Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Diseño de arquitectura de seguridad para la modernización de la agencia digital Píxel Design Costa Rica S.A.

Tinoco Alemán Journey Alberto

Septiembre, 2020

Tabla de contenido

Declaratoria de derechos de autor **6**
Dedicatoria **7**
Resumen ejecutivo **8**
Capítulo 1. Introducción **9**
1.1 Introducción 9
1.2 Antecedentes 10
1.3 Descripción del problema 13
1.4 Justificación 15
1.4.1 Viabilidad *16*
1.5 Objetivos 18
1.5.1 Objetivo general *18*
1.5.2 Objetivos específicos *18*
1.6 Alcance y limitaciones 19
1.6.1 Limitaciones *19*
Capítulo 2. Estado de la cuestión **21**
2.1 Descripción y requerimientos del análisis de impacto de negocio. 23
2.2 Descripción y requerimientos del análisis de riesgo. 29
2.3 Descripción y requerimientos de la evaluación de desempeño. 33
Capítulo 3. Marco metodológico **39**
3.1 Tipo de investigación 39
3.1.1 Obtención de la información *40*
3.1.2 Técnicas *40*
3.2 Alcance de la investigación 41
3.3 Enfoque 41
3.4 Diseño 42
3.4.1 Diseño de la arquitectura *43*

3.4.2 Diseño de indicadores 43
Capítulo 4. Análisis del diagnóstico 44
4.1 Revisión del análisis de impacto 44
4.2 Revisión del análisis de riesgo 47
4.3 Revisión de la estrategia 48
Capítulo 5. Propuesta de solución 50
5.1 Situación actual 50
5.2 Propuesta de solución 51
5.2.1 Evaluación de soluciones 58
5.2.1 Arquitectura de la solución recomendada 60
5.2.2 Indicadores de desempeño de los controles 61
Capítulo 6. Conclusiones y recomendaciones 69
6.1 Conclusiones 69
6.2 Recomendaciones 70
Capítulo 7. Reflexiones 72
Capítulo 8. Trabajos finales 74
Referencias 75
Anexos 77
Anexo A. Formulario de análisis de impacto de negocio 77
Anexo B. Formulario de análisis de riesgos 81
Anexo C. Formulario de evaluación de desempeño 82
Anexo D. Evaluación de herramientas por categoría según Gartner 84
1. Identity and Access Manager (IAM o IdM) 84
2. File Analysis Software (FA) 84
3. Mobile Device Management (MDM) 84
4. Endpoint Protection Plataform (EPP) 85
5. Security Awareness Program (SAP) 85
6. Distributed Version Control System (DVCS o git) 85

Índice de tablas

Tabla 3. Proceso de Análisis de Impacto de Negocio 24

Tabla 4. Proceso de Análisis de Riesgo 29

Tabla 5. Proceso de evaluación de desempeño. 33

Tabla 6. Lista de las funciones principales de negocio 44

Tabla 7. Resumen de resultados del Análisis de Impacto.....45

Tabla 8. Riesgos relacionados a los pilares de seguridad y la imagen 46

Tabla 9. Nivel de riesgos inherente 47

Tabla 10. Procesos de control para tratamiento de riesgos 52

Tabla 11. Indicador de acceso de usuarios.....62

Tabla 12. Indicador de clasificación de la información 63

Tabla 13. Indicador de seguridad de dispositivos móviles 64

Tabla 14. Indicador de eventos de código malicioso.....65

Tabla 15. Indicador de concientización de personal. 66

Tabla 16. Indicador de integridad de código 66

Tabla 17. Indicadores de desempeño para las herramientas de control.....68

Índice de ilustraciones

Ilustración 1. Productos principales de la agencia digital 11

Ilustración 2. Definición gráfica de productividad más seguridad.....12

Ilustración 3. Viabilidad de los proyectos 16

Ilustración 4. Procesos relacionados con la implementación de controles. 21

Ilustración 5. Ciclo de documentación de procesos de tecnología.....23

Ilustración 6. Nivel de implementación de controles por pilar. 48

Ilustración 7. Diagrama de riesgos, controles y herramientas.....56

Ilustración 8. Trabajo en temas de gestión de accesos 58

Ilustración 9. Herramientas para procesos de control 59

Ilustración 10. Arquitectura propuesta para la mitigación de riesgos. 60

Declaratoria de derechos de autor

El actual proyecto de investigación se elaboró tras el trabajo realizado por el autor para optar por el posgrado de Maestría Profesional en Ciberseguridad.

Como único autor de este proyecto, expreso mi consentimiento a la Universidad Cenfotec para la reproducción del documento con fines exclusivamente académicos y educativos, siempre y cuando se respete y se mencione la fuente, así como la confidencialidad de la empresa Píxel Design de Costa Rica S.A.

Autor: Journey Alberto Tinoco Alemán

Dedicatoria

Dedicado a mi hermosa esposa, por ser siempre un apoyo incondicional durante todos estos años de estudio. A mi madre, que siempre ha sido un pilar en mi vida, así como toda mi familia.

Journey Alberto Tinoco Alemán

Resumen ejecutivo

La agencia digital Píxel Design de Costa S.A. ha experimentado brechas de seguridad en el pasado y no cuenta con controles que protejan los recursos críticos. Se plantea la necesidad de abordar sus necesidades relacionadas con seguridad, por lo cual se genera un proceso de identificación de funciones críticas y de documentación de riesgos para diseñar una arquitectura de seguridad. El diseño de arquitectura no solo debe ser efectivo, eficiente y eficaz, sino también debe considerarse a un costo factible y con un esfuerzo sencillo de ejecutar.

Palabras claves: ciberseguridad, agencia digital, sistema de gestión seguridad, seguridad de la información, análisis de impacto de negocio, análisis de riesgos, amenazas, riesgos, controles de seguridad, contramedidas, arquitectura de seguridad.

Capítulo 1. Introducción

1.1 Introducción

Los inicios de la era digital generan que el oleaje tecnológico se incorpore en las empresas y personas. En otras palabras, las personas se transforman por las constantes necesidades tecnológicas que la misma sociedad demanda. De este modo, la presente investigación diseña una arquitectura para modernizar y asegurar los servicios de la agencia digital denominada Píxel Design Costa Rica S.A. Se consideran los principales principios de seguridad de la información.

Internamente, en Píxel Design Costa Rica S.A. existe el objetivo de mantenerse a la vanguardia tecnológica para ofrecer el negocio de sus clientes a un nuevo nivel al utilizar soluciones tecnológicas que los vinculen con un mercado en específico; es decir, la posibilidad de generar mejores soluciones podría otorgar una ventaja competitiva en sus actuales modelos de negocio.

A partir de lo descrito anteriormente, este proyecto busca recoger la mayor cantidad de información de la organización con el fin de postular un nuevo enfoque en el diseño de los servicios, de modo que sea más atractivo, rentable y seguro. En ocasiones, a las empresas que brindan servicios y/o productos digitales hechos a la medida se les dificulta adaptarse a nuevas tecnologías y dejan de lado principios como la escalabilidad y la seguridad.

Las agencias digitales viven entre la libertad de las agencias de publicidad y lo estructurado de una compañía de desarrollo de *software*. Efectivamente, para lograr fortalecer la agencia digital, se propone diseñar un modelo de gestión basado en la

estrategia de negocio, sin dejar de lado la gestión de riesgo que defina su entorno y productos de tal manera que mejore la usabilidad, confidencialidad, integridad y disponibilidad del servicio.

Un sistema de gestión de seguridad y una arquitectura que incluya los principios de continuidad de negocio en nuevas tecnologías llevarán a la organización a fortalecer su negocio para los nuevos requerimientos de la era digital.

1.2 Antecedentes

La agencia digital Píxel Design Costa Rica S.A. inició labores en 2003, tras un abrupto cierre del lugar donde laboraban sus socios. Ello dejó a muchos de los clientes sin respaldo y a algunos de los colaboradores con la posibilidad de apoyarlos. Uno de los primeros proyectos que se desarrolló fue para la Agencia de Refugiados de la ONU, denominada Acnur, la cual requería implementar su sitio web. De esta manera, se catapultó la agencia y se crearon otros temas como *branding*, video, aplicaciones móviles e incluso mercadeo.

El inicio de Píxel Design Costa Rica S.A. implicó un gran esfuerzo para sus dos socios. Atrajo día tras día proyectos más atractivos y retadores. En la actualidad, la cartera de proyectos de la agencia digital incluye desde sitios web informativos gubernamentales hasta sistemas informativos con interacción en redes sociales. Cada iniciativa ofrece una solución personalizada y única para los clientes.

Ilustración 1. Productos principales de la agencia digital

Nota: Lista de servicios y productos de la organización. Tomado de la agencia digital Píxel Design Costa Rica S.A.

A este respecto, las redes sociales son la evolución de las tradicionales maneras de comunicación entre los seres humanos. De esta forma, Píxel Design Costa Rica S.A. pretende convertirse en un intérprete entre la industria y los consumidores de servicios.

Lograr el éxito dónde grandes compañías no lo han alcanzado, posiciona muy bien los procesos de negocio dentro de la organización. Sin embargo, en un entorno tan cambiante como el *marketing* digital al utilizar tecnología en todos sus procesos, es normal dejar brechas que pueden ser aprovechadas por un atacante y debilitar la imagen corporativa.

Por lo tanto, se requiere fortalecer los puntos débiles como una máxima del proyecto. Incluso, resulta fundamental la implantación de un sistema de gestión de

seguridad para trazar una línea de cambio en todo lo concerniente a los procesos internos.

Para lograr dicha implementación se debe considerar la utilidad del *marketing* digital en la realimentación del cliente. A diferencia del *marketing* normal, que es en una sola vía (publicidad de un medio general dirigida hacia posibles clientes), el *marketing* digital busca mantener intocables las “4P” del mercadeo, las cuales se conocen en inglés como *product* (producto), *price* (precio), *place* (distribución) y *promotion* (comunicación). Dicha protección consiste en la relación uno a uno con los clientes para satisfacer necesidades directas totalmente personalizables.

La seguridad siempre se ha visto como un *stopper*[1] para negocio, por lo cual este proyecto contempla una adecuada inclusión de la gestión de seguridad que mejore los procesos de negocio, en un ámbito donde es crucial pensar en la productividad (efectividad, eficacia y eficiencia).

Ilustración 2. Definición gráfica de productividad más seguridad

Nota: Elementos por considerar para medir la productividad de un control. Tomado del libro “The Twelve Principles of Efficiency” por Harrington Emerson, 1912.

[1] Tapón, que detiene literalmente el normal flujo de las cosas.

1.3 Descripción del problema

La sociedad ha adaptado ampliamente muchos tipos de tecnología y con ella la cantidad de amenazas que logran poner en jaque a las organizaciones. Bajo esa premisa, las agencias digitales no están excluidas de ataques internos o externos y en el caso de Píxel Design Costa Rica S.A. Los controles fueron implementados de manera incipiente, a prueba y error, al carecer de contramedidas efectivas ante posibles problemas que pudieran afectar la confidencialidad, la integridad y la disponibilidad de la información.

Mientras una organización mantenga ausencia de gestión de riesgos, tanto la probabilidad, así como el impacto por un evento de seguridad se convertirán en bombas de tiempo, complejas y difíciles de operar.

Según *Global State of Information Security® Survey* del 2018 (GSISS), el 40 % de los encuestados mencionó que la automatización y el uso de robots podrían abrir una brecha para que un ciberataque surta consecuencias críticas sobre la operación. Las agencias digitales están llenas de programas que facilitan los procesos, pero funcionan como habilitadores para ser víctimas potenciales de fraudes.

De tal manera, se puede inferir el siguiente principio: sin prácticas adecuadas de gestión de la seguridad de la información es cuestión de tiempo para que se creen brechas en la infraestructura de Píxel Design Costa Rica S.A.

En la organización existe mucha expectativa y deseo de implementar controles que faciliten cada uno de los proyectos de desarrollo. Es normal pensar en mejoras

cuando se dirige una empresa, pero cada una de ellas debe ser acompañarse por un cuidadoso proceso de selección que no impacte el flujo normal de desarrollo.

En otras palabras, existe la intencionalidad dentro de la empresa de mejorar la seguridad. Sin embargo, no se quiere perjudicar la velocidad y la entrega de soluciones, lo que implica que es determinante realizar un análisis y elección de controles destinados a mejorar la productividad.

No obstante, la elección de controles conlleva, en muchos de los escenarios, la inversión económica en licencias, aplicaciones y hasta sistemas. Esto generalmente implica que la propuesta está acompañada de una amplia justificación que muestre cómo el beneficio del control es mayor a la inversión; en otras palabras, que dicho control sea menor al riesgo que se busca tratar.

Lo anteriormente mencionado constituye un hecho común en toda organización que ha tenido la necesidad de implementar un proceso de gestión de seguridad de la información. Incluso, las organizaciones con mayor nivel de madurez suelen tener problemas en la implementación de controles, así como lo muestra la encuesta "*Fall 2018 Digital Trust Insights*" de PwC, al indicar que solo el 53 % de los entrevistados mide, de manera proactiva, la gestión de riesgos y la incluyen desde el comienzo de los proyectos y obtienen controles efectivos.

Básicamente, logran controles con un nivel de viabilidad adecuado que debería ser simple, pues ya ha sido probado en muchas organizaciones, pero la realidad es otra. Los cambios en la tecnología y la forma en que avanzan los negocios tornan el proceso de gestión de seguridad como uno de los más difíciles de manejar. Una adecuada gestión incorpora dentro del modelo un proceso de mejora continua, el cual

consiste en generar adaptabilidad y resiliencia a la organización basados en indicadores de control.

Obtener los indicadores correctos es una tarea difícil. Las organizaciones invierten mucho esfuerzo para desarrollar tableros con el propósito de entender la operatividad de los controles. De esta manera, la creación de métricas fortalece la organización, pero causa problemáticas derivadas de la falta de madurez relacionada con la seguridad dentro de la empresa. Además, se puede enfatizar la carencia de datos históricos para iniciar con la elección de los controles, que obliga a partir casi de cero con la configuración de los datos.

Reunir los indicadores en un tablero no es suficiente. Lo más crítico es adaptar los procesos de desarrollo con los controles de seguridad y que los involucrados se sientan respaldados con los cambios en su trabajo con el fin no solo de cambiar las rutinas diarias, sino también de agregar una cultura de seguridad.

Para el diseño de la arquitectura de seguridad de Píxel Design Costa Rica S.A. se efectúa un análisis antes y otro después con el fin de certificar la correcta ejecución de la implementación incluyendo todos los riesgos que dicha validación conlleva. Esta es una nueva área de inmersión para la empresa, porque la posibilidad de encontrar problemas es muy alta, en consecuencia, el objetivo final del proyecto podría afectarse. En relación con cada decisión y estrategia, debe considerarse cada diseño e implementación.

1.4 Justificación

Píxel Design de Costa Rica S.A. tiene más de 15 años en su haber; sin embargo, la agencia de *marketing* digital no cuenta con un modelo de seguridad o

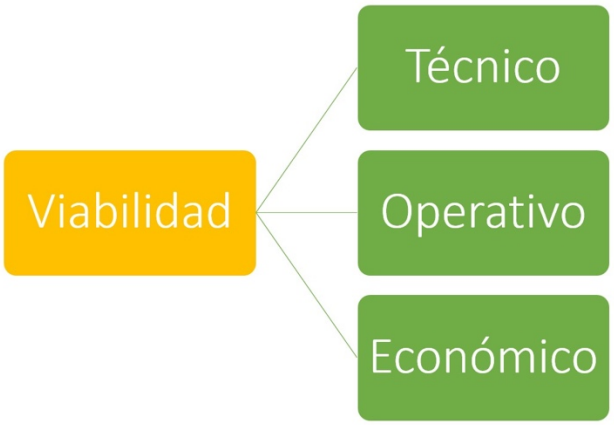
arquitectura robusta, puesto que cada uno de los controles por implementar han resultado como producto de eventos pasados que conllevaron consecuencias internas.

Con base en lo anterior, este proyecto busca diseñar una arquitectura que mejore la productividad de los desarrollos, cuya la seguridad de la información representa la base como proceso clave para la mejora continua de la organización. Todos los aspectos deben garantizar la viabilidad de la solución tanto en el aspecto técnico, operativo y económico.

1.4.1 Viabilidad

La sección de viabilidad permite describir la disponibilidad de los recursos para desarrollar los objetivos o las metas del proyecto mediante tres aspectos básicos, que se muestran a continuación en la ilustración 3.

Ilustración 3. Viabilidad de los proyectos



Nota. La imagen representa los conceptos que pueden ser parte del cálculo de la viabilidad de un proyecto. Tomado del libro "Evaluación de proyectos", por Gabriela Baca, 6ª Edición, Mc Graw-Hill, 2010.

1.4.1.1 Punto de vista técnico

El punto de vista técnico pretende c Actualmente, hay una adecuada disposición para el perfeccionamiento de controles e incluso existirá la posibilidad de apoyar la calidad de los productos. Por lo tanto, el proyecto es viable técnicamente.

1.4.1.2 Punto de vista operativo

Desde el punto de vista operativo, la organización acepta los controles que se diseñan durante el proceso de implementación y, una vez finalizados, se calculará la efectividad operativa. Los indicadores de desempeño sobre los controles de seguridad de la información se calculan sobre las superficies de ataque (personas, dispositivos, redes y aplicaciones) que indiquen de manera cuantitativa la efectividad (cumplimiento), la eficiencia (evaluación) y la eficacia (gestión) de la implementación de controles.

1.4.1.3 Punto de vista económico

Para alcanzar los objetivos, descritos en la siguiente sección, es imperante realizar un análisis de costo-beneficio. Se considera el proceso de análisis de riesgo. En caso de una implementación de soluciones que involucren un costo de licencia, aplicaciones o sistemas, se llevarán ante la agencia con el fin de validar si su compra es relevante.

Por lo demás, al ser una agencia digital, todos los formularios y la recolección de información se gestionará de manera digital; por lo tanto, se establece la viabilidad económica, pues el diseño no tendrá costo alguno para la agencia.

1.5 Objetivos

Cada uno de los objetivos fueron definidos utilizando la taxonomía de Bloom. La metodología ha sido probada en muchos ámbitos y es ampliamente aceptada por la academia.

1.5.1 Objetivo general

Diseñar una arquitectura de seguridad que implique la modernización de la agencia digital Píxel de Costa Rica S.A. y asegure los productos principales de la agencia ante las amenazas relacionadas con el *marketing* digital en aras del mejoramiento de la productividad mediante la implementación de controles en la cadena de producción.

1.5.2 Objetivos específicos

1. Determinar todos los posibles riesgos de la agencia mediante un análisis de impacto del negocio que determine las brechas relacionadas con la cadena de producción.
2. Optimizar la gestión de riesgos por medio del desarrollo de una estrategia que trate los riesgos encontrados en el análisis de impacto de negocio.
3. Implementar, dentro de la agencia digital, los controles de seguridad documentados dentro del análisis de riesgo, que incluyan previamente un estudio de factibilidad relacionado con las soluciones.
4. Recomendar una lista de herramientas orientadas a el tratamiento de los riesgos sin comprometer los tiempos de desarrollo dentro de la cadena de producción.

5. Adaptar la forma en que la seguridad se acopla a las superficies de ataque (personas, dispositivos, redes y aplicaciones) mediante la implementación de indicadores de desempeño, que involucren cada una de las superficies.

1.6 Alcance y limitaciones

El alcance es esencial para cualquier proyecto, porque describe las funcionalidades de la organización y desarrolla de forma precisa los controles que deben ser utilizados. Junto al alcance, siempre es necesario conocer las metodologías que se emplearán en el proyecto, así como establecer el seguimiento de las actividades ya terminadas. Todo lo anterior resulta necesario con el objeto de minimizar situaciones problemáticas que generen desgastes de tiempo valioso.

Nunca está de más documentar todo lo que se ha planeado, así como tener sentido común respecto a lo que fue previamente solicitado y lo que se espera que se entregue. Muchas veces, existen buenas intenciones, pero ninguna de ellas se enfoca en otorgar un valor agregado a la organización.

Este proyecto se limita al diseño y a la recomendación de implementación de los controles óptimos para la agencia. La decisión de inversión en estos controles está fuera del alcance de este proyecto.

1.6.1 Limitaciones

Entre las principales limitaciones del proyecto se mencionan las siguientes:

- La estructura de Píxel Design Costa Rica S.A. no es extensa. Ello implica que pueda existir recarga de controles o una restricción sobre el personal.

- Insuficiente apoyo de los socios con respecto a la seguridad de la información.
- La necesidad de personal calificado para la gestión de la seguridad de la información ayudaría bastante en el proceso; sin embargo, al momento, no hay apoyo adicional.
- Falta de recursos y costos no planeados.
- La confidencialidad de la información es uno de los ejes claves para darle confianza a los clientes.
- La industria de controles de seguridad está enfocada en organizaciones cuyo tamaño supera a las medianas empresas. Las soluciones de mayor calidad tienen costos superiores a la expectativa de las pequeñas empresas.

Capítulo 2. Estado de la cuestión

En este capítulo se atiende el estado de la cuestión del diseño de una arquitectura de seguridad para la mejora de la productividad. Cabe recalcar que, al mencionar la palabra productividad, se hace referencia a la efectividad, la eficacia y la eficiencia en los controles. Asimismo, cuando se menciona la palabra seguridad se alude a la confidencialidad, la integridad y la disponibilidad de la información que protegen los controles en la organización.

Derivado de la afirmación anterior, se puede deducir que el diseño de arquitectura está intrínsecamente relacionado con la implementación de controles y cómo estos interactúan con los procesos de negocio. La implementación de controles se efectúa a través de tres procesos en específico; análisis de impacto de negocio, análisis de riesgo y evaluación del desempeño.

Ilustración 4. Procesos relacionados con la implementación de controles.

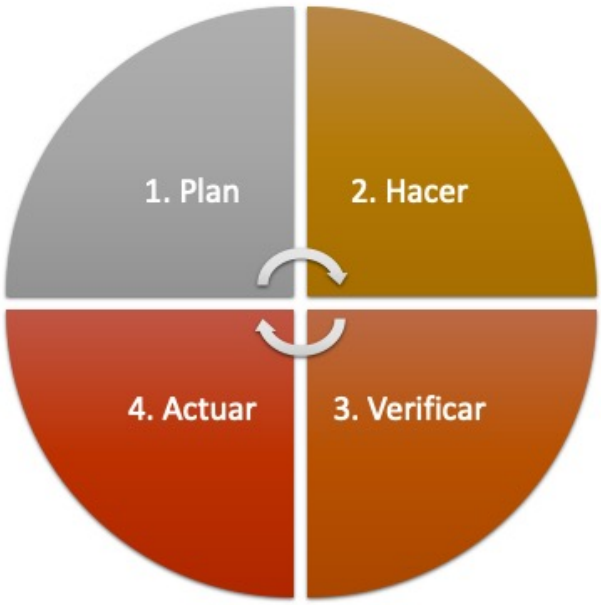
Nota. La imagen muestra los procesos principales para la implementación de un sistema de gestión de seguridad de la información. Tomado del estándar internacional ISO 27001:2013.

De manera detallada, se procede a describir el proceso con base en los siguientes estándares de industria:

1. **Análisis de impacto de negocio:** “ISO 22301:2012 Societal security — Business continuity management systems — Requirements”, cláusula 8.2.2.
2. **Análisis de riesgo:** “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 6.1.
3. **Evaluación del desempeño.** “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 6.2 y 9. Adicionalmente, el estándar “ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation”, cláusula 8.

Para la descripción de los procesos, los modelos y los estándares se utilizará el estándar “**ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes**”, cláusula 6.1. El proceso de documentación tiene el objetivo de llevar, registrar y guiar a las partes interesadas en todo lo relevante al ciclo de vida del desarrollo. El proceso contiene el conjunto de actividades para planificar, diseñar, desarrollar, producir, editar distribuir y mantener aquellos documentos que necesitan todas las partes interesadas. Este proceso consta de las siguientes actividades:

Ilustración 5. Ciclo de documentación de procesos de tecnología



Nota. Representación gráfica del ciclo de Deming. Tomado de Calidad, Productividad y Competitividad: la salida de la crisis (p.412), por William Edwards Deming, 1989.

2.1 Descripción y requerimientos del análisis de impacto de negocio.

La empresa debe establecer, implantar y mantener un proceso formal documentado para la evaluación y la determinación de la continuidad y la recuperación de prioridades, objetivos y metas. El proceso debe incluir la evaluación de los impactos de interrumpir las actividades que apoyan los productos y servicios de la empresa.

En el siguiente resumen se describe el proceso de **análisis de impacto de negocio**, con el cual se desarrollará la documentación y que sirve de base para las siguientes ejecuciones de la fase de operación.

Tabla 1. Proceso de Análisis de Impacto de Negocio

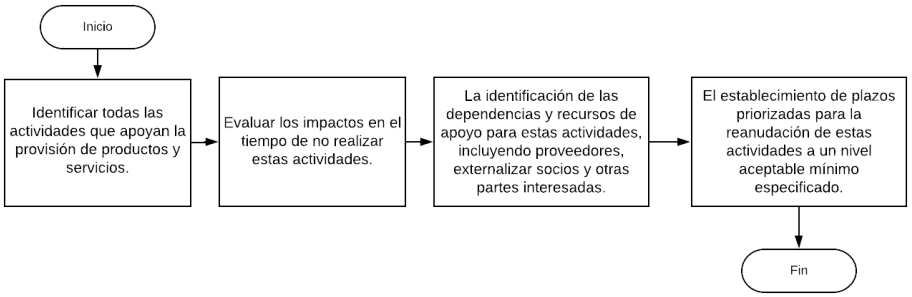
Proceso de análisis de impacto de negocio

Implementa-ción del proceso	Propósito
	La organización debe establecer, implementar y mantener un proceso de evaluación formal y documentado con el fin de evaluar la continuidad y la recuperación de los objetivos y metas. Este proceso debe incluir la evaluación de impactos de las actividades disruptivas que soportan a los productos y servicios de la organización. Referencia: “ISO 22301:2012 Societal security — Business continuity management systems — Requirements”, cláusula 8.2.2.
	Audiencia
	Este proceso involucra a todo el personal que trabaja dentro del alcance del Sistema de Gestión de Seguridad de la Información también debe ser consciente de la política de seguridad, de su contribución a la efectividad del sistema y de sus implicaciones en la resolución. Referencia: “ISO/IEC 27001:2013 Information

Proceso de análisis de impacto de negocio

	technology — Security techniques — Information security management systems — Requirements", cláusula 7.3.
	Responsable
	La alta dirección debe asegurarse de que las responsabilidades y las autoridades para los roles pertinentes sean asignadas y comunicadas dentro de la organización. La alta dirección debe asignar la responsabilidad y autoridad relacionada a: a) Asegurar que el sistema de gestión se establezca en conformidad con los requisitos de negocio y estándares adoptados. b) Informar sobre el desempeño a la alta dirección. Referencia: "ISO 22301:2012 Societal security — Business continuity management systems — Requirements", cláusula 5.4.
	Plazo de versión
	Anualmente. Referencia: "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", cláusula 8.

Proceso de análisis de impacto de negocio

Diseño y desarrollo	Actividades
	
Producción	Conservación
	La información documentada requerida debe ser controlada para asegurar que: a) Está disponible y es apropiada para su uso, donde y cuando sea necesario. b) Está adecuadamente protegida (por ejemplo, de pérdida de confidencialidad, uso inapropiado o pérdida de la integridad). Referencia: “ISO 22301:2012 Societal security — Business continuity management systems — Requirements”, cláusula 7.5.3.
	Acceso y privilegios

Proceso de análisis de impacto de negocio

	Al establecer el control de la información documentada, la organización debe asegurarse que existe una protección adecuada de la información (por ejemplo, protección contra el compromiso, la modificación o supresión no autorizada). Referencia: “ISO 22301:2012 Societal security — Business continuity management systems — Requirements”, cláusula 7.5.3.
	Mantenimiento
	Para controlar el uso de la información, la organización debe orientarse a las siguientes actividades, cuando sea aplicable: • Distribución, acceso, recuperación y uso. • Almacenamiento y conservación, incluyendo preservación de la legibilidad (es decir, lo suficientemente claro para leer), • Control de cambios (por ejemplo, control de versiones), • Retención y eliminación. • Prevención del uso no intencionado de la información obsoleta. Referencia: “ISO 22301:2012 Societal security — Business continuity management systems — Requirements”, cláusula 7.5.3.

Proceso de análisis de impacto de negocio

	Controles
	Se deberán establecer controles de acuerdo con el proceso de gestión de la configuración. Referencia: “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.2.
Mantenimien -to	Última modificación
	Se deberán llevar a cabo las tareas que se requieran cuando se realice la modificación de la documentación. Para aquellos documentos que están bajo la gestión de la configuración, las modificaciones se deberán administrar de acuerdo con el proceso de gestión de la configuración. Referencia “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.1.4.

Nota. Tabla confeccionada con base en el estándar “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.1

2.2 Descripción y requerimientos del análisis de riesgo.

En el siguiente resumen se describe el proceso de **análisis de riesgo**, con el cual se desarrollará la documentación y que sirve de base para las siguientes ejecuciones de la fase de operación.

Tabla 2. Proceso de Análisis de Riesgo

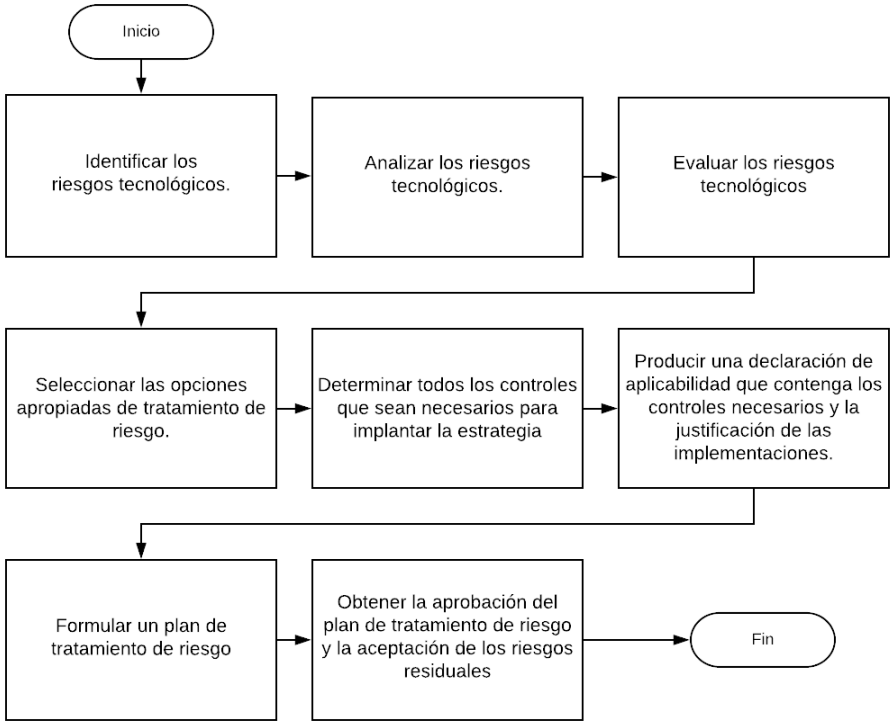
Proceso de análisis de riesgo

Implementa-ción del proceso	Propósito
	Determinar los riesgos y las oportunidades que le permitan asegurar que el Sistema de Gestión de Seguridad de la Información logre sus resultados, prevenir o reducir los efectos no deseados y lograr la mejora continua. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 6.1.
	Audiencia
	Este proceso involucra a todo el personal que trabaja dentro del alcance del Sistema de Gestión de Seguridad de la Información también debe ser consciente de la política de seguridad, de su contribución a la efectividad del sistema y de sus implicaciones en la resolución. Referencia: “ISO/IEC 27001:2013 Information

Proceso de análisis de riesgo

	technology — Security techniques — Information security management systems — Requirements", cláusula 7.3.
	Responsable
	La alta dirección debe demostrar liderazgo y compromiso especialmente en los siguientes puntos: a) Se deben asignar responsabilidades y autoridad para garantizar el cumplimiento de los controles. b) Informar a los socios el estado y el desempeño del Sistema de Gestión de Seguridad de la Información. Referencia: "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", cláusula 5.3.
	Plazo de versión
	Anualmente. Referencia: "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", cláusula 8.
	Flujo

Proceso de análisis de riesgo

Diseño y desarrollo	
Producción	Conservación
	Deberá definirse cómo se gestiona el ciclo de vida de la documentación al incluir creación, distribución, acceso, uso, almacenamiento y destrucción. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 7.5.
	Acceso y privilegios

Proceso de análisis de riesgo

La documentación requerida deberá estar controlada para asegurar: a) Está accesible y adecuada para su uso cuándo y dónde sea necesario. b) Está adecuadamente protegida. c) Se controlan los cambios. d) Se garantizan los periodos de retención y conservación. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 7.5.
Mantenimiento
No aplica.
Controles
Se deberán establecer controles de acuerdo con el proceso de gestión de la configuración. Referencia: “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.2.
Última modificación

Proceso de análisis de riesgo

Mantenimien-to	Se deberán llevar a cabo las tareas que se requieran cuando se realice la modificación de la documentación. Para aquellos documentos que están bajo la gestión de la configuración, las modificaciones se deberán administrar de acuerdo con el proceso de gestión de la configuración. Referencia “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.1.4.

Nota. Tabla confeccionada con base en el estándar “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.1

2.3 Descripción y requerimientos de la evaluación de desempeño.

En el siguiente resumen, se describe el proceso de **evaluación de desempeño**, con el cual se desarrolla la documentación y es la base de las actividades relacionadas con la fase de operación.

Tabla 3. Proceso de evaluación de desempeño.

Proceso de evaluación de desempeño

	Propósito

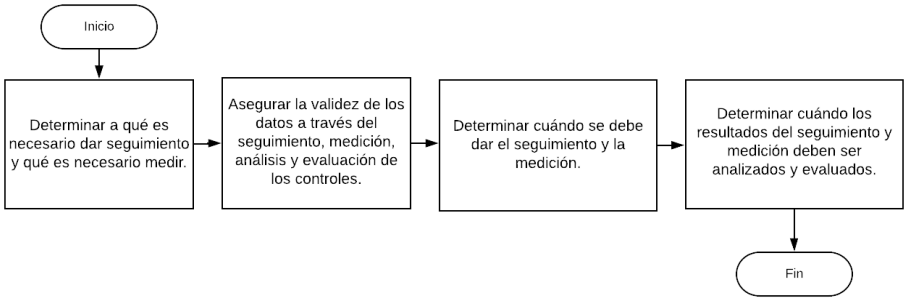
Proceso de evaluación de desempeño

Implementación del proceso	Establecer objetivos según funciones y niveles de forma que sean coherentes con la política de seguridad, sean medibles, tengan en cuenta los requisitos y necesidades del Sistema de Gestión de la Seguridad de la Información, así como los resultados del análisis de riesgos. Referencia: • "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", cláusula 6.2 y 9. • "ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation", cláusula 8.
	Audiencia
	Este proceso es para todo el personal que trabaja dentro del alcance del Sistema de Gestión de Seguridad de la Información. También, debe ser consciente de la política de seguridad, de su contribución a la efectividad del sistema y de sus implicaciones en la resolución. Referencia: "ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements", cláusula 7.3.

Proceso de evaluación de desempeño

Responsable
La alta dirección debe demostrar liderazgo y compromiso especialmente en los siguientes puntos: a) Se deben asignar roles y responsabilidades para garantizar el cumplimiento de los controles. b) Informar a los socios el estado y desempeño del Sistema de Gestión de Seguridad de la Información. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 5.3.
Plazo de versión
Anualmente. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 8.
Flujo

Proceso de evaluación de desempeño

Diseño y desarrollo	
Producción	Conservación
	Deberá definirse como se gestiona el ciclo de vida de la documentación al incluir creación, distribución, acceso, uso, almacenamiento y destrucción. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 7.5.
	Acceso y privilegios
	La documentación requerida deberá estar controlada para asegurar: a) Está accesible y adecuada para su uso en el lugar y tiempo necesarios. b) Está adecuadamente protegida. c) Se controlan los cambios.

Proceso de evaluación de desempeño

	d) Se garantizan los periodos de retención y conservación. Referencia: “ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements”, cláusula 7.5.
	Controles
	Se deberán establecer controles de acuerdo con el proceso de gestión de la configuración. Referencia: “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.2.
Mantenimien -to	Última modificación
	Se deberán llevar a cabo las tareas que se requieran cuando se realice la modificación de la documentación. Para aquellos documentos que están bajo la gestión de la configuración, las modificaciones se deberán administrar de acuerdo con el proceso de gestión de la configuración. Referencia “ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes”, cláusula 6.1.4.

Nota. Tabla confeccionada con base en el estándar "ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes", cláusula 6.1

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

La investigación y el diagnóstico implementados en este proyecto son de tipo evaluativo. El propósito, al que lleva la investigación, es identificar los riesgos asociados a la cadena de producción y determinar posibles brechas que puedan ser aprovechadas por agentes internos o externos, dentro de la agencia digital. Dicho tema está alineado a los objetivos descritos en este documento y plantea la generación de estrategias y la búsqueda de soluciones que beneficien la organización.

Las soluciones descritas en esta investigación necesitan del entendimiento y del análisis de los resultados, de manera que se pueda trazar una estrategia bajo los principios y controles de seguridad de la información. Dichas medidas deben ser soportadas por el análisis de la información recolectada en este proyecto y además ser validas en los procesos de la organización. Cada uno de los elementos utilizados en la investigación serán validados con los responsables que administran la agencia digital.

Una vez hecho todo el análisis de los riesgos, se requerirá una evaluación puntual y orientada a las necesidades de negocio para describir las diferentes soluciones que serán parte de la arquitectura y herramientas para el cumplimiento de los objetivos del proyecto.

3.1.1 Obtención de la información

Para efectos de este proyecto, se requiere un proceso de entendimiento de los procesos generales que son los pilares del negocio. Se realizan sesiones de trabajo directamente con los responsables principales de la continuidad del negocio. En la investigación se desarrollaron tres formularios claves con los cuales se identifican las brechas de seguridad que ponen en riesgo las necesidades del negocio. Dichos formularios se describen a continuación:

- **Formulario de Análisis de Impacto de Negocio:** Este formulario explora tres temas puntuales; las funciones que son críticas en el negocio basado en cinco parámetros de criticidad, los tiempos de respuesta que se relacionan a las funciones críticas del negocio y los recursos necesarios para mantener las funciones activas.
- **Formulario de Análisis de Riesgo:** Uno de los aspectos más importantes por identificar son los riesgos relacionados directamente a las funciones críticas de negocio. Dentro del formulario se identifican y ponderan cualitativamente los riesgos.
- **Formulario de Estrategia de Tratamiento de Riesgos:** Documento con el cual se plantean la situación actual y los controles actuales para tratar los riesgos identificados.

3.1.2 Técnicas

En la recolección de la información aparece la posibilidad de recolectar información a través de la observación o también al utilizar los formularios de investigación. Adicionalmente, la experiencia del investigador al desempeñar labores

en la agencia digital posibilitó contar con un entendimiento general de los procesos y la forma de trabajo de las solicitudes de requerimiento.

3.2 Alcance de la investigación

El alcance de la investigación está orientado a explorar la situación actual de la organización. Nunca se había hecho una exploración orientada a seguridad de la información, por lo que se utilizarán las principales técnicas relacionadas con la auditoria y la protección de datos.

Consecuentemente a la investigación realizada, se propone una solución orientada directamente a la gestión de riesgos y elección de los controles que servirán como facilitadores en el tratamiento de las brechas. Los controles incluyen una descripción detallada y se documentan los indicadores con que se evaluará el desempeño.

3.3 Enfoque

El enfoque de la investigación es cualitativo para facilitar la implementación de las técnicas de gestión de seguridad de la información dentro de la organización y está totalmente orientado a lograr los objetivos del proyecto. Es importante entender que, bajo el esquema de niveles propuesto en el estándar ISO/IEC 27001:2013, la organización se encuentra en un nivel de madurez 0, lo cual quiere decir que todos los procesos utilizan el sentido común del implementador y no se evalúa la eficacia de los controles actuales.

El hecho anteriormente descrito implica que se debe aspirar a ejecutar un proceso que cumpla con los siguientes principios de diseño:

- Principio de simplicidad: bajo este principio toda propuesta y solución deben implementarse, gestionarse y medirse de manera sencilla.
- Principio de economía: la solución propuesta debe ser a todo nivel más económica que los riesgos que pudieran materializarse en caso de no contar con contramedidas.
- Principio de valor: los entregables deben trascender los controles. Estos deben ser facilitadores de las operaciones del negocio.
- Principio de medición: las soluciones deben estar acompañadas de indicadores y métricas para calcular la productividad.
- Principio de sombrilla: no esperar cubrirlo todo, sino lo más importante.
- Principio de administración del conocimiento: en busca de una mejora en los procesos, se pretende que la solución se enfoque no solamente en la tecnología, sino también en las personas y en los procesos.

3.4 Diseño

Implementar una investigación evaluativa bajo el enfoque descrito anteriormente. Implica la inclusión de un método de revisión orientado a identificar, proteger, detectar, responder y recuperar las funciones críticas de la organización con una metodología basada en el uso de un sistema de gestión de seguridad de la información, donde los procesos claves giran alrededor de la gestión de riesgos para la mejora continua.

El resultado cuenta con un esquema de contramedidas relacionadas con el tratamiento de los riesgos identificados durante los análisis de diagnóstico que se elaboraron durante este proyecto.

3.4.1 Diseño de la arquitectura

El objetivo principal de un diseño de arquitectura es proveer un ambiente para que las funciones y otras aplicaciones trabajen correctamente mediante una representación gráfica de una o más capas tecnológicas. Adicionalmente, la representación puede ser enteramente física o lógica, dependiendo de la madurez técnica de organización, por lo cual para esta investigación se plantea mostrar una representación lógica fácil de comprender para la audiencia.

3.4.2 Diseño de indicadores

Se sugiere tener tres tipos de indicadores. El primero se relaciona con el cumplimiento, que se orienta a tener las tareas finalizadas. El segundo se refiere a la evaluación, que busca evaluar el rendimiento del proceso. El tercero se enfoca en la gestión, que consiste en mejorar el control cuando ya existe un nivel de maduración después de varias iteraciones.

Capítulo 4. Análisis del diagnóstico

La investigación inicia con el análisis de impacto. Esta tarea se basa en entender las funciones críticas que mantienen las operaciones. Una vez identificadas, se evalúan los posibles riesgos relacionados con los vectores de ataque. Asimismo, con la estrategia de la situación actual se puede medir el nivel de madurez con respecto a la elección de los controles de la agencia digital.

4.1 Revisión del análisis de impacto

Durante la revisión de la "Sección A" del *Anexo A. Formulario de análisis de impacto de negocio* se logran identificar las funciones más críticas de la organización. A continuación, se muestra la tabla con los criterios de criticidad:

Tabla 4. Lista de las funciones principales de negocio

Principales funciones del área de negocio		Criterios de criticidad					
#	Función	Aquella que genera mayor contacto con el cliente por período específico.	Aquella que genera mayor ganancia para la entidad.	Aquella que posee mayor impacto en los proyectos.	Aquella cuyos impactos podrían ser críticos en el corto plazo si se interrumpe.	Aquella de la cual dependen otras funciones críticas.	Funciones críticas del área de negocio.
1	Recepción de llamadas.						No crítica
2	Realización de propuesta económica y seguimiento cliente.	X	X		X		Crítica
3	Definición de alcance y tiempo de entrega según propuesta aprobada.			X		X	Crítica
4	Revisión de nuevas solicitudes en el proceso de desarrollo para crear nuevas propuestas económicas.						No crítica
5	Cierre y propuesta post-venta.						No crítica

Nota. La tabla muestra las funciones principales de la organización y los criterios para determinar la criticidad. Tomado del Anexo A. Formulario de análisis de impacto de negocio.

De la anterior tabla sobresalen dos funciones, debido a que cumplen uno o más criterios de criticidad. Las funciones son "Realización de propuesta económica y

seguimiento de clientes", así como la "Definición de alcance y tiempo de entrega según propuesta aprobada", que para sus efectos esta última consiste en el levantamiento de requerimientos y el desarrollo de la solución de los clientes.

Adicionalmente, a través del Análisis de Impacto se le da un RTO[2] a las funciones críticas y se identifican los activos de información sensible, así como su RPO[3]. Ambos datos permiten tener una visión más detallada de lo que se debe proteger e identificar los posibles riesgos relacionados con ellos.

Tabla 5. Resumen de resultados del Análisis de Impacto

1. Funciones críticas del negocio

No.	Función	Área de negocio	RTO	Criticidad	Nivel de criticidad
1	Definición de alcance y tiempo de entrega según propuesta aprobada	1	De 4 horas a 1 día	Crítica	Alta
2	Realización de propuesta económica y seguimiento cliente	1	Mayor a 4 días	Crítica	Medio

2. Información sensible

No.	Información	Físico/Electrónico	Lugar de almacenamiento	Promedio de modificación	Reconstrucción
1	Presentaciones de la empresa	Electrónico	Dropbox, email y DDs.	5 horas	8 horas
2	Propuestas económicas	Electrónico	Dropbox, email y DDs.	3 horas	8horas
3	Correos electrónicos	Electrónico	Dropbox, email y DDs.	20 minutos	8 horas
4	PDF	Electrónico	Dropbox, email y DDs.	30 minutos	2 días
5	Código fuente	Electrónico	Dropbox, email y DDs.	2 horas	2 días
6	Archivos de diseños	Electrónico	Dropbox, email y DDs.	20 minutos	2 días

Nota. Las tablas indican las funciones críticas de la organización y los tipos de activos de información. Tomado del Anexo A. Formulario de análisis de impacto de negocio.

Mediante un ejercicio de generación de posibles brechas, donde se correlacionen los pilares de la seguridad y las funciones críticas de negocio, se puede tener una vista a los posibles riesgos generales, que podrían comprometer los

[2] RTO: Tiempo de respuesta objetivo ("Recovery Time Objective"), según el Disaster Recovery Institute Internacional, es el tiempo objetivo para la restauración y recuperación de funciones o recursos en un tiempo aceptable sin servicio o ejecución cuando haya un caso de disrupción en las operaciones.

[3] RPO: Punto de recuperación objetivo ("Recovery Point Objective"), según el Disaster Recovery Institute Internacional. Es el máximo punto de recuperación de la información almacenada en la que se puede restaurar sin que perjudique las operaciones luego de un incidente.

tiempos de entrega máximos descritos anteriormente y se pueden identificar los siguientes riesgos:

Tabla 6. Riesgos relacionados a los pilares de seguridad y la imagen

Pilar \ Funciones	Definición de alcance y tiempo de entrega según propuesta	Realización de propuesta económica y seguimiento cliente
Disponibilidad	• Detención de los servicios relacionados con las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.	
	• Pérdida de la disponibilidad de los servicios relacionados con la definición y la finalización de tiempos de entrega debido al uso inapropiado de privilegios y accesos.	
	• Interrupción de los servicios y bloqueo a la información por ataques de denegación, programas malignos o acciones ejecutadas por un agente interno o externo.	
	• Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.	
Integridad	• Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.	

Pilar \ Funciones	Definición de alcance y tiempo de entrega según propuesta	Realización de propuesta económica y seguimiento cliente
Confidencialidad	• Robo de códigos fuentes e información de clientes a través de escalación de permisos realizado por usuarios o aplicaciones.	

Nota. La tabla contiene los riesgos originados de la relación entre los pilares de seguridad y el Análisis de Impacto.

En resumen, existen **seis riesgos** iniciales que pueden comprometer la disponibilidad de las **dos funciones críticas** en la organización y a los **seis activos de información sensible**. Además, el tiempo de recuperación objetivo es de **24 horas (RTO)** y el punto de recuperación objetivo es de **8 horas (RPO)**.

4.2 Revisión del análisis de riesgo

Durante la revisión del *Anexo B. Formulario de análisis de riesgos* se ponderaron, de manera cualitativa los riesgos desarrollados durante la etapa del Análisis de Impacto. Es importante mencionar que la probabilidad y el impacto de todos los riesgos fue calculado según el criterio experto de los administradores de negocio, de manera que fueran ellos mismos quienes priorizaron su nivel de riesgo, tal como se muestra en la siguiente tabla:

Tabla 7. Nivel de riesgos inherente

Código	Descripción	Probabilidad		Impacto		Nivel de Riesgo
		Frecuencia	Controles	Función crítica 1. Realización de propuesta económica y seguimiento cliente.	Función crítica 2. Definición de alcance y tiempo de entrega según propuesta aprobada.	
RISK-01-DIS	Detención de los servicios relacionados a las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.	Se podría materializar en menos de 1 mes.	Existen más de dos controles que contengan el riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Intermedio (48)
RISK-02-DIS	Pérdida de la disponibilidad de los servicios relacionados a la definición y finalización de "tiempos de entrega" debido al uso inapropiado de privilegios y accesos.	Se podría materializar en menos de 1 mes.	Existe al menos un control que contenga el riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (90)
RISK-03-DIS	Interrupción de los servicios y bloqueo a la información por ataques de denegación, malware o acciones ejecutadas por un agente interno o externo.	Se podría materializar en menos de 1 mes.	No existe un control relacionado al riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Alto (60)
RISK-04-DIS	Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.	Se podría materializar en menos de 6 meses	Existe al menos un control que contenga el riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Intermedio (42)
RISK-05-INT	Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.	Se podría materializar en menos de 3 meses	Existe al menos un control que contenga el riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (80)
RISK-06-CON	Robo de códigos fuentes e información de clientes a través de escalación de permisos realizado por usuarios o aplicaciones.	Se podría materializar en menos de 3 meses	No existe un control relacionado al riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (90)

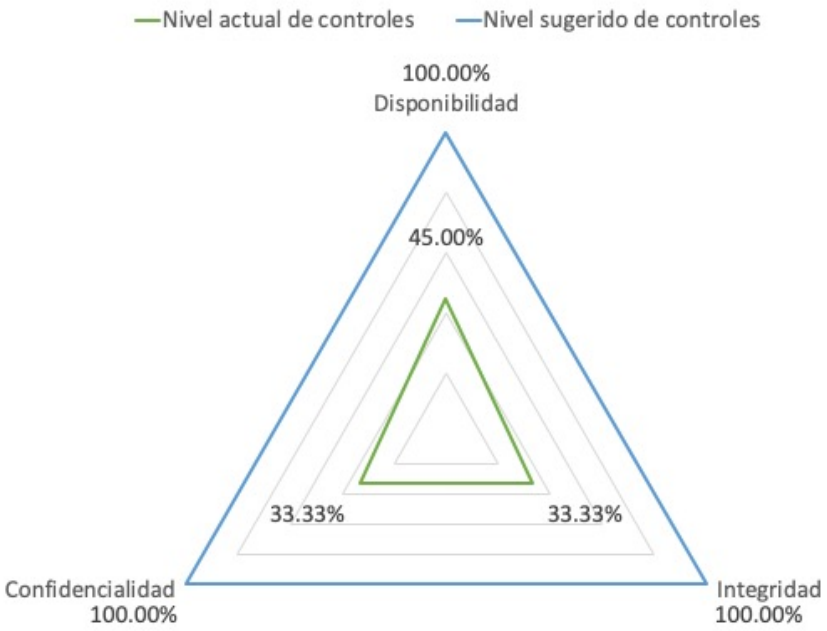
Nota. En la tabla se muestra la ponderación de los riesgos. Tomado del Anexo B. Formulario de análisis de riesgos.

En resumen, existen **tres riesgos críticos** que deben ser atendidos con prioridad, dándoles como tratamiento la implementación de controles de mitigación. También, se encuentra **un riesgo alto** y **dos riesgos intermedios**, los cuales también se tratarán con controles que disminuyan la frecuencia de ocurrencia. Determinar el nivel de riesgo permite orientar los esfuerzos a resolver lo más crítico primero.

4.3 Revisión de la estrategia

En esta etapa se ejecutó una revisión del *Anexo C. Formulario de evaluación de desempeño*. En el formulario se documenta la existencia y las herramientas relacionadas con los riesgos con el fin de tener una visión de la madurez y efectividad de las herramientas.

Ilustración 6. Nivel de implementación de controles por pilar.



Nota. En la ilustración se muestra los niveles de control implementados en la organización versus lo recomendable. Tomado del Anexo C. Formulario de evaluación de desempeño.

A manera de resumen, se visualiza que del 100 % de controles sugeridos, solo están implementados en un **45 % los relacionados a la disponibilidad**, mientras que los dirigidos a **integridad y confidencialidad tienen un 33.33 % de uso**. Las herramientas que se utilizan para resguardar la seguridad son 1Password (usada para mantener la confidencialidad) y BitBucket (utilizada en la protección de la integridad del código fuente). Adicionalmente, se recalca que todas las decisiones de seguridad se han realizado al utilizar solamente el sentido común.

Capítulo 5. Propuesta de solución

5.1 Situación actual

Del análisis de diagnóstico, se puede concluir que la organización no ha implementado algún proceso de madurez o mejora continua. Todas las implementaciones relacionadas con seguridad se realizan por una necesidad de sentido común. La información sensible es almacenada y compartida a través de su herramienta de Dropbox, correo electrónico, servidores y equipos de los colaboradores.

La organización no quiere interrumpir las labores de sus dos funciones críticas, las cuales son “Definición de alcance y tiempo de entrega según propuesta” y “Realización de propuesta económica y seguimiento cliente”. Con base en estas funciones, se determinaron seis riesgos que pueden poner en peligro los objetivos generales de negocio. Dichos riesgos son los siguientes:

- RISK-01-DIS: Detención de los servicios relacionados con las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.
- RISK-02-DIS: Pérdida de la disponibilidad de los servicios relacionados con la definición y la finalización de "tiempos de entrega", debido al uso inapropiado de privilegios y accesos.
- RISK-03-DIS: Interrupción de los servicios y bloqueo a la información por ataques de denegación, código malicioso o acciones ejecutadas por un agente interno o externo.

- RISK-04-DIS: Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.
- RISK-05-INT: Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.
- RISK-06-CON: Robo de códigos fuentes e información de clientes a través de escalación de permisos realizado por usuarios o aplicaciones.

Para la protección de la agencia digital las **dos herramientas** más importantes son 1Password[4] y BitBucket[5]. Ambas herramientas, aunque útiles, están limitadas por la naturaleza del mismo negocio y de los flujos de trabajo en la agencia digital. El costo anual de 1Password es de $96.00 dólares por usuario y para BitBucket es de $72.00 dólares por usuario también. Ello implica una inversión anual en seguridad de **$168.00 por usuario**.

5.2 Propuesta de solución

La solución se basa enteramente en una gestión de riesgo relacionada con las funciones. Se propone iniciar como primera fase al nombrar procesos de control para el tratamiento de los riesgos. Los procesos de control, más que una herramienta, son flujos de actividades para controlar las brechas que se pueden dar en las personas, procesos o tecnología. A continuación, se muestran los procesos y subprocesos claves para tratar el riesgo:

---

[4] 1Password: Es un gestor de contraseñas para empresas centrado en la privacidad. La herramienta además puede comprobar a lo que cada persona tiene. Fuente: https://1password.com

[5] BitBucket: Es una herramienta para la administración de versiones de código, incluso con la capacidad de organización en varios ambientes como desarrollo y producción. Fuente: https://bitbucket.org

Tabla 8. Procesos de control para tratamiento de riesgos

Riesgo	Proceso de control	Subprocesos de apoyo
RISK-02-DIS: Pérdida de la disponibilidad de los servicios relacionados con la definición y la finalización de tiempos de entrega, debido al uso inapropiado de privilegios y accesos.	CNTRL-02-DISP-A92: Administración de acceso de usuarios.	• Registrar y quitar accesos. Mediante un proceso o herramienta se registra el acceso a la información. • Creación de accesos temporales. Cuando se crea un acceso temporal a servidores, computadoras, aplicaciones o acceso a la red, el acceso se bloquea automáticamente luego de indicar una fecha específica. • Administración de acceso. El control de acceso se realiza a través de un método centralizado de administración. • Resguardo de las contraseñas secretas. Existe un almacén de contraseñas dónde se protegen contraseñas. • Revisión de derechos de acceso. Verificar y consultar en tiempo real los privilegios de lectura y cambio sobre los archivos. • Remover y ajustar los derechos de acceso. Sistema para eliminar accesos de manera directa y en tiempo real.
RISK-06-CON: Robo de códigos fuentes e información de clientes mediante la escalación	CNTRL-06-CON-A82: Clasificación de la información.	• Clasificar la información. Proceso para determinar el nivel de criticidad de los datos o archivos almacenados en servidores y en la nube.

Riesgo	Proceso de control	Subprocesos de apoyo
de permisos realizado por usuarios o aplicaciones.		• Etiquetar la información. Herramienta para clasificar archivos y equipos para clasificar la información. • Proceso de manejo de activos. Lista de activos de la información.
RISK-05-INT: Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.	CNTRL-05-INT-A83: Tratamiento de dispositivos.	• Administrar eliminación de dispositivos y almacenamiento. Proceso para eliminar la información. • Procedimiento para uso de dispositivos y almacenamiento. Lineamiento relacionado al uso de activos de información. • Transferencia física de archivos. Procedimiento para manejar la información.
RISK-03-DIS: Interrupción de los servicios y bloqueo a la información por ataques de denegación, código malicioso o acciones ejecutadas por un agente interno o externo.	CNTRL-03-DIS-A122: Protección contra código malicioso.	• Solución contra código malicioso. Se cuenta con herramientas de identificación y prevención contra código malicioso.

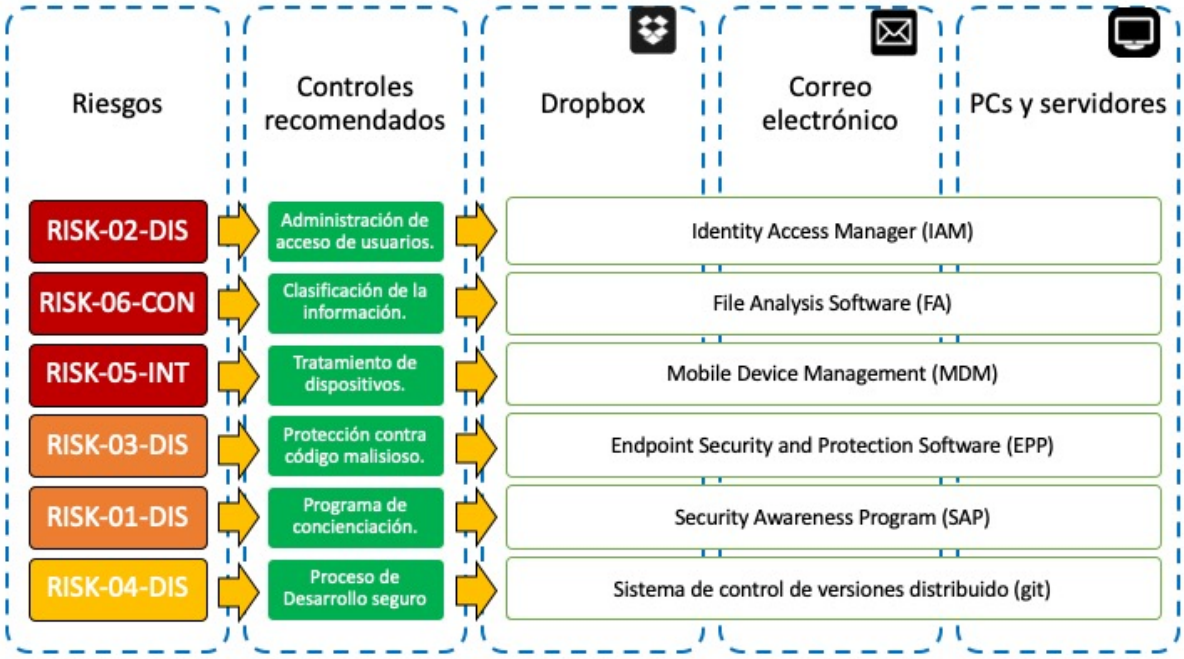
Riesgo	Proceso de control	Subprocesos de apoyo
RISK-01-DIS: Detención de los servicios relacionados a las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.	CNTRL-01-DIS-A81: Responsabilidad en el uso de activos	• Inventario de activos. Lista de activos con la criticidad y tipo de información. • Un responsable por activo. Lista de activos con el responsable de su resguardo. • Uso aceptable de activos y componentes. Lineamiento para el uso apropiado de los activos. • Retorno de activos. Procedimiento para quitar o trasladar responsable de los activos.
RISK-04-DIS: Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.	CNTRL-04-DISP-A142: Proceso de desarrollo y apoyo seguro.	• Política de desarrollo seguro. Existencia de pautas o procedimientos para revisar la calidad y seguridad del código del cliente. • Procedimiento de control de cambios. Se tiene un procedimiento o herramienta para el control de cambios en equipos o equipos sensibles. • Revisión técnica después de cualquier cambio. Se tiene un procedimiento a nivel técnico para el control de cambios en equipos o equipos sensibles. • Restricciones en cambios sobre productos. Manejo de versionamiento y

Riesgo	Proceso de control	Subprocesos de apoyo
		cambios en desarrollo previo a producción. • Principios de desarrollo seguro. Lineamiento de desarrollo seguro para estandarizar todo lo relevante a la generación de código. • Tener un ambiente de desarrollo seguro. Existe un área donde se prueban las funcionalidades, previo la salida a producción. • Monitoreo de las actividades de terceros. Se identifican y monitorean las actividades de terceros sobre la infraestructura interna. • Proceso de desarrollo de pruebas. Se tienen identificadas y documentadas las pruebas que se realizan previa salida a producción. • Proceso de aceptación de pruebas. Existe una persona o herramienta diferente a la persona que ejecuta las pruebas, cuya responsabilidad sea certificar las pruebas.

Nota. La tabla muestra los procesos y los subprocesos de control relacionados a los riesgos encontrados. Tomados del estándar internacional ISO/IEC 27001:2013.

Los procesos de control permiten contar con una primera línea de acción para la gestión de los riesgos. El elegir un proceso en específico facilita la medición del desempeño contra un evento en específico. Este no es el único beneficio. La elección de utilizar una herramienta se vuelve más precisa. Con lo anterior, se plantea un esquema de riesgos, controles y herramientas asignadas a los activos de información sensible. En el siguiente diagrama se puede comprender de una forma más intuitiva como los controles se transforman en herramientas:

Ilustración 7. Diagrama de riesgos, controles y herramientas.



Nota. La imagen indica las categorías de herramientas relacionadas a los controles mitigantes de los riesgos. Tomados de la lista de herramientas en Gartner.

La manera en que se presenta cada una de las herramientas abre la necesidad de identificar el alcance y los requerimientos. Con tal objetivo, se utilizan activos de

información sensible como base para describir los controles. A continuación, se describe cada una de las herramientas que forma parte de la arquitectura final:

- Identity and Access Manager (IAM o IdM): El objetivo principal de esta herramienta es asegurar que solo las personas autorizadas cuenten con el acceso necesario a los recursos correctos en el momento adecuado.
- File Analysis Software (FA): Este tipo de herramienta protege la información utilizando políticas de seguridad y restricciones mediante escaneos sobre archivos, tales como archivos de Microsoft Word, Excel, PowerPoint, entre otros. De esta manera, se clasifica y resguarda la información.
- Mobile Device Management (MDM): Esta herramienta permite aprovisionar, asegurar e incluso administrar los dispositivos móviles, así como, los datos que se encuentran internamente.
- Endpoint Protection Plataform (EPP): Es una solución que se ejecuta en los dispositivos de usuario final y servidores con el fin de prevenir muchos tipos de códigos maliciosos y detectar aplicaciones que no son de confianza para alertar a los responsables.
- Security Awareness Program (SAP): Como su nombre lo indica es un programa de concientización que permite la capacitación y el entrenamiento en temas de seguridad y riesgo.
- Distributed Version Control System (DVCS): Es una solución para administrar de manera completa el código fuente de la organización. Mantiene un histórico de versiones y control de cambios.

Existen seis herramientas en el mercado que pueden apoyar la gestión de los riesgos en la agencia digital. Estas herramientas son conocidas en el mercado, pero

no están presentes en todas las organizaciones, según una encuesta de la empresa consultora Deloitte, en temas de autenticación, solo el 19 % de las organizaciones trabajan en un tema parecido. Sin embargo, el hecho que solo ciertas empresas trabajen con el tema no significa que se puedan considerar para agencias digitales con un número pequeño de colaboradores.

Ilustración 8. Trabajo en temas de gestión de accesos

Nota. La imagen muestra los esfuerzos en las organizaciones relacionados a la gestión de accesos. Tomado de "The future of cyber survey 2019" desarrollada por la consultora Deloitte.

5.2.1 Evaluación de soluciones

Las soluciones recomendadas según el estudio de capacidades provisto por Gartner, Inc. se muestra en el *Anexo D. Evaluación de herramientas por categoría según Gartner* Estas herramientas tratan los riesgos y mejoran los procesos de control. Son las siguientes:

Ilustración 9. Herramientas para procesos de control

Nota. La imagen describe las herramientas seleccionadas para apoyar los procesos de control. Tomado del Anexo D. Evaluación de herramientas por categoría según Gartner

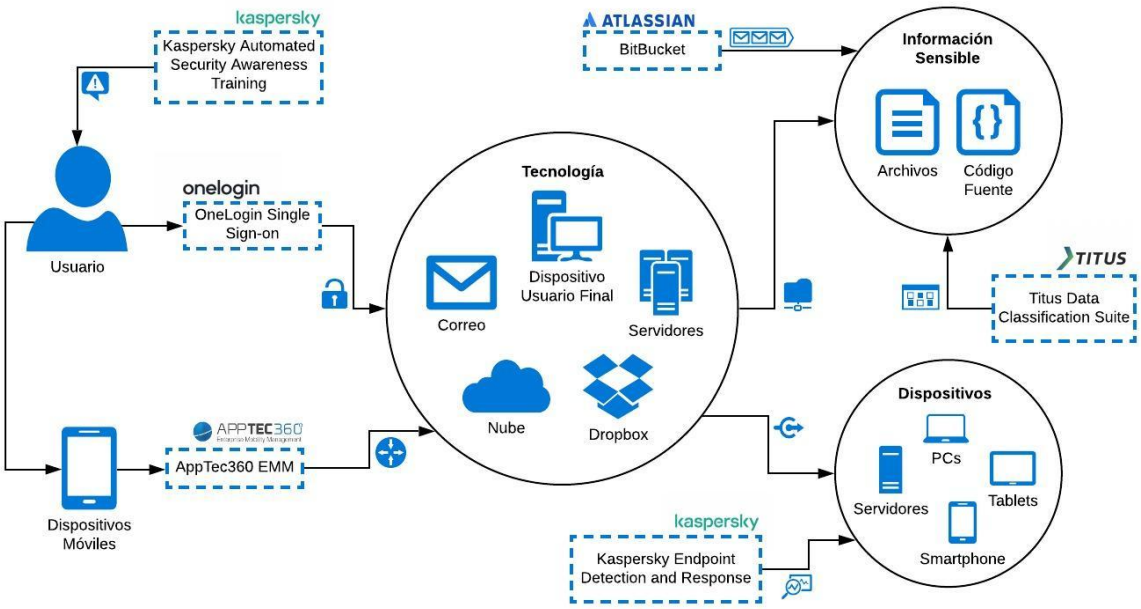
Las herramientas mencionadas proponen una inversión anual de $260.00 dólares por usuario y $38.00 dólares por dispositivo. Estos costos no requieren compra de equipo o recursos de implementación, debido a que cuentan con el soporte (está incluido en el costo de la licencia). Si se comprara la solución con la inversión actual de $168.00 dólares al año por usuario, se tendría un incremento de $92 dólares por usuario y $38.00 dólares por dispositivo.

Sin embargo, el incremento vendría acompañado de una mitigación más orientada a la gestión de riesgos y a una mayor flexibilidad en las operaciones del día tras día por la integración con otros dispositivos móviles.

5.2.1 Arquitectura de la solución recomendada

A continuación, se describe la solución recomendada para la agencia digital con base en un esquema enteramente de soluciones en la nube y orientada a tratar los riesgos descubiertos durante la investigación del proyecto:

Ilustración 10. Arquitectura propuesta para la mitigación de riesgos.



Nota. La imagen indica los controles y su relación con los activos de la información de la agencia digital. Desarrollado en este proyecto como parte de las mejoras en la organización.

La solución está dirigida a fortalecer los procesos de control. Se propone que exista un entrenamiento a los usuarios finales con la herramienta Kaspersky Automated Security Awareness Training con el fin de concientizar y capacitar en temas de seguridad. También, se plantea para los usuarios administrar y controlar su

autenticación utilizando OneLogin Single Sign-On, la cual está mucho mejor ubicada en el mercado que 1Password, la herramienta que actualmente se utiliza.

Para el control total de dispositivos, se implementa el uso de AppTec360 EMM, que, además de ser una herramienta sin costo para empresas de menos de 25 usuarios, está muy bien posicionada en el mercado. Además, existe una necesidad latente de proteger los dispositivos contra código malicioso. Prácticamente, es una urgencia activa en la organización para lo que se sugiere la herramienta de Kaspersky Endpoint Detection and Response (KEDR), la cual es la opción cuyo costo y calidad es más atractiva.

En el caso de la información sensible relacionada con el código fuente, se propone el uso de BitBucket para control de cambios y el proceso de desarrollo. Cabe recalcar que la herramienta ya está siendo utilizada dentro de la organización, por lo cual ya se cuenta con experiencia en su uso. En el caso de todos los tipos de archivos, se propone el uso de Titus Data Classification Suite, una herramienta para clasificar información, de manera que la información sea vista solo por aquellos que realmente la ocupan ver.

5.2.2 Indicadores de desempeño de los controles

Toda implementación relacionada a procesos de control debe ir acompañada de indicadores que aseguren la mejora continua del sistema de gestión. Cada indicador adicionalmente debe contar con el cálculo que se indicó en el punto *3.4 Diseño* del Marco Metodológico. A continuación, se ofrece la lista de indicadores de mejora continua:

Tabla 9. Indicador de acceso de usuarios

IND-001: Acceso de usuarios.	
Proceso de control:	CNTRL-02-DISP-A92: Administración de acceso de usuarios.
Herramienta	OneLogin Single Sign-On
Indicador de cumplimiento	1. **Número de nuevas cuentas.** Con este indicador se lleva un control de cuantas licencias existen y cuántas deben ser renovadas.
Indicador de evaluación	2. **Número de cuentas huérfanas.** Indicador relacionado con el uso de las cuentas. Permite, además, evaluar el desempeño de las herramientas en corporativas en uso.
Indicador de gestión	3. **Número de excepciones en los mecanismos de reconciliación.** Consiste en medir la productividad de la herramienta utilizando “excepciones”. Este término consiste en escenarios dónde no se utiliza la herramienta y se busca solventar de otra manera diferente a la propuesta. Una cantidad importante de excepciones levantaría la alerta de la falta de productividad de la herramienta.

Nota. La tabla contiene los indicadores de desempeño relacionados con el proceso de control de acceso de usuarios. Los indicadores fueron desarrollados a partir de los riesgos.

Tabla 10. Indicador de clasificación de la información

IND-002: Clasificación de la información	
Proceso de control	CNTRL-06-CON-A82: Clasificación de la información
Herramienta	Titus Data Classification Suite
Indicador de cumplimiento	1. **Activos de información confidencial etiquetados**Elementos categorizados e ingresados a la herramienta de clasificación de la información.
Indicador de evaluación	2. **Número de activos con información confidencial no categorizados como tal.** Indicador orientado a evaluar si los activos con información confidencial verdaderamente tienen el trato adecuado.
Indicador de gestión	3. **Número de activos de información sin etiquetar.** Consiste en el número de activos que no se están clasificando.

Nota. La tabla contiene los indicadores de desempeño relacionados con el proceso de control de clasificación de la información. Los indicadores fueron desarrollados a partir de los riesgos.

Tabla 11. Indicador de seguridad de dispositivos móviles

IND-003: Seguridad de dispositivos móviles.	
Proceso de control	CNTRL-05-INT-A83: Tratamiento de dispositivos
Herramienta	AppTec360 EMM
Indicador de cumplimiento	1. **Dispositivos bajo cumplimiento de línea base.** Indicador utilizado para conocer el número de dispositivos que cumplen la línea base del MDM.
Indicador de evaluación	2. **Número de alertas de seguridad registradas sin resolver.** Este indicador se construye con la cantidad total de eventos relacionados con seguridad.
Indicador de gestión	3. **Número de dispositivos sin la herramienta.** Cantidad de dispositivos con la aplicación deshabilitada, borrada o jamás instalada.

Nota. La tabla contiene los indicadores de desempeño relacionados al proceso de control del tratamiento de dispositivos. Los indicadores fueron desarrollados a partir de los riesgos.

Tabla 12. Indicador de eventos de código malicioso

IND-004: Eventos de código malicioso.	
Proceso de control	CNTRL-03-DIS-A122: Protección contra códigos maliciosos.
Herramienta	Kaspersky Endpoint Detection and Response
Indicador de cumplimiento	1. **Dispositivos con la herramienta de EDR.** Son los dispositivos que cuentan con la herramienta instalada y activa.
Indicador de evaluación	2. **Cantidad de infecciones encontradas.** Número de archivos comprometidos por código malicioso.
Indicador de gestión	3. **Número de dispositivos con el EDR desactualizado.** Cantidad de aplicaciones no actualizadas a la última versión oficial.

Nota. La tabla contiene los indicadores de desempeño relacionados al proceso de control de protección contra códigos maliciosos. Los indicadores fueron desarrollados a partir de los riesgos.

Tabla 13. Indicador de concientización de personal.

IND-005: Concientización de personal	
Proceso de control	CNTRL-01-DIS-A81: Responsabilidad en el uso de activos
Herramienta	Kaspersky Automated Security Awareness Training.
Indicador de cumplimiento	1. **Número de personas entrenadas.** Personas que han recibido capacitación y entrenamiento relacionados con seguridad.
Indicador de evaluación	2. **Cantidad de fallos durante el entrenamiento.** Cantidad de errores cometidos por el personal durante las pruebas de ataques hechos por la herramienta de concientización.
Indicador de gestión	3. **Cantidad de eventos de seguridad relacionados al error humano.** Es el número de fallas humanas contabilizadas en los eventos de seguridad. Una cantidad mayor a cinco fallos humanos al año requiere un replanteo en el programa de concientización.

Nota. La tabla contiene los indicadores de desempeño relacionados con el proceso de control de responsabilidad en el uso de activos. Los indicadores fueron desarrollados a partir de los riesgos.

Tabla 14. Indicador de integridad de código

IND-006: Integridad de código	
Proceso de control	CNTRL-04-DISP-A142: Proceso de desarrollo y apoyo seguro.
Herramienta	BitBucket
Indicador de cumplimiento	1. **Cantidad de proyectos protegidos.** Es el indicador que calcula el número de proyectos de BitBucket.
Indicador de evaluación	2. **Número de modificaciones erróneas al código fuente.** Este es el valor de la herramienta relacionado con errores de escritura o borrado de versiones de código fuente.
Indicador de gestión	3. **Número de versiones perdidas en proyectos.** Este indicador cuantifica el número de veces que se ha perdido una sola versión en los proyectos. En otras palabras, la cantidad de veces que se haya tenido que trabajar para reestablecer una versión perdida.

Nota. La tabla contiene los indicadores de desempeño relacionados al proceso de control de desarrollo y apoyo seguro. Los indicadores fueron desarrollados a partir de los riesgos.

Con base en las tablas de descripción de los indicadores, se puede generar la tabla de desempeño de controles que se ve a continuación:

Tabla 15. Indicadores de desempeño para las herramientas de control

Herramienta	Cumplimiento	Evaluación	Gestión
1. OneLogin Single Sign-on	Número de nuevas cuentas	Número de cuentas huérfanas	Número de excepciones en los mecanismos de reconciliación
2. Titus Data Classification Suite	Activos de información confidencial etiquetados	Número de activos con información confidencial no categorizados como tal	Número de activos de información sin etiquetar
3. AppTec360 EMM	Dispositivos bajo cumplimiento de línea base	Número de alertas de seguridad registradas sin resolver.	Número de dispositivos sin la herramienta
4. Kaspersky Endpoint Detection and Response	Dispositivos con la herramienta de EDR	Número de dispositivos con el EDR desactualizado	Cantidad de infecciones materializadas
5. Kaspersky Automated Security Awareness Training	Número de personas entrenadas	Cantidad de fallos durante el entrenamiento	Cantidad de eventos de seguridad relacionados al error humano
6. BitBucket	Cantidad de proyectos protegidos	Número de modificaciones erróneas al código fuente	Número de versiones perdidas en proyectos

Nota. La tabla muestra el resumen de indicadores relacionados con las herramientas y los objetivos de desempeño.

Con los indicadores de control se toman las decisiones concernientes al tratamiento de riesgo. Cada uno de ellos refleja la postura de seguridad de la organización y permite tener una visión integral en el tiempo de las mejoras producidas en las personas, los procesos y la tecnología.

Capítulo 6. Conclusiones y recomendaciones

6.1 Conclusiones

La investigación enfrentó muchos retos durante su ejecución, incluso una pandemia de por medio. Sin embargo, ante situaciones tan transformadoras, se lograron detectar las debilidades de la mayoría de las organizaciones. Por lo tanto, se puede concluir con respecto a los objetivos de este proyecto los siguientes puntos:

- Existen procesos críticos que no estaban visualizados en la agencia digital. En la investigación, se identificó que las funciones críticas no se utilizaban como insumo para toma de decisiones. No todo es crítico, porque las grandes organizaciones conocen que las funciones principales resultan esenciales en relación con las otras funciones facilitadoras de las tareas principales.
- No se tienen mapeados los riesgos asociados los procesos críticos. Si se desea invertir adecuadamente los recursos, se debe iniciar por detectar los vectores que pueden comprometer dichos elementos. En el caso actual, aún existen muchas mejoras en los procesos.
- No existía un costo asociado a cada individuo de la organización relacionado con mantener la seguridad de la información. La seguridad suele mantenerse de lado, debido a que no genera aparentemente un valor económico, pero, conforme pasa el tiempo, las organizaciones notan que este rubro es indiscutible.
- Solo una de las seis herramientas que son sugeridas en esta investigación eran parte de la agencia digital. Este hecho demuestra que existe un nivel de

madurez, pero totalmente dirigido al sentido común, el cual es un riesgo conforme pasa el tiempo.

- Un sistema de gestión de seguridad genera por efecto un aseguramiento del proceso de transformación digital. Al entender los pasos de cambio en la agencia digital, se puede comprobar como los controles no son limitantes del negocio. Más bien, se convierten en facilitadores que proporcionan un apoyo ante cualquier eventualidad.

6.2 Recomendaciones

Una vez finalizada la arquitectura propuesta en esta investigación, se recomienda seguir estos puntos para fortalecer su implementación:

- Mantener un proceso de análisis de impacto de negocio con planes de recuperación contra desastres asignados a los procesos críticos. Los planes de recuperación o DRP, por sus siglas en inglés, consisten en la documentación de las actividades que se deben hacer en caso de un siniestro. Así, contar con ellos es de gran importancia para cualquier empresa tecnológica.
- Iniciar la implementación de las herramientas de control según el orden de criticidad expuesto en el trabajo. El uso de procesos y principios de continuidad de negocio facilitan la priorización de esfuerzos, porque dan una visibilidad muy clara, a todo nivel, de las dependencias directas de negocio.
- Los principios de los indicadores de desempeño se pueden reproducir a otros procesos. Medir el desempeño no solo es un ámbito de seguridad. También,

puede ser homologado cada proceso para lograr una visión de productividad en cada área.

- Establecer fechas de revisión de riesgos y desarrollar el ejercicio según el programa de concientización. Tener puntos en el tiempo, dedicados a visualizar mejoras, es una práctica que las mejores empresas implementan y que les genera resiliencia ante las situaciones más complicadas.

Capítulo 7. Reflexiones

Al partir de una realidad actual donde la seguridad y la protección de los datos cobra mayor relevancia en el desarrollo de las empresas, resulta de interés ofrecer un aporte al cursar la Maestría de Ciberseguridad y específicamente plasmar conocimientos adquiridos en la experiencia del investigador, tanto laboral como educativa, para que sea de provecho para futuras generaciones de profesionales, con el fin de brindar una perspectiva clara de la manera más sencilla de resguardar los pilares de seguridad en las empresas.

Cada conocimiento que se ha ido adquiriendo, se desea potenciarlo al máximo para practicarlo en las labores diarias. Además, se desea motivar a las personas lectoras a fijarse metas constantes para ser palanca en el crecimiento de mejores prácticas, que puedan ser aplicadas con mayor naturalidad en las empresas.

Pero, no todo ha sido bueno. Dentro de esta gran experiencia de búsqueda de conocimiento profesional e interés de seguir adquiriendo conocimiento, se hallaron limitantes. Específicamente, se identificó la falta de anuencia del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICIT) a permitir el desarrollo de un proyecto de posgrado, a través de alguna iniciativa.

En este caso particular, el investigador se encontraba completamente interesado en aportar a esta institución u otra institución pública, porque se consideró conveniente para todos que pueda obtener aportes interesantes constantemente y esta hubiese sido una oportunidad perfecta para ello.

Esta limitante generó sentimientos de tristeza. Se lamenta la frustración del plan por colaborar directamente a una empresa pública, a pesar de la firme intención

e interés mostrados por más de un año con respuestas negativas, que no permitieron el desarrollo de alguna iniciativa por parte del investigador. Ante lo cual, se efectuó el trabajo de estudio en una empresa privada, la cual escuchó la propuesta innovadora y útil para su crecimiento y el del investigador. Se extiende un profundo agradecimiento a Píxel Design de Costa Rica S.A.

Capítulo 8. Trabajos finales

Mediante el desarrollo de esta investigación con la que han podido fortalecer y explorar diversas alternativas en el planteamiento de la seguridad, se han atravesado caminos que permiten un manejo responsable, eficiente y con un impacto mínimo de costos para la organización. Esto ayudará en el futuro a planear de una forma más entendible la gestión de seguridad.

La experiencia de diseñar una arquitectura para un sistema de gestión de seguridad preliminar, en una empresa pequeña, conlleva a enfrentarse con el reto de implementarlo en un ambiente de mayor nivel, específicamente en el actual lugar de trabajo. Adicionalmente, esta investigación es la antesala para elaborar contramedidas e indicadores de desempeño más exitosos.

Para finalizar, el trabajo de seguridad nunca acaba, es indispensable mejorar los procesos de Análisis de Impacto de Negocio y Análisis de Riesgos, así como otros procesos no revisados en la investigación. Interesa mantenerse actualizado en las últimas innovaciones de la tecnología y la seguridad.

Referencias

Anderson, L. W. (2001). A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Boston, MA: Pearson Education Group.

Baca, G. (2010). Evaluación de Proyectos. México: Mc Graw-Hill. Recuperado de https://www.academia.edu/37915939/Gabriel_baca_urbina_evaluacion_de_proyectos_6ta_edicion

Casadesus-Masanell, R. (2004). Dinámica Competitiva y modelos de negocio. Universia Business Review. 4, cuarto trimestre: 8-17

Chapple, Mike (2018). Official Study Guide Eight Edition. Recuperado de https://www.isc2.org/Training/Self-Study-Resources

Harrington, E. (1912). The Twelve Principles of Efficiency. N. Y., The Engineering Magazine Co.

PwC (2018). Digital Trust Insights. Recuperado de https://www.pwc.com/mx/es/servicios-consultoria/ciberseguridad-y-privacidad/digital-trust.html

Sánchez, E. (s.f.). Cómo encriptar y asegurar datos sensibles. Recuperado de http://www.pcactual.com/articulo/zona_practica/paso_a_paso/4374/como_encriptar_asegurar_datos_sensibles.html

Westerman, G., Bonnet, D. y Mcafee, A. (2014). The Nine Elements of Digital Transformation. MIT Sloan Management Review. Recuperado de http://sloanreview.mit.edu/article/the nine elements of digital transformation/

Anexos

Anexo A. Formulario de análisis de impacto de negocio

Sección A: Datos de la compañía

Información general

1	Nombre de la compañía:	Píxel Design Costa Rica S.A.	4	Fecha de elaboración:	30/01/2020
2	Nombre de quién elabora:	Joel Tinoco Torres	5	Tipo de área:	Negocio
3	Área responsable:	Negocio y desarrollo	6	Cantidad de personas en el área:	10-49 personas

Sección B: Funciones del área de negocio

Tabla con los criterios para evaluaciar la funciones principales de negocio.

Principales funciones del área de negocio		Criterios de criticidad					
#	Función	Aquella que genera mayor contacto con el cliente por período específico.	Aquella que genera mayor ganancia para la entidad.	Aquella que posee mayor impacto en los proyectos.	Aquella cuyos impactos podrían ser críticos en el corto plazo si se interrumpe.	Aquella de la cual dependen otras funciones críticas.	Funciones críticas del área de negocio.
1	Recepción de llamadas.						No crítica
2	Realización de propuesta económica y seguimiento cliente.	X	X		X		Crítica
3	Definición de alcance y tiempo de entrega según propuesta aprobada.			X		X	Crítica
4	Revisión de nuevas solicitudes en el proceso de desarrollo para crear nuevas propuestas económicas.						No crítica
5	Cierre y propuesta post-venta.						No crítica

Sección C: Descripción de funciones del área de negocio

FUNICIÓN CRITICA: Realización de propuesta económica y seguimiento cliente.

1. Justificación de la criticidad

¿Por qué es crítica esa función?	La empresa depende de esta función para la generación de clientes nuevos.
¿Qué es crítica en su ejecución?	Recepción de llamada, filtro de cliente, creación de la cotización, realización de reuniones comerciales, asesoría al cliente con los servicios ideales y seguimiento óptimo al cliente.
¿Cuándo es más crítica?	Cuando está un 80% de los recursos de desarrollo y diseño osciosos.
¿Con cuáles áreas de negocio o externos tiene dependencia?	Departamento de Dirección de Proyectos, Departamente Creativo y Departamento de Programación.

2. Objetivo de Tiempo de Recuperación (RTO)

Impacto cualitativo (Operacional)	**¿Por qué hay impacto? (Justificación de impacto)**	Satisfacción, Imagen, Servicio al cliente		
	¿En cuánto tiempo? (Nivel de impacto)	**Inapreciable**	**Moderado**	**Severo**
		De 1 día a 2 días	De 2 días a 4 días	Mayor a 4 días
Impacto cuantitativo (Financiero)	**¿Por qué hay impacto? (Justificación de impacto)**	Porque generamos nuevos proyectos y no hay flujo de efectivo		
	¿En cuánto tiempo? (Nivel de impacto)	**Inapreciable**	**Moderado**	**Severo**
		De 1 día a 2 días	De 2 días a 4 días	Mayor a 4 días
Impacto legal y de obligaciones regulatorias	**¿Conoce si el o los impactos identificados de esta función crítica implican una sanción para la Entidad o sus funcionarios?**			No
	¿Conoce si el impacto identificado de esta función crítica implica un daño a terceros (entidades, acreedores, inversionistas u otros entes relacionados)?			No

3. Objetivo de Punto de Recuperación (RPO)

	¿Cuáles sistemas se requieren que apoyen la función?	
Sistemas para la función crítica	CRM zoho Central Teléfonica VoIP Evernote Pages Whatsapp Dropbox Correos Electrónicos Sicop Firma Digital SAM	
Tiempo de recuperación	**¿Cuánto tiempo tomaría recuperar la información?**	De 8 a 24 horas
Punto de recuperación	**¿En términos de tiempo, cuántos datos se podría perder en caso de un evento de interrupción y donde la dificultad de su recuperación no ponga en riesgo la continuidad de la función?**	De 8 a 24 horas
	¿Por qué?	Ya que su recuperación es fácil o en el peor de los casos se realizan el documento de nuevo para cotizar.

4. Requerimiento de Registros Vitales

¿Qué información (archivo físico (F) o electrónico (E)) es requerida para el desarrollo de la función?

Información para la función crítica	**Información**	**Físico/Electrónico**	**¿Qué tan cambiante es esa información?**	
	Presentaciones de la empresa	Electrónico	5	horas
	Propuestas económicas	Electrónico	3	horas
	Correos electrónicos	Electrónico	20	minutos

	Dada una interrupción, ¿se puede reconstruir la información?	Sí
Reconstru-cción de la información	**¿Cuánto tiempo tarda la reconstrucción?**	8 horas
	¿Cómo se procede para reconstruir la información perdida? ¿A dónde o a quién se acude (papeles, cintas, etc.)?	Dropbox, Correos anteriores, SAN.
	¿Qué tratamiento se tiene para la administración de la información crítica?	Se almacena externamente.
Administra-ción de la información	**¿Cómo se administra?**	Se administra automáticamente y si falla se contacta a un proveedor externo
	¿Se han identificado problemas en la administración?	Si, han ocurrido casos en el inicio de la implementación donde no se carga automáticamente en el SAN y también han ocurrido errores de eliminación de archivos, donde ambas situaciones se han resuelto.

FUNICIÓN CRITICA: Definición de alcance y tiempo de entrega según propuesta aprobada.

1. Justificación de la criticidad

¿Por qué es crítica esa función?	Si esta función no se define correctamente el equipo de trabajo no tiene claridad del proyecto lo cuál repercute en los entregables, tiempos de ejecución por ende en la satisfacción del cliente y el retorno de la inversión.
¿Qué es crítica en su ejecución?	Definir el alcance con sus entregables bajo una línea de tiempo aprobada previamente.
¿Cuándo es más crítica?	En el inicio de cada proyecto (kick-off).
¿Con cuáles áreas de negocio o externos tiene dependencia?	Dirección de Proyectos, Departamento de Programación y Departamento Creativo.

2. Objetivo de Tiempo de Recuperación (RTO)

Impacto cualitativo (Operacional)	**¿Por qué hay impacto? (Justificación de impacto)**	Satisfacción al cliente, Errores de desarrollo, Calidad de los entregables, Compromiso de los recursos internos, Selección incorrecta de recursos.		
	¿En cuánto tiempo? (Nivel de impacto)	**Inapreciable**	**Moderado**	**Severo**
		Menor o igual a 1 hora	De 1 hora a 4 horas	De 4 horas a 1 día
Impacto cuantitativo (Financiero)	**¿Por qué hay impacto? (Justificación de impacto)**	Retorno de la inversión, Retrabajo, Ejecución de Garantías, Oportunidades comerciales perdidas.		
	¿En cuánto tiempo? (Nivel de impacto)	**Inapreciable**	**Moderado**	**Severo**
		Menor o igual a 1 hora	De 1 hora a 4 horas	De 4 horas a 1 día
Impacto legal y de obligaciones regulatorias	**¿Conoce si el o los impactos identificados de esta función crítica implican una sanción para la Entidad o sus funcionarios?**			Sí
	Detalle	Cuando son contrataciones de Gobierno existen multas o garantías a ejecutarse. En caso de algunos proyectos privados también se pueden ejecutar estos procesos pero son muy pocos o casi nulos los que incurren en estos procesos.		
	¿Conoce si el impacto identificado de esta función crítica implica un daño a terceros (entidades, acreedores, inversionistas u otros entes			Sí
	Detalle	Afecta al consorcio cuando se ingresa a un proyecto con esta figura. Además cualquier proyecto que se ejecute incorrectamente afecta a la organización o empresa que nos contrató de forma directa.		

3. Objetivo de Punto de Recuperación (RPO)

	¿Cuáles sistemas se requieren que apoyen la función?	
Sistemas para la función crítica		Teamwork Time Doctor Favro Teamwork Chat Zoom Dropbox SAM Bitbucket Servidores
Tiempo de recuperación	**¿Cuánto tiempo tomaría recuperar la información?**	De 4 a 8 horas
Punto de recuperación	**¿En términos de tiempo, cuántos datos se podría perder en caso de un evento de interrupción y donde la dificultad de su recuperación no ponga en riesgo la continuidad de la función?**	De 8 a 24 horas
	¿Por qué?	Se utilizan los sistemas en la nube y podemos solventar la recuperación.

4. Requerimiento de Registros Vitales

¿Qué información (archivo físico (F) o electrónico (E)) es requerida para el desarrollo de la función?

Información para la función crítica	**Información**	**Físico/Electrónico**	**¿Qué tan cambiante es esa información?**	
	PDF	Electrónico	30	minutos
	Código fuente	Electrónico	2	horas
	Archivos de diseños	Electrónico	20	minutos

	Dada una interrupción, ¿se puede reconstruir la información?	Sí
Reconstru-cción de la información	**¿Cuánto tiempo tarda la reconstrucción?**	2 días
	¿Cómo se procede para reconstruir la información perdida? ¿A dónde o a quién se acude (papeles, cintas, etc.)?	Se utilizan los sistemas actuales de repositorios para solventar la reconstrucción.
	¿Qué tratamiento se tiene para la administración de la información crítica?	Se almacena externamente.
Administra-ción de la información	**¿Cómo se administra?**	De forma manual con cada recurso para poder cargar en repositorios y servidores.
	¿Se han identificado problemas en la administración?	Si, los usuarios pueden incurrir en errores de carga de la información o faltar a los procesos internos de respaldo.

Sección D: Lista de recursos

	E.1 ¿Cuántos recursos?	E.2 ¿En qué condiciones?	E.3 Si ya los poseen, ¿dónde se ubican?
Recurso humano			
Jefes de departamento / Supervisores	2	-	Oficinas Centrales
Personal administrativo	2	-	Oficinas Centrales
Personal interno (sin incluir jefes, supervisores o administrativos)	28	-	Oficinas Centrales
Personal externo	2	-	Externo
Tecnología			
Computadoras	35	Excelentes	Oficinas Centrales
Acceso a las aplicaciones	7	Excelentes	Oficinas Centrales
Teléfono	1	Excelentes	Oficinas Centrales
Fax	0	-	-
Radios de comunicación	0	-	-
Impresoras / Multifuncionales	2	Excelentes	Oficinas Centrales
Televisores	3	Excelentes	Oficinas Centrales
Proyectores	2	Excelentes	Oficinas Centrales
Fotocopiadora	0	-	-
Instalaciones			
Escritorios	Para 35 persona(s)	Bueno	Oficinas Centrales
Espacio de oficinas	Para 40 persona(s)	Excelentes	Oficinas Centrales
Espacio de almacenamiento (m^2)	200 m2	Excelentes	Oficinas Centrales
Espacio para reuniones (m^2)	20 m2	Excelentes	Oficinas Centrales
Servicios de soporte			
Mensajería	Sí	Excelente	Externo
Seguridad física	Sí	Media	Oficinas Centrales
Vehículos	2	Excelente	Oficinas Centrales
Motocicletas	0	-	-

Sección E: Resumen

1. Funciones críticas del negocio

No.	Función	Área de negocio	RTO	Criticidad	Nivel de criticidad
1	Definición de alcance y tiempo de entrega según propuesta aprobada	1	De 4 horas a 1 día	Crítica	Alta
2	Realización de propuesta económica y seguimiento cliente	1	Mayor a 4 días	Crítica	Medio

2. Información sensible

No.	Información	Físico/Electrónico	Lugar de almacenamiento	Promedio de modificación	Reconstrucción
1	Presentaciones de la empresa	Electrónico	Dropbox, email y DDs.	5 horas	8 horas
2	Propuestas económicas	Electrónico	Dropbox, email y DDs.	3 horas	8horas
3	Correos electrónicos	Electrónico	Dropbox, email y DDs.	20 minutos	8 horas
4	PDF	Electrónico	Dropbox, email y DDs.	30 minutos	2 días
5	Código fuente	Electrónico	Dropbox, email y DDs.	2 horas	2 días
6	Archivos de diseños	Electrónico	Dropbox, email y DDs.	20 minutos	2 días

Anexo B. Formulario de análisis de riesgos

Análisis de Riesgo

Principales riesgos derivados de la funciones críticas de la organización

Código	Descripción	Probabilidad		Impacto		Nivel de Riesgo
		Frecuencia	Controles	Función crítica 1. Realización de propuesta económica y seguimiento cliente.	Función crítica 2. Definición de alcance y tiempo de entrega según propuesta aprobada.	
RISK-01-DIS	Detención de los servicios relacionados a las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.	Se podría materializar en menos de 1 mes.	Existen más de dos controles que contengan el riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Intermedio (48)
RISK-02-DIS	Pérdida de la disponibilidad de los servicios relacionados a la definición y finalización de "tiempos de entrega" debido al uso inapropiado de privilegios y accesos.	Se podría materializar en menos de 1 mes.	Existe al menos un control que contenga el riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (90)
RISK-03-DIS	Interrupción de los servicios y bloqueo a la información por ataques de denegación, malware o acciones ejecutadas por un agente interno o externo.	Se podría materializar en menos de 1 mes.	No existe un control relacionado al riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Alto (60)
RISK-04-DIS	Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.	Se podría materializar en menos de 6 meses	Existe al menos un control que contenga el riesgo.	Retrasos en tiempo, pagos o plazos de entrega.	Retrasos en tiempo, pagos o plazos de entrega.	Intermedio (42)
RISK-05-INT	Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.	Se podría materializar en menos de 3 meses	Existe al menos un control que contenga el riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (80)
RISK-06-CON	Robo de códigos fuentes e información de clientes a través de escalación de permisos realizado por usuarios o aplicaciones.	Se podría materializar en menos de 3 meses	No existe un control relacionado al riesgo.	Pérdida de clientes, sanciones económicas o de garantías.	Pérdida de clientes, sanciones económicas o de garantías.	Crítico (90)

Anexo C. Formulario de evaluación de desempeño

Estrategia para atender los controles

RISK-02-DIS		
Descripción del riesgo: Pérdida de la disponibilidad de los servicios relacionados a la definición y finalización de "tiempos de entrega" debido al uso inapropiado de privilegios y accesos.		Crítico (90)
Control		
CNTRL-02-DISP-A92: Administración de acceso de usuarios.	¿Existe control efectivo?	Descripción
Registrar y quitar accesos. A través de un proceso o herramienta se registra el acceso a la información.	Sí	Se utiliza 1Password para control de accesos a servidores solamente
Creación de accesos temporales. Cuando se crea un acceso temporal a servidores, computadoras, aplicaciones o acceso a la red, el acceso se bloquea automáticamente luego de indicar una fecha específica.	No	Nunca realizamos accesos temporales
Administración de acceso. El control de acceso se realiza a través de un método centralizado de administración.	No	Tenemos diferentes accesos y no está centralizado
Resguardo de las contraseñas secretas. Existe un almacen de contraseñas dónde se protegen contraseñas.	Sí	Se utiliza 1Password
Revisión de derechos de acceso. Verificar y consultar en tiempo real los privilengios de lectura y cambio sobre los archivos.	No	No tenemos dicho control
Remover y ajustar los derechos de acceso. Sistema para eliminar accesos de manera directa y en tiempo real	Sí	Se realiza solo con 1Password para servidores y queda pendiente para otras funciones de la empresa

RISK-06-CON		
Descripción del riesgo: Robo de códigos fuentes e información de clientes a través de escalación de permisos realizado por usuarios o aplicaciones.		Crítico (90)
Control		
CNTRL-06-CON-A82: Clasificación de la información.	¿Existe control efectivo?	Descripción
Clasificar la información. Proceso para determinar el nivel de criticidad de los datos o archivos almacenados en servidores y en la nube.	No	Actualmente no se realiza este control
Etiquetar la información. Herramienta para clasificar archivos y equipos para clasificar la información.	No	Actualmente no se realiza este control
Proceso de manejo de activos. Lista de activos de la información.	No	Actualmente no se realiza este control

RISK-05-INT		
Descripción del riesgo: Pérdida de la integridad debido a modificaciones no autorizadas que afecten la entrega de productos.		Crítico (80)
Control		
CNTRL-05-INT-A83: Tratamiento de dispositivos.	¿Existe control efectivo?	Descripción
Administrar eliminación de dispositivos y almacenamiento. Proceso para eliminar la información.	No	Actualmente no se realiza este control
Procedimiento para uso de dispositivos y almacenamiento. Lineamiento para el uso de activos relacionados a la información.	No	Actualmente no se realiza este control
Transferencia física de archivos. Procedimiento para manerjar la información.	No	Actualmente no se realiza este control

RISK-03-DIS		
Descripción del riesgo: Interrupción de los servicios y bloqueo a la información por ataques de denegación, malware o acciones ejecutadas por un agente interno o externo.		Alto (60)
Control		
CNTRL-03-DIS-A122: Protección contra malware.	¿Existe control efectivo?	Descripción
Controles contra malware. Se cuenta con herramientas de identificación, prevención y respuesta a malware.	No	Existen controles a nivel de desarrollo para algunos clientes pero no como una política para todos los proyectos y tampoco a nivel

RISK-01-DIS		
Descripción del riesgo: Detención de los servicios relacionados a las funciones críticas debido a problemas con los dispositivos internos en la agencia digital.		Intermedio (48)
Control		
CNTRL-01-DIS-A81: Responsabilidad en el uso de activos	¿Existe control efectivo?	Descripción
Inventario de activos. Lista de activos con la criticidad y tipo de información.	No	No se tienen estos controles
Un responsable por activo. Lista de activos con el responsable de su resguardo.	No	No se tienen estos controles
Uso aceptable de activos y componentes. Lineamiento para el uso apropiado de los activos.	No	No se tienen estos controles
Retorno de activos. Procedimiento para quitar o trasladar responsable de los activos.	No	No se tienen estos controles

RISK-04-DIS		
Descripción del riesgo: Daño a la imagen, multas y pérdida de garantías debido a problemas en la entrega de servicios.		Intermedio (42)
Control		
CNTRL-04-DISP-A142: Proceso de desarrollo y apoyo seguro.	¿Existe control efectivo?	Descripción
Política de desarrollo seguro. Existencia de pautas o procedimientos para revisar la calidad y seguridad del código del cliente.	No	No existe
Procedimiento de control de cambios. Se tiene un procedimiento o herramienta para el control de cambios en equipos o equipos sensibles.	Sí	Se utiliza bitbucket
Revisión técnica después de cualquier cambio. Se tiene un procedimiento a nivel técnico para el control de cambios en equipos o equipos sensibles.	No	No existe
Restricciones en cambios sobre productos. Manejo de versionamiento y cambios en desarrollo previo a producción.	Sí	Se utiliza bitbucket
Principios de desarrollo seguro. Lineamiento de desarrollo seguro para estandarizar el desarrollo seguro.	Sí	Se utilizan principios a nivel conceptual pero no existe una validación correcta
Tener un ambiente de desarrollo seguro. Existe un área donde se prueban las funcionalidades previa la salida a producción.	Sí	Se tienen 2 ambientes clave de desarrollo y en algunos casos el cliente brinda dicho ambiente
Monitoreo de las actividades de outsourcings. Se identifican y monitorean las actividades de terceros sobre la infraestructua interna.	Sí	Si, pero actualmente no hay control donde se evidencien los procesos y actividades externas
Proceso de desarrollo de pruebas. Se tienen identificadas y documentadas las pruebas que se realizan previa salida a producción.	Sí	Se realiza un checklist, pero no se valida internamente en todos los casos
Proceso de aceptación de pruebas. Existe una persona o herramienta diferente a la persona que ejecuta las pruebas, cuya responsabilidad sea certificar las pruebas.	No	Esta es una faltante muy grave en la empresa

Anexo D. Evaluación de herramientas por categoría según Gartner

Fuente: Gartner, Inc.

1. Identity and Access Manager (IAM o IdM)

Criterios	Peso	1Password	Okta	Microsoft Azure Active Directory	Auth0 Platform	OneLogin Single Sign-on	JumpCloud	SecureAuth Identity Platform	RSA SecurID Access
Registrar y quitar accesos	5	4.7	4.7	4.6	4.4	4.7	4.6	4.3	4.4
Autenticación de usuario	5	4.6	4.8	4.8	4.7	4.6	4.8	4.5	4.7
Integración con Mac y Windows	5	4.4	4.6	4.5	4.4	4.4	4.8	4.3	4.1
Multiple factor de autenticación	5	4.1	4.6	4.5	4.4	4.4	4.5	4.3	4.5
Acceso a evento de ingreso y actividad	5	4.2	4.5	4.5	3.8	4.2	3.9	4.2	4.3
Calidad técnica	5	4	4.4	4.5	4.7	4.5	4.6	4.3	4.5
Calidad del soporte	5	4.1	4.5	4.5	4.3	4.6	4.6	4.2	4.4
Facilidad de implementación	5	4.5	4.5	4.5	4.2	4.5	4.6	4.3	4.3
Precio flexible	5	3.7	4.4	4.3	3.7	4.4	4.6	3.9	4.1
TOTAL	45	38.3	41	40.7	38.6	40.3	41	38.3	39.3
Costo por usuario/año		$96.00	$192.00	$108.00	$0.00	$96.00	$120.00	$24.00	$48.00

2. File Analysis Software (FA)

Criterios	Peso	Varonis Data Security Platform	Netwrix Auditor	Titus Data Classification Suite	Druva inSync	Veritas Data Insight	Data Dynamics StorageX	Spirion
Capacidad del producto	5	4.7	4.5	4.4	4.5	4.8	4.2	4
Fácil integración	5	4.5	4.3	4.2	4.5	4.5	4	4
Soporte	5	4.6	4.4	4.3	4.5	4.3	3.9	4.5
Calidad técnica	5	4.6	4.4	4	4.6	4.5	4	4.5
Integración con Dropbox	5	1	1	4	1	1	1	1
TOTAL	25	19.4	18.6	20.9	19.1	19.1	17.1	18
Costo por usuario/año		$250.00	$379.00	$59.00	$72.00	$34.99	$150.00	$140.00

3. Mobile Device Management (MDM)

Criterios	Peso	Scalefusion	Hexnode MDM	Cisco Meraki Systems Manager	Codeproof	AppTec360 EMM	Jamf Pro (formerly Casper Suite)	Sophos Mobile
Capacidades del producto	5	4.8	4.9	5	4.3	4.5	4.9	4
Administración de dispositivos móviles	5	4.8	4.9	4.9	4.7	5	4.7	3
Administración del APP	5	4.8	4.7	4.8	3.3	4.5	4.6	4
Administración de la seguridad personal	5	4.5	4.6	4.9	4.7	5	4.4	4.2
Soporta multiples usuarios	5	4.6	4.5	5	5	5	4.4	4
Escalabilidad	5	4.6	5	4.9	4.7	4	4.6	4
Arquitectura de nube	5	4.6	4.7	5	4.3	5	4.7	3.8
Soporte remoto	5	4.6	5	4.8	4.3	4	4.6	3.6
Administración de clientes	5	4.8	4.6	4.9	4.7	5	4.7	4
Administración y usabilidad	5	4.8	4.7	5	4.3	4.5	4.7	4.2
Acceso a contenido	5	4.4	4.4	4.9	4	4.5	4.3	4
Soporte por brechas en el dispositivo	5	4.6	4.6	4.9	4.3	4.5	3.9	4
TOTAL	60	55.9	56.6	59	52.6	55.5	54.5	46.8
Costo por endpoint/año		$30.00	$72.00	$40.00 + equipos	$50.00	$0.00 Menos de 25	$84.00	$47.00

4. Endpoint Protection Plataform (EPP)

Criterios	Peso	SentinelOne	Falcon Crowdstrike	Panda Adaptive Defense 360	VMware Carbon Black EDR	Malwarebytes	Kaspersky Endpoint Detection and Response (KEDR)	Windows Defender Advanced Threat Protection	Cybereason Defense Platform
Capacidad del producto	5	4.9	4.9	4.6	4.7	4.7	4.9	4.5	4.7
Detección	5	4.9	4.9	4.6	4.7	4.8	4.9	4.5	4.7
Contención y remediación	5	4.9	4.8	4.6	4.6	4.8	4.8	4.4	4.7
Infraestructura	5	4.9	4.8	4.4	4.5	4.7	4.8	4.4	4.7
Investigación	5	4.8	4.7	4.5	4.8	4.6	4.9	4.4	4.3
Facilidad de integración	5	4.8	4.7	4.4	4.4	4.7	4.8	4.5	5
Soporte	5	4.8	4.8	4.5	4.4	4.7	4.9	4.4	4.7
Calidad técnica	5	4.8	4.8	4.3	4.5	4.6	4.9	4.4	4.5
Precio flexible	5	4.7	4.5	4.5	4.2	4.6	4.9	4.2	4
TOTAL	45	43.5	42.9	40.4	40.8	42.2	43.8	39.7	41.3
Costo por endpoint/año		$45.00	$227.88	$51.99	$30.00	$39.99	$38.00	$72.72	$79.99

5. Security Awareness Program (SAP)

Criterios	Peso	Lucy Security	Proofpoint	Kaspersky Automated Security Awareness Training	Infosec IQ	The Defence Works Security Awareness Training	MyCompliance Cloud	Enterprise Awareness Training Program	Security Awareness & Compliance Training	CyberVista Certify	iLMS
Capacidad del producto	5	4.2	4.5	4.9	4.7	5	4.6	4.6	4.5	5	4.3
Simulación de ataques de phishing	5	4.4	4.5	4.8	4.8	4.9	4.5	4.7	4.6	5	4.3
Calidad de los modulos de entrenamiento	5	4.3	4.7	4.8	4.6	4.9	4.7	4.7	4.8	4.7	4.7
Contenido de los modulos de entrenamiento	5	4.3	4.7	4.9	4.7	5	4.7	4.7	4.8	4.8	4.7
Variedad de contenido	5	4	4.7	4.9	4.6	4.9	4.5	4.6	4.7	4.8	4.8
Calidad de la consola de administración	5	3.9	4.4	4.8	4.6	4.8	4.5	4.6	4.3	5	4.8
Calidad de los reportes	5	4.2	4.3	4.9	4.5	4.7	4.4	4.5	4.2	4.8	4.4
Contenido en español	5	4	4.5	4.5	0	0	0	0	0	0	0
TOTAL	40	33.3	36.3	38.5	32.5	34.2	31.9	32.4	31.9	34.1	32

6. Distributed Version Control System (DVCS o git)

Criterios	Peso	Bitbucket	PTC Integrity	Parasoft Development Testing Platform	ReQtest	Jama Connect	Polarion ALM
Capacidad del producto	5	4.6	4	4	4	4	4
Facilidad de integración con terceros	5	4.2	4	4.5	4	5	3.5
Uso de APIs	5	4.4	4	4.5	5	4	3.5
Calidad de entrenamiento	5	4.4	4	4.5	4	5	3.5
Fácil implementación	5	4.5	4.3	4.5	4	5	4
TOTAL	5	22.1	20.3	22	21	23	18.5
Costo por usuario/año		$72.00	$1,000.00 + otros	$899.00	$540.00	$1,380.00	$0.00 + otros