. |

| | | | |
|---|---|---|---|
| SG-PERS-RRS-010 | 1. Inquire with the control owner to determine whether or non-employees are required to sign a confidentiality agreement prior to being granted access to sensitive information. Additionally, inquire of the control owners if the organization enforces to re-sign access agreements to maintain access to organizational information systems when access agreements have been updated. 2. Inspect Company Third Party Security Policies to determine if requirements are defined for providing non-employees with the organization's data privacy and security policies prior to gaining access to the organization's systems or resources.3. Obtain a population of third-party non-employees who have access to Company's systems or resources.4. For a selected sample. inspect evidence validating that all requirements defined in the Company Third Party Security Policies were documented and approved prior to provisioning access to the Company's systems or resources. | - | 1. A defined population of non-employees for a specified time period and/or area.2. For the selected sample provide the signed Confidentiality Agreements or other third-party agreements detailing protection requirements for sensitive information.3. Policies regarding third party security |

| | | | |
|---|---|---|---|
| SG-PERS-RRS-020 | 1. Obtain the Company enterprise IT organizational chart and supporting documentation.<br><br>2. Review the document and verify it contains overall IT organization's personnel roles and responsibilities along with relevant personnel's authority and accountability.<br><br>3. Discuss with control owner and verify if the roles & responsibilities for IT personnel are defined based on overall business needs and IT objectives. | - | 1. Enterprise IT organizational chart and supporting documentation. |

| | | | |
|---|---|---|---|
| SG-PERS-RRS-030 | 1. Inquire with the control owners to determine if employees acknowledge that they have read and understood their responsibilities outlined in the Code of Conduct Handbook. 2. Inquire with the control owners to determine what agreements a new user must sign. 3. Inspect a copy of each agreement to determine whether new personnel must agree to comply with (at minimum): - an employee handbook; - confidentiality agreement; - code of conduct; - security and corporate policy acknowledgment form. 4. Inquire with control owners to determine how employees obtain the Code of Conduct handbook and how the employees acknowledge their responsibilities. 5. Obtain the organization's Information Security Policy for Governance Roles and inspect that the policy requires employees to acknowledge that they have read and understand the information security policy. 6. Obtain a population of new employees (excluding employees obtained via a merger or acquisition) from the Company HR system. 7. Inspect the employee personnel file for a sample of new employees (full time, part time, and interns) selected from the HR system (excluding employees obtained via a merger or acquisition) and determine if the employee has reviewed and signed, within 30 days of their hire | - | 1. Information Security Policy for Governance Roles.2. Evidence of how new and current employees receive the Code of Conduct handbook.3. Evidence of acknowledgement from the selected sample of employees.4. Annual security awareness training records 5. ISMS manual 6. Employee Handbook7. Code of Conduct8. Information Security Policies9. Background check policy10. Evidence all new employees, including contractors, hired during the current testing period who have access to the critical Infrastructure rooms and organization area have acknowledged each of the following documents:- Employee Handbooks- Confidentiality Agreements- Code of Conduct- Security and Corporate Policy Acknowledgement forms. |

| | | | |
|---|---|---|---|
| | date, the Code of Conduct agreement and Employee Handbook which includes the Confidentiality agreement and Security and Corporate Policy Acknowledgement Form. | | |

| | | | |
|---|---|---|---|
| SG-PM-NIL-060 | 1. Obtain project management methodology or process documentation from control owner.<br><br>2. Verify that the documentation specifies the requirement<br>- of active risk management and quality assurance throughout the project lifecycle<br>- of recording risks faced by the project<br>- of eliminating or minimizing risks through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change.<br><br>3. Obtain a list of projects completed in the past 2 years. Select an appropriate sample from the list and obtain project risk register for each project in the sample. Verify if the risk register outlines project specific risks, impacts and ways of risk treatment agreed upon by stakeholders. | - | 1. Project management methodology or process documentation<br><br>2. Population: System extract or register of projects<br><br>3. For a sample of program/ projects selected, project risk register |

| | | | |
|---|---|---|---|
| SG-PRMT-NIL-020 | 1. Obtain project management methodology or process documentation from control owner.2. Verify that the documentation specifies:- the requirement of post implementation reviews to ascertain whether the project delivered the planned results and benefits- identification of any outstanding activities3. Obtain a list of projects completed in the past 2 years. Select an appropriate sample from the list and obtain post implementation review reports. Verify if the reports meet the requirements stated in the project management methodology or process documentation. | - | 1. Project management methodology or process documentation2. Population: System extract or register of projects3. For a sample of program/ projects selected, post-implementation review reports |

| | | | |
|---|---|---|---|
| SG-PRMT-QMT-010 | 1. Obtain quality management process documentation.<br><br>2. Verify if the document specifies the requirement of:<br>- establishment and maintenance of a quality management system (QMS) which provides a formal and continuous approach for quality management<br>- an overall quality plan being maintained and regularly communicated to promote continuous improvement<br>- analyzing QMS data for effectiveness and opportunities for improvement, including corrective and preventive actions to eliminate the cause of identified and potential nonconformities<br><br>3. Obtain a list of projects completed in the past 2 years. Select an appropriate sample from the list and obtain quality plans for each project in the sample. Verify if the plan meets the requirements stated in the quality management process documentation. | - | 1. Quality management process documentation<br><br>2. Population: System extract or register of projects<br><br>3. For a sample of program/ projects selected, quality plans for each |

| | | | |
|---|---|---|---|
| SG-PRMT-QMT-010 | 1. Obtain quality management process documentation.2. Verify if the document (standards, practices, and procedures) specifies incorporating relevant quality management practices into the definition, monitoring, reporting and ongoing management of solutions development and service offerings. | - | 1. Quality management process documentation (standards, practices, and procedures) |

| | | | |
|---|---|---|---|
| SG-STRT-OSD-050 | 1. Inquire with the control owners to verify if mechanisms are in place to incorporate risk tolerance while defining business processes.<br><br>2. Inquire with the control owners to determine if information protection needs for defined mission/business processes are developed based on risk tolerance and if business processes are revised until the desired risk tolerance levels are achieved.<br><br>3. Inspect formalized Risk Tolerance and Management plans and procedures to determine if the defined processes align with inquiry understanding and clearly state the key stakeholders involved in this process.<br><br>4. Obtain evidence validating a defined mission/business process being continually developed based on risk tolerance and noting when the desired risk tolerance level was achieved. | - | 1. Risk Management scoring criteria<br><br>2. Evidence of risk tolerance mechanisms implemented into operational business that follow the risk scoring categories<br><br>3. Evidence of risk tolerance mechanism review and updates at least annually |

| | | | |
|---|---|---|---|
| SG-STRT-OSD-050 | 1. Obtain an organization-wide risk management strategy documentation and examine to determine whether the following were outlined: -acceptable risk assessment methodologies; -risk mitigation strategies; -a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance; -and an approach for monitoring risk over time. 2. Examine when the documentation was last reviewed, or the last update was performed to determine whether the risk strategies are kept up to date. | - | 1. Obtain an organization-wide risk management strategy documentation. |

| | | | |
|---|---|---|---|
| SG-STRT-OSD-050 | 1. Inquire with the control owners and relevant stakeholders to determine if a process for determining organizational risk tolerance is clearly expressed and defined.<br><br>2. Obtain relevant risk tolerance policies and procedures to determine if a clear procedure and strategy is expressed for determining organizational risk tolerance and that key stakeholder roles and responsibilities are outlined.<br><br>3. Obtain relevant documentation demonstrating the organizational risk tolerance and determine whether the organization has incorporated its understanding of its role in determining risk tolerance. Inspect the documentation to determine if the organization evaluates the external environment, internal environment, its role in the critical Infrastructure, business objectives, and sector specific risks, while determining risk tolerance. | - | 1. Supporting documentation for building out risk tolerance |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-010 | 1. Inquire with the control owners and inspect configuration standards to validate whether or not the organization performs logging related to both unauthorized actions and access. The following items are examples of logging mechanisms that should be in place:Action-related logging events:- all changes, additions, or deletions to any account with root or administrative privileges;- initialization, stopping, or pausing of audit logs; - creation and deletion of system level objects;- creation, modification, enabling, disabling, and removing of accounts;- initialization and the stopping or pausing of audit logs.- system security configuration changes-activation and de-activation of protection systems (e.g., A/V and IDS)-management activities, system and application startup/shutdown/errors, file changes, and security policy changes.- other organization defined abnormal action-related events.Access-related logging events:- successful and unsuccessful account logon events;- all individual access to cardholder data;- access to all audit trails;- elevation of privileges.- other organization defined abnormal access-related events.2. Inquire of the control owners and, for a sample selection of logs, inspect evidence to validate whether the organization:-Captures the following | - | 1. System generated list of production servers and network devices as of present day with source, filter / query details, etc.2. Log configurations for a sample of production servers and network devices. 3. Evidence that the organization performs logging related to both unauthorized actions and access. 4. Policies and procedures related to access control, account management, audit and accountability, storage engineering, and audit record content. 5. Evidence that the organization configures information systems to allocate storage space for the retention of audit records.[Fed Ramp]1. Evidence to validate whether the information system off-loads audit records on an organization-defined frequency to a different system.[FEDRAMP HIGH]1. Evidence that the organization can extend or limit auditing as necessary to meet organizational requirements. |

| | | | |
|---|---|---|---|
| | information in log entries: - Type of event - User Identification - Source and Destination IP address - Port and Protocol used - Terminal address and location - Date and time stamp - Activity type attempted (login, login help, update, delete, insert, create, file upload/download, etc.) - Activity success/fail - Before and after values - Identity or name of affected data, system component, or resource.- monitors information system accounts for abnormal usage and activity;- reports abnormal usage and activity on information system accounts to specified personnel;- configures information systems to generate audit records that contain information on what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of individuals associated with the event;- continuously writes logs from production servers, network devices, databases and storage management hosts to system logs and forwards them to the logging and alerting system in real-time in order to provide backup media for records other than the audited system;- configures the information system to provide the capability to generate audit records for defined auditable events for specified information system components;- configures the information | | |

| | | | |
|---|---|---|---|
| | system to allow specified personnel to select which auditable events should be audited by specific system components;- configures the information system to provide capabilities for specified individuals to change the performed audits on information system components based on defined selectable event criteria within specified thresholds.3. Inspect policies and procedures around access control, account management, audit and accountability, storage engineering, and audit record content and validate whether or not the organization: - defines abnormal information system account usage and the personnel to be notified upon the identification of abnormal system usage;- configures the information system to generate audit records that contain information on what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of individuals associated with the event;- defines the additional detailed information required to be included in audit records that the information system generates;- defines the information system components that provide audit record generating capabilities for defined auditable events;- defines the personnel whom are allowed to select which auditable events are to be audited by specified | | |

| | | | |
|---|---|---|---|
| | information system components, and change the auditing performed on specified information system components;- defines the information system components that auditing is performed on;- defines the time thresholds that must be met for specified individuals to change the audit functions performed on information system components;- defines the event criteria that can be selected by specified individuals or roles to support the capabilities of changing audit functions performed on information system components;- continuously writes logs from production servers, network devices, databases and storage management hosts to system logs and forwards them to the logging and alerting system in real-time in order to provide backup media for records other than the audited system4. Inspect audit record storage capacity related to information system configuration settings and determine that the organization configures information systems to allocate storage space for the retention of audit records and that it is sufficient in accordance to defined requirements. | | |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-010 | 1. Inquire with the control owner and verify whether the organization reviews the list of audited events for different information systems and updates/enhances the list of audited events.<br><br>2. Inspect system capabilities and validate whether or not automated review and alerting processes are in place.<br><br>3. Inquire with the control owner and inspect evidence to validate whether the process of determining the events that are logged includes participation from multiple stakeholders across the enterprise and that the administrators contact Security prior to taking any actions for the system if known or suspected anomalous activity is identified. | - | 1. Evidence that automated review and alerting processes are in place.<br><br>2. Evidence depicting the process of determining which events are logged.<br><br>3. Evidence of alert classification per criticality and daily alert review. |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-020 | 1. Inquire with the control owners and inspect evidence to validate whether the organization: - Captures audit logs or other alerts from all Company systems for events such as unauthorized activity or anomalous activity.- Forwards alerts and logs to a designated monitoring facility unless a defined business exception exists.2. Inquire of management and inspect evidence to validate whether the organization: - has authorized personnel review information correlated from security events;- logs of system components that store, process or transmit cardholder data; - logs of critical system components;- logs of servers and system components performing security functions (i.e. firewalls, IDS/IPS), authentication servers, etc);- performs reviews on a frequency in accordance with policies and guidelines;- has personnel perform follow-ups to exceptions and anomalies identified during the log-review process.3. Obtain and inspect audit log settings for each hardware device and the software installed on it and determine the following: - that the logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction; - that systems are configured to record logs in a standardized | [FedRAMP] 1. Inquire of management to validate whether the organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support response to suspicious activities. 2. Inquire of management and inspect evidence to validate whether the organization: - reports findings to organization-defined personnel; - provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; - does not alter the original content or time ordering of audit records; - provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records. | 1. Information Security policies and procedures.2. Evidence that authorized personnel review information correlated from security events.3. Evidence that logs are reviewed on a frequency in accordance with policy. 4. Evidence showing that exceptions identified from the log reviews are followed up and/or resolved. 5. Evidence of findings reported to organization-defined personnel.6. Evidence related to the collection, storage, review, and reporting of logs. |

| | | | |
|---|---|---|---|
| | format such as syslog entries or those outlined by the Common Event Expression initiative;- that if systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format. | | |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-020 | 1. Discuss with each system administrator to understand if the administrator performs periodic review of the audit logs and if there is a documented formal process for review of audit logs.<br><br>2. For a sample of systems, conduct discussions with the system administrators to determine if the audit log review results have been documented.<br><br>3. Inquire of management and inspect evidence to validate whether the organization:<br>- has authorized personnel review information correlated from security events;<br>- performs reviews on a frequency in accordance with policies and guidelines;<br>- has personnel perform follow-ups to exceptions and anomalies identified during the log-review process. | [FedRAMP]<br>1. Inquire of management to validate whether the organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support response to suspicious activities.<br><br>2. Inquire of management and inspect evidence to validate whether the organization:<br>- reports findings to organization-defined personnel;<br>- provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents;<br>- does not alter the original content or time ordering of audit records;<br>- provides the capability to process audit records for events of interest based on organization-defined audit fields within audit records. | 1. Policies and procedures related to log review.<br><br>2. Information Security policies and procedures.<br><br>3. Evidence that logs are reviewed on a frequency in accordance with policy.<br><br>4. Evidence showing that exceptions identified from the log reviews are followed up and/or resolved.<br><br>5. Evidence of findings reported to organization-defined personnel.<br><br>6. Evidence related to the collection, storage, review, and reporting of logs. |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-020 | 1. Inquire with the control owner to validate whether the organization: - Uses logical access controls to restrict access to in-scope production system logs and protect audit information from unauthorized modification and deletion via access control mechanisms, physical segregation, and/or network segregation by all users and customers;- Requires that only the individuals with the defined business-related roles and needs can access audit trail files;- Writes logs for external-facing technology (wireless, firewalls, DNS) on a secure, centralized, internal log server;- Configures audit records to read-only for customers, and customers are not able to delete or disable audit logs;- Assigns responsibility to customers for audit record retention requirements; - Authorizes only pre-defined privileged users access to manage the audit functionality.2. Inspect the administrative configurations for the log aggregation tools to determine whether users are unable to delete or modify log records.3. Inspect the access logs to all audit trails and determine that all user access is logged, and that only users with "view setup and configuration" and "manage users" permissions are allowed to view login history.4. Inspect information system settings, files actively monitored, and results from | - | 1. Application configurations demonstrating that deleting logs is not possible.2. Sudoer list to determine who has server level access to delete logs.3. Access logs to all audit trails 4. Information system configurations.5. Audit files actively monitored6. Centralized online storage of monitored alerts7. Results from monitoring activities 8. Cryptographic mechanisms 8. Automated access mechanisms 10. Audit and accountability policies and procedures11. Exceptions containing documentation of consultation with Security Engineering Solutions and the Cyber Threat Center12. CSIRT Monitoring, Auditing, and Logging Procedure13. System configurations14. System logging permissions[FedRAMP]1. Population of audit records, from which a sample will be selected. |

| | | | |
|---|---|---|---|
| | monitoring activities and validate whether the organization protects the audit tools from unauthorized access, modification, and deletion.5. Inspect policies and procedures addressing audit and accountability and validate whether the organization: - protects audit information and audit tools from access, modification and deletion;- uses cryptographic mechanisms to protect integrity of audit information and audit tools;- log owners ensure their logs are being produced as expected and are not tampered with;- only authorizes access to a defined set of privileged users for audit management functionalities.6. Inspect system configurations and permissions and determine that the organization secures audit trails in the following ways:- configuring the system to authorize view-access for audit trail files by job role;- protecting audit trail files from unauthorized changes and edits through the use of access control mechanisms, physical segregation, separation of duties, and network segregation;- ensuring integrity of log entries by validating system administrators and log owners cannot change or delete log entries;- backing up audit trail files to a centralized log server or difficult-to-alter media;- writing external-facing technology logs onto a secure and centralized | | |

| | | | |
|---|---|---|---|
| | internal server or media.7. For a sample selection of logs, inspect evidence validating:-a central accessible location online is utilized to store monitored alerts;-alerts stored offline are retained in accordance with the Corporate Records Retention Schedule;-any identified exceptions contain documentation of consultation with Security Engineering Solutions and the Cyber Threat Center. | | |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-020 | 1. Inquire with the control owner to verify that the organization retains logs for in-scope production systems in accordance with retention requirements.<br><br>2. Inspect security policies and procedures to verify that they define and outline the organization's audit log retention policies and procedures for audit log retention and availability.<br><br>3. Inspect configurations for the in-scope systems to determine it is configured to retain logs in accordance with retention requirements.<br><br>4. Observe a user querying the log aggregation tool and determine through inspection of the log records that logs for in-scope production systems are available in accordance with retention requirements. (PCI - last three months' logs immediately available for analysis, HITRUST - 1 year).<br><br>5. Obtain a population of audit records for specific devices from the audit log aggregation tool.<br><br>6. Select a sample of audit records for specific devices dating back a full year.<br><br>7. Inspect the selected sample of audit records and determine whether the records are available and viewable within the system | [FedRAMP]<br>1. Inspect disk space allocation in the audit log aggregation tool and determine that the organization maintains sufficient storage space to allocate to the retention of audit records as defined in policies and procedures.<br><br>2. Verify that the information system off-loads audit records onto a different system or media than the system being audited. | 1. Population of audit records, from which a sample will be selected.<br><br>2. Information security policies and procedures.<br><br>3. Configurations for the in-scope systems. |

| | | | |
|---|---|---|---|
| | and retained according to defined requirements. | | |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-030 | 1. Inquire with control owners that logs are configured to capture all actions taken specifically by individuals with root or administrative privileges.2. Inspect log configuration settings to determine that all administrative actions will be logged and monitored for their respective environments.3. Obtain a population of production servers selected from the vulnerability scanning tool and asset inventory, select a sample and inspect the selected sample to determine that they are configured to log escalation of privilege events. | - | 1. System generated list of production servers, network devices, as of present day with the source, filter/query details, etc., to evidence completeness of the population.2. Configuration for logging for a sample of servers. |

| | | | |
|---|---|---|---|
| TV-SIEM-AUL-040 | 1. Inquire with the control owners to determine if an audit of privileged accounts is conducted periodically to detect any accounts which have been misused and whether discrepancies are investigated for the following:<br>- Production Servers/Storage Arrays;<br>- Production Network Devices;<br>- Production Databases;<br>- Application Event Log Files.<br><br>2. Inspect a sample of audit records for systems that directly process, store, or transmit sensitive data and determine whether the organization monitors administrative setup activities logged, such as configuring items and settings, performed by explicitly authorized personnel. Validate that the level of detail includes the success/failure of the event, the time the event occurred, the account involved, and the process involved. | - | 1. Provide a population of audit records, from which a sample will be selected.<br><br>2. Audit records evidencing monitoring of privileged access activities for systems that directly process, store, or transmit sensitive data. |

| | | | |
|---|---|---|---|
| TV-SIEM-NMO-010 | 1. Inquire with control owners to determine if external alerts and advisories are monitored on an ongoing basis, and actions are taken as necessary.2. Observe that staff involved in detection and response activities are subscribed to receive email notifications and updates regarding security alerts, advisories and directives that have or could have an impact on customer data.3. Inspect the organization's website portal and determine if it contains details regarding security alerts, advisories and directives that had or could have an impact on customer data. | - | 1. Policies and procedures related to external alert and advisory monitoring.2. Evidence that staff involved in detection and response activities are subscribed to receive email notifications and updates regarding security alerts, advisories and directives.3. Evidence of incident and threat reporting mechanisms.[Cloud]1. Evidence of external alerts and advisories received from US-CERT. |

| | | | |
|---|---|---|---|
| TV-SIEM-NMO-020 | 1. Inquire of the control owners to determine the following:<br>- if inbound and outbound communications and network traffic to the production network and information systems is monitored using host based and network based IDS/IPS devices that generate alerts in the event of compromise;<br>- if the organization collects and analyzes DMZ and other critical network segment flows to detect anomalous activity;<br>- if the organization monitors traffic leaving the organization to detect unauthorized use of encryption;<br>- if the organization monitors, restricts, and reviews traffic between trusted and untrusted connections;<br>- if Security is responsible for the configuration of detection and prevention rules.<br>- if the host based or network based intrusion detection systems have the capability to identify and prevent the use of prohibited functions, ports, protocols, and services.<br><br>2. Select a sample of IDS/IPS alert incident tickets from the IDS/IPS event repository and inspect the ticket details to determine that the incident was resolved and/or is actively worked to resolution. Validate IDS/IPS alerts are centrally monitored. | [PCI]<br>1. Inspect system configurations and network diagrams to determine that IDS/IPS are in place to monitor traffic at the perimeter and critical points of the cardholder data environment<br><br>2. Inspect system configurations to determine that the IDS is set to alert personnel of events.<br><br>3. Inspect IDS/IPS configurations and vendor documentation to determine that the IDS/IPS are configured, maintained, and updated per vendor instructions.<br><br>(Fed Ramp)<br><br>1. Determine whether the individual intrusion detection tools are connected into an information system-wide intrusion detection system. | 1. Evidence that inbound and outbound communications and network traffic to the production network is monitored using IDS devices that generate alerts in the event of compromise<br><br>2. Population of incident tickets and evidence related to each sample selected (to be specified)<br><br>3. Population of IDS devices within the production network and evidence that they are configured to receive automatic definition and signature updates on an ongoing basis.<br><br>4. Network diagram |

| | | | |
|---|---|---|---|
| | 3. Inspect the population of IDS/IPS devices within the production network and validate that they are configured to:<br>-receive automatic definition and signature updates on an ongoing basis;<br>-enable queries and analysis of logs from a central location;<br>-capture IP addresses of the source and destination of the activity, timestamps, alert names, event data, as well as the names of the related files and objects that were grounds for the alert;<br>-capture user IDs, MAC addresses, process IDs, and event IDs if available;<br>-automate processes and alerts to mitigate high-risk threats, as defined by Security;<br>-prevent un-authorized disclosure of Company information. | | |

| | | | |
|---|---|---|---|
| TV-SIEM-NMO-020 | 1. Inquire of the control owners to determine the following:- if inbound and outbound communications and network traffic to the card-holder data network and information systems is monitored using host based and network based IDS/IPS devices that generate alerts in the event of compromise;- if the organization collects and analyzes DMZ and other critical network segment flows to detect anomalous activity;- if the organization monitors traffic leaving the organization to detect unauthorized use of encryption;- if the organization monitors, restricts, and reviews traffic between trusted and untrusted connections;- if Security is responsible for the configuration of detection and prevention rules.2. Select a sample of IDS/IPS alert incident tickets in the PCI environment from the IDS/IPS event repository and inspect the ticket details to determine that the incident was resolved and/or is actively worked to resolution. Validate IDS/IPS alerts are centrally monitored.3. Inspect the population of IDS/IPS devices within the production network and validate that they are configured to:-enable queries and analysis of logs from a central location;-capture IP addresses of the source and destination of the activity, timestamps, alert names, event data, as well as the names of the | [PCI] 1. Inspect system configurations and network diagrams to determine that IDS/IPS are in place to monitor traffic at the perimeter and critical points of the cardholder data environment 2. Inspect system configurations to determine that the IDS is set to alert personnel of events. 3. Inspect IDS/IPS configurations and vendor documentation to determine that the IDS/IPS are configured, maintained, and updated per vendor instructions. (Fed Ramp) 1. Determine whether the individual intrusion detection tools are connected into an information system-wide intrusion detection system. | 1. Evidence that inbound and outbound communications and network traffic to the card-holder data network is monitored using IDS devices that generate alerts in the event of compromise2. Population of incident tickets and evidence related to each sample selected (to be specified)3. Population of IDS devices within the production network and evidence that they are configured to receive automatic definition and signature updates on an ongoing basis.4. PCI Network diagram5. IDS vendor documentation and Security approval. |

| | | | |
|---|---|---|---|
| | related files and objects that were grounds for the alert;-capture user IDs, MAC addresses, process IDs, and event IDs if available;-automate processes and alerts to mitigate high-risk threats, as defined by Security;-prevent un-authorized disclosure of Company information. | | |

**Lista de controles según marcos de seguridad de la industria**

| Control Objective ID | NIST CSF v1_0 | ISO 27001_2 | ISO 27002_2 013 | PCI DSS v3_2 | NIST 800-53 r4 MOD | COBIT 5 | SOC2 TSP 2016 | SANS CSC 20 |
|---|---|---|---|---|---|---|---|---|
| IA-ASMT-INV-010 | ID.AM-1<br>ID.AM-2<br>PR.DS-3 | - | A.8.1.1<br>A.8.1.2 | 2.4<br>11.1.1<br>9.7.1<br>9.9.1 | CM-8<br>CM-8 (1)<br>CM-8 (5) | APO01.06<br>BAI09.01<br>BAI09.02<br>BAI09.03<br>BAI09.04<br>DSS05.06<br>DSS06.06 | - | 1.1<br>1.3<br>1.4 |
| IA-ASMT-INV-010 | ID.AM-1<br>ID.AM-2<br>PR.DS-3 | - | A.8.1.1<br>A.8.1.2 | 2.4<br>11.1.1<br>9.7.1<br>9.9.1 | CM-8<br>CM-8 (1)<br>CM-8 (5) | APO01.06<br>BAI09.01<br>BAI09.02<br>BAI09.03<br>BAI09.04<br>DSS05.06<br>DSS06.06 | - | 1.1<br>1.3<br>1.4 |
| IA-ASMT-INV-010 | ID.AM-1<br>ID.AM-2<br>PR.DS-3 | - | A.8.1.1<br>A.8.1.2 | 2.4<br>11.1.1<br>9.7.1<br>9.9.1 | CM-8<br>CM-8 (1)<br>CM-8 (5) | APO01.06<br>BAI09.01<br>BAI09.02<br>BAI09.03<br>BAI09.04<br>DSS05.06<br>DSS06.06 | - | 1.1<br>1.3<br>1.4 |
| IA-ASMT-INV-010 | ID.AM-1<br>ID.AM-2<br>PR.DS-3 | - | A.8.1.1<br>A.8.1.2 | 2.4<br>11.1.1<br>9.7.1<br>9.9.1 | CM-8<br>CM-8 (1)<br>CM-8 (5) | APO01.06<br>BAI09.01<br>BAI09.02<br>BAI09.03<br>BAI09.04<br>DSS05.06<br>DSS06.06 | - | 1.1<br>1.3<br>1.4 |
| IA-ASMT-INV-010 | - | - | - | - | - | BAI09.05 | - | |
| IA-DICP-DRT-020 | - | - | - | 3.2<br>3.2.1<br>3.2.2<br>3.2.3 | - | - | - | 13.1 |
| IA-PPCO-DLK-010 | PR.DS-5 | - | - | - | - | DSS05.07 | - | 13.3<br>13.4<br>13.6 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 13.8<br>13.9 |
| ID-IDAM-ADA-010 | - | - | A.9.2.3 | 12.5.4<br>7.1.2 | AC-6 (5) | DSS05.04<br>DSS06.03 | - | 5.8<br>5.9<br>11.6 |
| ID-IDAM-NIL-010 | PR.AC-4 | - | A.13.1.1<br>A.6.1.2 | - | AC-5 | DSS06.02<br>DSS06.03 | - | |
| ID-IDAM-NIL-020 | PR.AC-1 | - | A.9.2.1<br>A.9.2.2 | - | AC-2<br>AC-3 | - | CC5.1<br>CC5.2 | |
| ID-IDAM-NIL-020 | PR.AC-1 | - | - | 7.1.4 | AC-2<br>AC-3<br>AC-6 (1) | DSS05.04<br>DSS06.03 | CC5.1<br>CC5.2<br>CC5.4 | 14.4 |
| ID-IDAM-NIL-020 | PR.AC-4<br>PR.PT-3 | - | A.9.4.1 | 7.1<br>7.1.1<br>7.1.3 | AC-2<br>AC-3<br>AC-6<br>AC-6 (10) | DSS05.04<br>DSS06.03 | C1.2 | 5.1 |
| ID-IDAM-NIL-020 | PR.AC-4<br>PR.PT-3 | - | A.9.4.1 | 7.1<br>7.1.1<br>7.1.3 | AC-2<br>AC-3<br>AC-6<br>AC-6 (10) | DSS05.04<br>DSS06.03 | C1.2 | 5.1 |
| ID-IDAM-NIL-020 | PR.AC-1 | - | - | 7.2<br>7.2.1<br>7.2.2<br>7.2.3 | AC-2 (1) | DSS05.04 | CC5.1<br>C1.2 | |
| ID-IDAM-NIL-020 | - | - | - | 8,7 | - | - | - | |
| ID-IDAM-NIL-020 | - | - | - | - | AC-6 (2) | - | - | |
| ID-IDAM-NIL-020 | - | - | - | 8,5 | - | - | - | |
| ID-UAPD-NIL-010 | PR.AC-1 | - | - | 8.6<br>8.1.1<br>8.1<br>8.1.2 | IA-2<br>IA-8<br>IA-4<br>IA-5 (3) | DSS05.04 | CC5.1<br>CC5.3 | |
| ID-UAPD-NIL-010 | PR.AC-1 | - | - | 8.6<br>8.1.1 | IA-2<br>IA-8 | DSS05.04 | CC5.1<br>CC5.3 | |
| ID-UAPD-NIL-010 | PR.AC-1 | - | - | 8.1<br>8.1.2 | IA-4<br>IA-5 (3) | - | - | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ID-UAPD-NIL-030 | - | - | - | - | PS-5 | - | - | |
| ID-UAPD-NIL-030 | PR.AC-1 PR.IP-11 | - | A.9.2.1 A.9.2.2 A.9.2.6 | 8.1.3 8.1.4 | AC-2 (2) AC-2 (3) PS-4 | - | CC5.2 CC5.4 | 16.3 16.6 |
| ID-UAPD-NIL-030 | PR.AC-1 PR.IP-11 | - | A.9.2.1 A.9.2.2 A.9.2.6 | 8.1.3 8.1.4 | AC-2 (2) AC-2 (3) PS-4 | - | CC5.2 CC5.4 | 16.316.6 |
| ID-UAPD-NIL-030 | PR.IP-11 | - | - | - | AC-2 | - | - | |
| ID-UAPD-NIL-050 | - | - | A.9.2.5 | - | AC-2 | DSS05.04 DSS06.03 | - | 16.2 |
| ID-UAPD-NIL-050 | - | - | A.9.2.5 | - | AC-2 | DSS05.04 DSS06.03 | - | 16.2 |
| ID-UAPD-NIL-050 | - | - | A.9.2.5 | - | AC-2 | DSS05.04 DSS06.03 | - | 16.2 |
| RC-COMP-NIL-010 | ID.GV-3 | - | A.18.1.1 A.18.1.2 | - | - | EDM03.02 MEA03.01 MEA03.02 MEA03.03 | - | |
| RC-COMP-NIL-010 | ID.GV-3 | - | A.18.1.1 A.18.1.2 | - | - | EDM03.02 MEA03.01 MEA03.02 MEA03.03 | - | |
| RC-PSGM-AUP-010 | - | - | - | - | AC-8 | - | - | |
| RC-RIAT-NIL-010 | ID.RA-3 ID.RA-4 ID.RA-5 | 8.2 6.1.2 | - | 12,2 | RA-3 | APO12.01 APO12.02 EDM03.01 EDM03.02 | CC3.1 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SG-FIPM-PPM-010 | - | - | - | - | - | BAI01.01<br>BAI01.02<br>BAI01.04<br>BAI01.05<br>BAI01.07<br>BAI01.08<br>BAI01.09<br>BAI01.12<br>BAI02.01<br>BAI02.04<br>BAI03.06<br>BAI03.07<br>BAI07.01 | - | |
| SG-FIPM-PPM-010 | - | - | - | - | - | BAI01.01 | - | |
| SG-FIPM-PPM-010 | - | - | - | - | - | BAI01.02<br>BAI01.03<br>BAI01.07<br>BAI02.02<br>BAI02.04<br>EDM01.02 | - | |
| SG-FIPM-PPM-020 | - | - | - | - | - | APO05.01<br>APO05.03<br>APO06.02<br>APO06.03<br>BAI01.02 | - | |
| SG-FIPM-PPM-030 | - | - | - | - | - | BAI01.03<br>BAI01.05<br>BAI01.06<br>BAI01.11 | - | |
| SG-FIPM-PPM-040 | - | - | - | - | - | BAI01.05 | - | |
| SG-FIPM-PPM-040 | - | 5.1<br>7.1 | - | - | - | - | - | |
| SG-FIPM-PPM-060 | - | - | A.6.1.5 | - | - | BAI02.03 | - | |
| SG-PERS-RRS-010 | PR.IP-11 | - | A.13.2.4<br>A.7.3.1 | - | PS-6 | - | - | |
| SG-PERS-RRS-020 | - | - | - | - | - | APO01.02 | - | |
| SG-PERS-RRS-030 | - | - | A.7.2.1 | 12.6.2 | - | - | - | |
| SG-PM-NIL-060 | - | - | - | - | - | BAI01.10<br>BAI02.03<br>BAI03.06 | - | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SG-PRMT-NIL-020 | - | - | - | - | - | BAI01.13<br>BAI07.01<br>BAI07.08 | - | |
| SG-PRMT-QMT-010 | - | - | - | - | - | APO11.01<br>APO11.02<br>APO11.04<br>APO11.06<br>BAI01.09 | - | |
| SG-PRMT-QMT-010 | - | - | - | - | - | APO11.02<br>APO11.04<br>APO11.05<br>BAI01.09 | - | |
| SG-STRT-OSD-050 | ID.RM-1 | 5,1 | - | - | SA-2 | - | - | |
| SG-STRT-OSD-050 | ID.RM-1 | 6.2<br>8.1 | - | - | - | APO01.03<br>APO12.05<br>EDM03.01<br>EDM03.02 | - | |
| SG-STRT-OSD-050 | ID.BE-2<br>ID.BE-3<br>ID.RM-2<br>ID.RM-3 | 4,1 | - | - | - | APO01.03<br>EDM03.01 | - | |
| TV-SIEM-AUL-010 | DE.CM-3<br>PR.PT-1 | - | A.12.4.1<br><br>A.13.1.1 | 10.1<br>10.2<br>10.3<br><br>10.2.1<br><br>10.2.4<br><br>10.2.5<br><br>10.2.6<br><br>10.2.7<br><br>10.3.1<br><br>10.3.2 | AC-2 (4)<br>AU-12<br>AU-2<br>AU-3<br>AU-3 (1)<br>SI-4 | DSS01.03<br>DSS05.04 | - | 1.2<br>5.4<br>5.5<br>16.8<br>16.10 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | 10.3.3<br>10.3.4<br>10.3.5<br>10.3.6 | | | | |
| TV-SIEM-AUL-010 | - | - | - | - | AU-2<br>AU-2 (3) | - | - | |
| TV-SIEM-AUL-020 | DE.AE-2<br>DE.AE-3<br>PR.PT-1 | - | A.12.4.3 | 10.6<br>10.6.1<br>10.6.2<br>10.6.3 | | DSS05.07 | - | 6.2<br>6.4 |
| TV-SIEM-AUL-020 | DE.AE-2<br>DE.AE-3<br>PR.PT-1 | - | A.12.4.3 | 10.6<br>10.6.1<br>10.6.2<br>10.6.3 | | DSS05.07 | - | 6.2<br>6.4 |
| TV-SIEM-AUL-020 | - | - | A.12.4.2 | 10.5<br>10.2.3<br>10.5.1<br>10.5.2<br>10.5.4 | AU-6<br>AU-6 (1)<br>AU-6 (3)<br>AU-7<br>AU-7 (1) | - | - | |
| TV-SIEM-AUL-020 | - | - | - | 10,7 | AU-11 | DSS01.03 | - | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TV-SIEM-AUL-030 | - | - | A.12.4.3 | 10.2.2 | - | - | - | 14.6 |
| TV-SIEM-AUL-040 | - | - | - | - | AC-6 (9) | - | - | 5.2 |
| TV-SIEM-NMO-010 | RS.CO-5 | - | - | - | - | - | - | |
| TV-SIEM-NMO-020 | DE.CM-1 | - | - | 11,4 | | DSS05.02<br>DSS05.03 | - | 12.3<br>12.9<br>13.7 |
| TV-SIEM-NMO-020 | DE.CM-1 | - | - | 11,4 | | DSS05.02<br>DSS05.03 | - | 12.3<br>12.9<br>13.7 |