UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

TESIS PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR
JORGE MARTÍN RODRÍGUEZ CASTRO

ASESOR
Mtro. GREGORIO LEÓN TENORIO

Chiclayo, 2019

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Organizaciones a nivel mundial llevan a cabo sus operaciones mediante el uso de sistemas Web bajo la modalidad de suscripción. A esto se denomina *Software como Servicio* (Software As a Service, SaaS) y su uso se ha extendido y diversificado. Internet, el medio utilizado por las empresas que proveen estos servicios, ha evolucionado, facilitando la vida de las personas y organizaciones, pero es también uno de los entornos más expuestos a ataques y eventos de riesgo.

La gestión de riesgos es un proceso que permite a las organizaciones planificar la forma en que un evento adverso es afrontado, reduciendo así su impacto. El proceso es vital, por lo que este estudio presenta un Modelo de Gestión de Riesgos de Tecnologías de la Información que esté ajustado a las necesidades de empresas que brindan SaaS.

El modelo contempla el análisis del sector y del contexto de la organización, la identificación de los activos, sus amenazas y vulnerabilidades; la valoración de los riesgos y la proposición de planes de tratamiento, así como acciones de seguimiento, control, comunicación y consulta. El modelo formula además un procedimiento para la identificación de las funciones y procesos críticos, sus tiempos de recuperación y sus procedimientos alternos, como apoyo en la continuidad del negocio.

Los instrumentos utilizados fueron sometidos a análisis estadístico, comprobando su confiabilidad. El modelo fue evaluado por expertos, lo que ha permitido demostrar su validez y aplicabilidad como herramienta para la gestión efectiva del riesgo asociado al uso de tecnología.

Palabras clave: riesgo, riesgo de TI, gestión de riesgos, continuidad de negocio.

ABSTRACT

Organizations around the world are performing their operations by using Web systems under subscription models. This operation model is known as Software as a Service (SaaS) and it is widely used. Internet, the mean used by these companies has evolved, making the lives of people and organizations easier, but it is also one of the environments more exposed to attacks and risk events.

The risk management is a process make possible organizations to plan the way a risk event is faced, reducing its impact. This process is vital, and this document presents an Information Technology Risk Management Model that fit the needs for SaaS companies. The model includes the organization context analysis, the identification of the assets, their threats and vulnerabilities; risk assessment and treatment plans, and also monitoring actions, control, communication and consultation. The model formulates also a procedure to identify critical functions and processes, their recovery times and alternate procedures, in order to support the business continuity.

The instruments used were tested by using statistical analysis, demonstrating its reliability. The model was evaluated by experts, demonstrating its validity and applicability as a tool for the effective risk management related with the use of technology.

Keywords: risk, IT risk, risk management, business continuity.

INTRODUCCIÓN

En el ámbito global, de acuerdo al Reporte de Riesgos Globales del Foro Económico Mundial del 2018 (The Global Risk Report 2018 13th Edition – World Economic Forum) tanto los ciberataques como el fraude o robo de datos se encuentran entre sus riesgos con alta probabilidad e impacto. Los ciberataques ocupan el tercer lugar de los top 10 riesgos con mayor probabilidad y el puesto 6 en cuanto a impacto, mientras que el fraude o robo de datos ocupa el puesto 4 en probabilidad. De igual forma, aunque no figura entre los top 10, las fallas en infraestructura de información crítica son un riesgo importante debido a su interconexión con otros aspectos del quehacer humano y la dependencia cada vez mayor de la tecnología. [1]

El informe da cuenta de los graves perjuicios económicos de los ciberataques ocurridos durante el 2017:

> "El impacto financiero de las brechas en ciberseguridad está en crecimiento, y algunos de los enormes costos el 2017 relacionados a ataques de ransomware, que significó cerca del 64% del correo malicioso. Un ejemplo notable fue el ataque WannaCry –que afectó 300000 computadoras en 150 países- y NotPetya, que causó pérdidas por US$300 millones a un número de negocios afectados". [1, p. 6]

Por otro lado, se menciona que el Internet de las cosas (IoT) se va a expandir, de 8.4 billones de dispositivos en el 2017 a 20.4 billones en el 2020: "Lo que alguna vez pensamos que podría ser un ataque a gran escala, en la actualidad se vuelve algo común" [1, p. 15].

Uno de los objetivos del reporte es motivar a los individuos y organizaciones a pensar de forma crítica y creativa acerca de cómo se puede responder rápidamente a un ambiente de riesgo en evolución. [1, p. 53]

Por su parte, Deloitte ha conducido el año 2017 la décima edición de su encuesta global de gestión de riesgo, aplicada a 77 organizaciones del sector financiero mundial y cuyo cuestionario dedica una sección a los sistemas de información para la gestión de los

riesgos y tecnología. El extenso informe describe los siguientes hallazgos clave: los riesgos crecientes de ciberseguridad, las instituciones son menos efectivas al manejar nuevos tipos de riesgos, desafíos significativos planteados por los riesgos de datos y sistemas IT, una batalla por el talento de gestión de riesgos, mayor uso de pruebas de estrés (relacionados a aspectos financieros), creciente importancia y costo de cumplimiento, aumento de la supervisión del directorio, puesto de CRO (Chief Risk Officer) casi universal y, crecimiento estable en la adopción de ERM. [2]

El reporte indica que la adopción de programas para la gestión de riesgos se ha extendido a nivel mundial:

> "73% de instituciones que reportan que cuentan con un ERM. Adicionalmente, otro 13% de instituciones indicó que están actualmente implementando un programa de ERM, mientras que el 6% indicó que planean crear uno en el futuro.
>
> Los programas ERM son más comunes en los Estados Unidos, Canadá (89%) y Europa (81%), conducido principalmente por regulaciones, más que en Asia Pacífico (69%) o Latinoamérica (38%). Sin embargo, 50% de los encuestados indicó que su institución está actualmente implementando un programa de ERM." [2, p. 26]

Desde el punto de vista de la tecnología utilizada en la gestión de riesgos, el reporte refiere:

> "Muchos encuestados tienen preocupaciones significativas acerca de la agilidad de sus sistemas de información en la gestión de riesgos en sus instituciones. Casi la mitad de los encuestados están extremadamente o muy preocupados acerca de la adaptabilidad de la tecnología con respecto a los riesgos debido a los cambios en las regulaciones (52%), sistemas antiguos o arquitecturas adecuadas (51%), falta de flexibilidad para ampliar los sistemas existentes (48%) y falta de integración (44%)." [2, p. 56]

El estudio revela además que son justamente las presiones regulatorias las que fuerzan a las organizaciones a mejorar su gestión y estrategia de riesgos de datos. Eso explica por qué en Norteamérica (44%) y Europa (33%) los encuestados consideran que su

organización es efectiva en almacenes de datos, comparado con Asia Pacífico (17%) y Latinoamérica (0%) [2, p. 56]

> El estudio concluye: "Las instituciones que reducen sus inversiones en gestión de riesgos podrían descubrir que no pueden ajustar con facilidad sus capacidades si nuevos requisitos son impuestos. Muchas instituciones han encontrado incluso que los nuevos requerimientos regulatorios han creado una nueva normalidad y un nuevo conjunto de expectativas en la industria, y que no esperan que esto cambie." [2, p. 57]

En el Perú, como casi en toda Latinoamérica la gestión de riesgos es aún una tarea pendiente en muchas organizaciones, principalmente en aquellas que no están sujetas a regulación o quienes estando sujetas a un sistema regulatorio no lo cumplen totalmente. En el ámbito de las tecnologías de información y en específico en el ámbito de la gestión de proyectos de TI existen estudios desde hace ya varios años que dan cuenta de la falta de gestión de riesgos y controles para mitigarlos. Un estudio del año 2008 de la Universidad Nacional Mayor de San Marcos conducido por el ingeniero Javier del Carpio analiza la gestión de riesgos en proyectos de TI en sectores como manufactura, banca, comunicaciones, instituciones académicas, gobierno, consultoría y servicios, entre otros. De acuerdo al estudio sólo el 43% de las organizaciones encuestadas implementan políticas de gestión de riesgos para proyectos de TI pero dichas políticas tenían una antigüedad de 3 años o más y de los cuales el 46% no disponía de los recursos para conducir el proceso. En la misma tendencia, el 59% de las organizaciones no utilizaban herramientas en el proceso de gestión. [3]

EY (antes Ernst & Young) lanzó la encuesta "Gobierno, Riesgo y Cumplimiento 2015" para analizar la situación en la que se encontraban las instituciones con respecto a la gestión del riesgo. Numa Arellano, socio de consultoría de EY, publicó en el 2016 un artículo citando algunos hallazgos:

La encuesta muestra que el 58% de las empresas peruanas encuestadas no cuenta con una gerencia de riesgos, mientras que del 42% restante, solo un 9% le reporta funcionalmente al directorio o a alguno de sus comités (e.g., comité de riesgos o de auditoría).

El 77% de los empresarios encuestados indicó que evalúa el perfil de riesgo de sus organizaciones de forma anual, de manera que no tienen capacidad óptima de respuesta frente a cualquier riesgo que se le pueda presentar a la empresa esporádicamente.

Otro hallazgo relevante de la Encuesta GRC 2015, tanto en el Perú como a nivel global, es la falta de coordinación en los esfuerzos de gestión de riesgos (históricamente esta es una tarea que ha pasado de mano en mano entre áreas específicas de la empresa), así como la falta de un diseño de procesos en estos. Este hallazgo se ve claramente en el caso peruano donde solo el 27% de los encuestados considera que la función de GRC se encuentra bien coordinada entre las diferentes áreas de la organización. No obstante, es auspicioso saber que el 58% se proyecta a que sus actividades de riesgo dentro de las empresas estén bien coordinadas dentro de próximos tres años. [4]

Arellano concluye afirmando:

> "En esta perspectiva, la Encuesta GRC 2015 nos muestra que las organizaciones están buscando un enfoque más amplio, coordinado e innovador para gestionar exitosamente las oportunidades y retos que generan los riesgos. Esto requiere una transformación en la manera en la que la organización gestiona sus riesgos. Es necesario construir una organización "consciente" de los riesgos. Sin riesgo, no hay recompensa." [4]

A nivel local, un estudio realizado por docentes de la Universidad Católica Santo Toribio de Mogrovejo en el año 2016 titulado "Modelo de gestión de riesgos de TI para procesos que contribuyen a la generación de valor en la universidades privadas" da cuenta que 6 de las 11 universidades que fueron materia del estudio no implementan gestión de riesgos o la implementan de manera poco efectiva, haciendo notar además que hay una falta incluso de conocimiento de los conceptos de gestión de riesgos de TI, incluso a nivel de la gerencia de TI de dichas organizaciones. Esto conduce a la toma de respuestas reactivas frente a situaciones adversas con la posibilidad de generar pérdidas económicas y afectación de la imagen institucional. [5]

Este trabajo de investigación será aplicado en una empresa que ofrece software como servicio (SaaS). Con sede en Londres, esta empresa brinda servicios en dos rubros

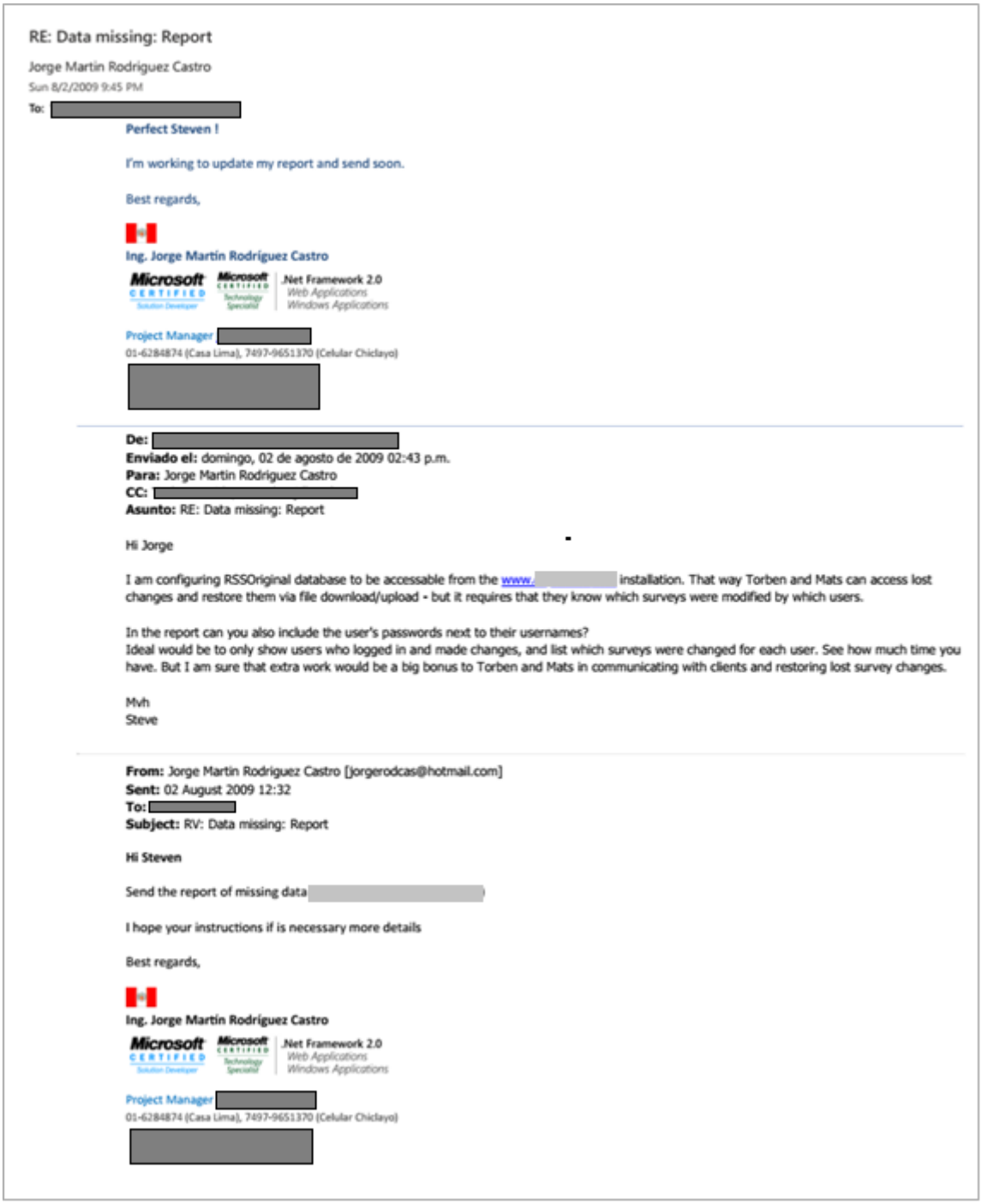
específicos: a). diseño, distribución y procesamiento de encuestas; b). diseño, distribución y procesamiento de boletines electrónicos (newsletters & email marketing).

La empresa tiene 16 años en el mercado y brinda sus servicios a través de aplicaciones web en Internet bajo la modalidad de suscripciones.

Su sede principal en Londres opera físicamente bajo la modalidad de co-working (espacio de trabajo compartido) es decir, el edificio alberga también a otras empresas y emprendimientos. Casi todos los empleados trabajan de forma remota pues viven en distintos países: Dinamarca, Suecia, Bulgaria, Polonia y Perú.

La empresa enfrenta varios problemas asociados a los riesgos propios de su modelo de negocio y forma de operación.

Uno de los problemas más críticos son los ataques que la empresa ha tenido a los activos de información en los últimos 10 años. El primero ocurrió en el año 2009 y fue un ataque contra la base de datos de uno de los sistemas a través de la inyección SQL. El segundo, a inicios de 2018 fue un ataque distribuido de denegación de servicio (DDoS, por sus siglas en inglés) al servidor donde se encuentran los sitios Web (servicio tercerizado). En el primer caso, se tomaron acciones correctivas decididas en ese momento (respuesta reactiva). En el segundo caso, la empresa de hosting aplicó las medidas correctivas. Esto trajo como consecuencia la pérdida de información, y se afectó la confianza por parte de nuestros clientes, la interrupción de las operaciones y en cierta medida se puso en riesgo la continuidad del negocio, además de las pérdidas económicas estimadas en alrededor de US$2500 dólares. Como evidencia, las siguientes imágenes muestran mensajes de correo sobre ambos incidentes. En el primer caso, un hilo de conversación donde se discute el proceso de recuperación luego del incidente; en el segundo, la notificación de la empresa de hosting acerca del evento detectado:



RE: Data missing: Report

Jorge Martin Rodriguez Castro
Sun 8/2/2009 9:45 PM
To: [redacted]

Perfect Steven !

I'm working to update my report and send soon.

Best regards,

Ing. Jorge Martin Rodriguez Castro
Microsoft CERTIFIED Solution Developer | Microsoft CERTIFIED Technology Specialist | .Net Framework 2.0 Web Applications Windows Applications
Project Manager [redacted]
01-6284874 (Casa Lima), 7497-9651370 (Celular Chiclayo)
[redacted]

De: [redacted]
Enviado el: domingo, 02 de agosto de 2009 02:43 p.m.
Para: Jorge Martin Rodriguez Castro
CC: [redacted]
Asunto: RE: Data missing: Report

Hi Jorge

I am configuring RSSOriginal database to be accessable from the www.[redacted] installation. That way Torben and Mats can access lost changes and restore them via file download/upload - but it requires that they know which surveys were modified by which users.

In the report can you also include the user's passwords next to their usernames?
Ideal would be to only show users who logged in and made changes, and list which surveys were changed for each user. See how much time you have. But I am sure that extra work would be a big bonus to Torben and Mats in communicating with clients and restoring lost survey changes.

Mvh
Steve

From: Jorge Martin Rodriguez Castro [jorgerodcas@hotmail.com]
Sent: 02 August 2009 12:32
To: [redacted]
Subject: RV: Data missing: Report

Hi Steven

Send the report of missing data[redacted]

I hope your instructions if is necessary more details

Best regards,

Ing. Jorge Martin Rodriguez Castro
Microsoft CERTIFIED Solution Developer | Microsoft CERTIFIED Technology Specialist | .Net Framework 2.0 Web Applications Windows Applications
Project Manager [redacted]
01-6284874 (Casa Lima), 7497-9651370 (Celular Chiclayo)
[redacted]

Figura 1. Hilo de conversación sobre el proceso de recuperación de datos post-ataque por inyección SQL.

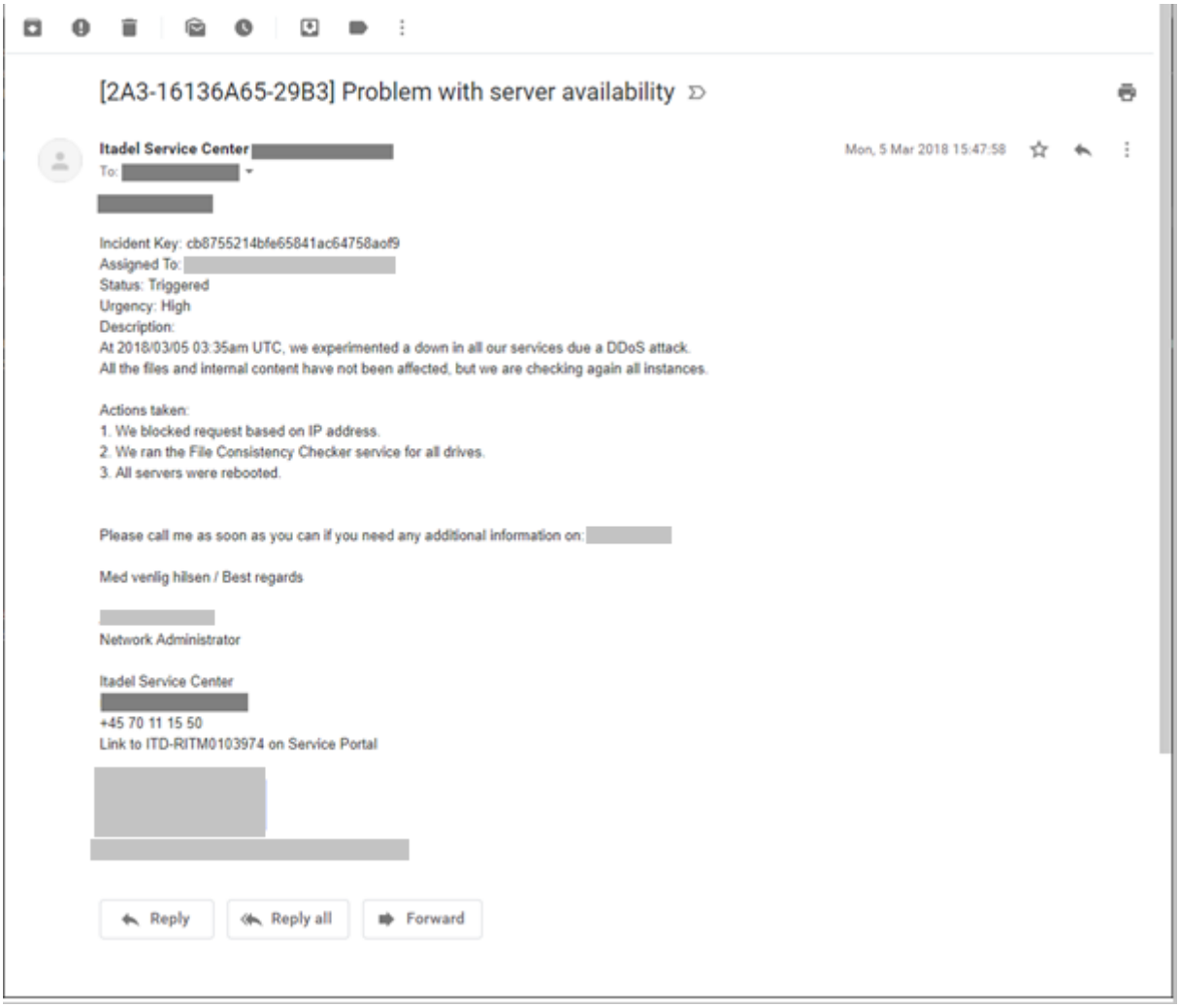


Figura 2. Notificación del servicio de Hosting sobre ataque DDoS detectado.

Por otro lado, los procedimientos de control de cambios en las aplicaciones Web han ocasionado que se modifiquen archivos de código fuente que ya habían sido previamente modificados por otra persona, sin un registro o sistema de control de código fuente donde se pueda identificar al responsable, las acciones realizadas o en qué momento se llevaron a cabo dichas modificaciones. Esto ha ocurrido por lo menos 8 veces en los últimos dos años y ha traído como consecuencia problemas entre el personal pues el tiempo invertido en una actualización se ve perdido por este tipo de acciones. Otra consecuencia es la inestabilidad que se genera en los sitios Web y en las aplicaciones.

Por otro lado, existe un acceso irrestricto a los servidores de producción por parte de varios empleados de la empresa al no contarse con políticas que definan perfiles de

acceso. Esto constituye un riesgo potencial constante para la empresa, pues si bien es cierto que hasta el momento no ha ocurrido ningún incidente, debe garantizarse la seguridad de los activos más importantes de la empresa; más aún cuando son las políticas las que permiten adoptar las acciones a aplicar desde el punto de vista técnico.

Las copias de seguridad son generadas sin la aplicación de algún mecanismo que restrinja su restauración; esto es, sin aplicar algún tipo de encriptación a los archivos generados, o contraseñas o algún otro medio que asegure la confidencialidad de las copias de seguridad. La potencial consecuencia de esta práctica es la filtración de la información pues bastaría restaurar la copia de seguridad y la información estaría disponible.

El acceso a la red privada virtual se hace mediante el uso de cuentas de acceso proporcionadas por un tercero (la empresa proveedora de la VPN). La organización no ha adquirido cuentas de acceso para todo el personal bajo la justificación que algunos empleados no requieren tener una conexión permanente a la red; por esto, es práctica común que más de un usuario haga uso de una misma cuenta para el acceso a la red privada virtual, lo que les da a su vez acceso a los servidores. Aunque no se han suscitado incidentes negativos, esta práctica se contrapone a las medidas mínimas de seguridad que deberían tenerse con respecto al acceso a los activos de la empresa, para los cuales, la identificación del usuario es un factor de suma importancia.

Varias de las operaciones que tienen que ver con modificaciones de datos no tienen pistas de auditoría, es decir, no se guarda información acerca de quién llevó a cabo dichas acciones ni bajo qué circunstancias. Cuando ocurre algún problema relacionado con los datos es difícil o no es posible poder determinar la responsabilidad de dichas acciones. Se han suscitado al menos dos problemas con clientes el año pasado, quienes refirieron que los datos de sus clientes no eran los correctos o que la programación de sus distribuciones habían sido alteradas, no pudiéndose determinar las circunstancias ni el agente que llevó a cabo dichas alteraciones. En ambos casos se corrigieron los problemas pero esto genera un impacto negativo en la imagen de la empresa y la pérdida económica ocasionada en la utilización de recursos para restablecer la información original fue de aproximadamente 600 dólares.

Como toda organización apoyada en la tecnología, los medios de comunicación más frecuentes utilizados en la organización son el correo electrónico, el chat y las llamadas vía Skype. El problema se suscita cuando se hace uso de estos medios para enviar información sensible o credenciales, tanto de la organización como de los clientes, sin las medidas de seguridad pertinentes. Esto ocurre con cierta regularidad, principalmente durante la corrección de errores o asistencia a los clientes. Esto constituye un riesgo potencial de seguridad y podría ocasionar que la empresa sea víctima de robo de información dada la exposición de datos confidenciales.

El desarrollo de nuevas aplicaciones es un proceso cuyas actividades son conocidas y llevadas a cabo por el personal involucrado, pero hay ocasiones en las que se establecen límites de tiempo de entrega cortos y se sacrifican actividades, como la documentación. El problema crece cuando no es posible documentar los nuevos desarrollos, incluso luego de haberse finalizado pues hay otras tareas prioritarias que atender. Esta mala práctica tiene ya varios años y la documentación de las aplicaciones existentes es escasa. Anualmente, se llevan a cabo 40 nuevas tareas de desarrollo, aproximadamente. Las consecuencias se evidencian cuando se quiere dar mantenimiento a las aplicaciones existentes y no se cuenta con la documentación requerida, lo que implica a su vez la utilización de mayor tiempo, pues es necesario analizar y entender qué se implementó en su momento y cómo se hizo a fin de poder efectuar el mantenimiento correspondiente.

Los citados anteriormente son sólo algunos de los problemas con los que la organización se enfrenta en su operación diaria y la situación problemática descrita hace evidente la necesidad de contar con un modelo de gestión de riesgos que pueda aplicarse en la organización a fin de minimizar su impacto, apoyar la continuidad del negocio y otorgarle valor a la compañía.

Lo expuesto nos lleva a formular el problema: ¿De qué manera la continuidad del negocio puede ser apoyada en una empresa que brinda software como servicio?
La respuesta a este problema es que la implementación de un modelo de gestión de riesgos de tecnologías de la información permitirá apoyar en la continuidad del negocio en una empresa que brinda software como servicio, lo que a su vez persigue el cumplimiento de objetivos concretos, como:

- El establecimiento de un modelo para la gestión de riesgos de TI que armonice o conjugue criterios guías de estándares, modelos y normas vigentes y reconocidas.
- La determinación de un procedimiento para la identificación de los procesos críticos de TI que contribuyen a la continuidad del negocio.
- La formulación de una estrategia de capacitación y concientización del personal de la organización con respecto a los riesgos de TI, su prevención y tratamiento.
- La validación del modelo propuesto en base a los estándares adoptados para certificar su aplicabilidad y contribuir así en los procesos de las empresas que brindan software como servicio.

La presente investigación se justifica en el aspecto económico pues la gestión efectiva de riesgos y su mitigación genera ahorro de costos ante la ocurrencia de un incidente. Por otro lado, la gestión de riesgos contribuye a cautelar los activos y procesos críticos de la organización que hacen posible que el negocio opere con normalidad, trayendo no sólo estabilidad económica sino también prosperidad.

Se justifica también en el aspecto tecnológico por la propuesta de implementación de un modelo de gestión de riesgos de tecnologías de la información en base a la armonización de estándares y guías ampliamente reconocidas y aceptadas por la industria. La empresa basa sus operaciones y servicios en las tecnologías de la información, abarcando infraestructura física, sistemas de información y datos.

Respecto a los dos aspectos mencionados, es oportuno citar a Ramírez, A., Ortiz, Z. (2011) quienes manifiestan:

> "El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico." [6]

Se justifica en el aspecto social pues el personal será concientizado acerca de la importancia de la gestión de riesgos de TI en la organización y permitirá que adopten una

actitud proactiva frente al riesgo, no sólo en el ámbito laboral sino en cualquier actividad diaria. Por otro lado, una empresa que gestiona sus riesgos da una imagen más sólida y de confianza a la sociedad, aspectos claves para garantizar la tranquilidad de las personas de quienes se gestiona información.

Se justifica en el aspecto personal pues este trabajo es una forma de contribuir con la organización y demostrar que el compromiso con ella va más allá del cumplimiento de los deberes como empleado. Todo esfuerzo adicional que como trabajador pueda llevar a cabo para contribuir al mejoramiento de la empresa contribuirá también a la satisfacción de los directivos, colegas y clientes, al mejoramiento del clima laboral y la estabilidad de la organización. Finalmente, poder aportar con esta investigación al desarrollo académico de la región y del país.

CAPÍTULO I. MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

María Fernanda Molina Miranda [18] identifica las amenazas que afectan a los activos de forma directa o indirecta. El trabajo hace un análisis de riesgo tecnológico de orden cualitativo y no involucra aspectos financieros en el estudio y describe la organización física de la institución a través de sus 5 campus, las instalaciones físicas y características de seguridad de la Gerencia de Tecnologías y Sistemas de Información, ubicada en al campus principal. Asimismo, se indica que la GTSI no cuenta con políticas formales de seguridad, administración de cuentas, acciones contra incidentes, detección de intrusos, entre otros, y no cuenta con un responsable de la seguridad de la información. El trabajo ha permitido conocer el nivel de madurez de la seguridad aplicada en la institución, así como sugerir los controles necesarios para la reducción de los niveles de riesgo e impacto; además, se ha desarrollado el plan de seguridad (política de seguridad + plan de ejecución). El trabajo hace un análisis de los riesgos de la Gerencia de Tecnología con énfasis en la seguridad de la información y utiliza ISO 27001 para plantear una lista de salvaguardas basada en amenazas generales y no cubre aquellas relacionadas a robo de información, filtración de datos, protección de datos, ciberataques, etc., que son temas recurrentes en la actualidad.

Paulino Meléndez [19] describe inicialmente la situación de las empresas de manufactura mexicanas a través de los años con respecto al nivel de certificación que tenían de la norma ISO 9001. Los problemas detectados en el sector de manufactura van desde el nivel de eficacia que tienen las empresas, el cual en su mayoría llega al 50%; además, la mayoría de empresas toman acciones correctivas en lugar de preventivas ante la ocurrencia de incidencias. El estudio plantea la necesidad de proponer un modelo de gestión de riesgos, debido a que la nueva versión de la norma ISO 9001:2015 ya considera en su requisito 6.1: "acciones para abordar riesgos y oportunidades". Uno de los estándares considerados por el autor es la utilización de la norma ISO31000:2009 para la evaluación y gestión de los riesgos, pero como una base para la formulación de un modelo de gestión propio, pues

considera a la norma como genérica. Se considerarán los aspectos metodológicos de este estudio y algunas herramientas de levantamiento de información que resultan de utilidad.

Tres investigadores de Indonesia [20] destacan la importancia de la unidad de Service Desk como un punto central de contacto de los usuarios cuando ocurren interrupciones en el servicio, solicitudes de servicio y solicitudes de cambio. Este estudio se enfoca en los riesgos asociados a procesos de TI, más que en riesgos de los activos de TI, debido a la escasez de estudios con esta orientación. Este estudio hace uso de Cobit 5 for Risk y se enfoca en los procesos DSS02 (Manage Service Request and Incidents) y APO12 (Manage Risk). El trabajo ha sido dividido en tres fases: recolección de datos (mediante entrevistas, revisión documental y observación) que tiene como resultado la lista de riesgos; la segunda fase de análisis de datos, cuyo resultado son los eventos de riesgo (que consiste en una lista de tipos de riesgo, categorías, factores externos e internos); y la tercera fase de análisis de riesgos que tiene como resultado la obtención de la evaluación de los riesgos con sus planes de mitigación. El resultado de la investigación encontró que la mayoría de los riesgos está en la categoría de operaciones del personal con experiencia y destrezas en TI, por lo que las actividades fueron mapeadas al proceso DSS01 de Cobit: Gestión de Operaciones, y a APO07: Gestión del Recurso Humano. El estudio concluye con la recomendación de reestructurar el área a fin de optimizar la implementación de este proceso del negocio, más aún cuando las funciones principales de dicha área no han sido completamente especificadas. Dos aspectos de este trabajo que servirán de base para esta investigación son: el enfoque de evaluar los riesgos de un proceso de TI en lugar de un activo; y el detalle con que se hizo la evaluación de los riesgos y los resultados obtenidos en cada fase.

Caballero y Kuna, en Abril del 2018 realizan el análisis y gestión de riesgos en proyectos de software [25] con la finalidad de proponer un método ágil y de bajo costo que pueda ser implementado por empresas de bajo presupuesto, haciendo uso de la metodología SEI CRM y Magerit v3. La investigación finalizará con la obtención de una herramienta software para la gestión del método propuesto. Este trabajo servirá como fuente a esta investigación al hacer uso de la metodología Magerit en su más reciente versión.

Celi Arévalo, en un estudio realizado el año 2016, sobre la gestión de riesgos de TI y la efectividad de los sistemas de seguridad de información [26] da cuenta del nivel de

superficialidad con que las instituciones llevan a cabo su evaluación de riesgos y cómo generan sus perfiles de riesgo. La investigación propone además el establecimiento de un modelo para la gestión de riesgos operativos de TI como parte del SGSI pues refiere que de acuerdo a Basilea II el riesgo operacional ha desplazado a los riesgos de crédito y mercado como foco de interés para este tipo de organizaciones. El estudio precisa además la importancia de generar perfiles de riesgo que cumplan tres criterios básicos: implantación eficaz de TI, procesos de gobierno y cultura sobre el riesgo. El resultado fue la implementación del modelo de gestión de riesgos de TI, se logró disponer de un registro de los activos y demuestra que la metodología permite obtener información valiosa para la toma de decisiones. El aporte para esta investigación se centra justamente en el establecimiento de un modelo de gestión de riesgos de TI.

F. Valencia, C. Marulanda y M. López presentan el 2016 un trabajo de investigación que establece los aspectos diferenciadores entre lo que es gobierno y gestión de riesgos de TI en comparación al riesgo organizacional [27]. Este estudio manifiesta que las normas, como ISO 38500:2008, marcos de referencia como COBIT, y las diversas metodologías para la gestión del riesgo presentan similitudes en sus contenidos y estructuras, siendo el objetivo del estudio presentar las diferencias entre el riesgo de la organización y el riesgo de TI, principalmente en dos aspectos: los activos y el impacto. El estudio aporta una clasificación de activos en doce capas y evalúa su impacto en función de los tres pilares de la gestión de la información: confidencialidad, integridad y disponibilidad. El citado trabajo resulta de especial interés para esta investigación pues es clave diferencias los ámbitos de acción de la gestión del riesgo (organizacional y de TI) a fin de delimitar el alcance del estudio.

El trabajo de investigación presentado el 2018 por García, Huamaní y Loparte [28] propone un modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. Este estudio hace uso de los estándares ISO/IEC 27005 y la metodología OCTAVE-S y añade un enfoque cuantitativo para el cálculo del riesgo residual basados en los controles establecidos como parte de la aplicación del modelo. La aplicación de este modelo logró reducir el riesgo en la empresa objeto de estudio en un 53% y creó una lista de 17 indicadores a fin que la empresa pueda verificar el cumplimiento de los controles. Aunque este estudio hace uso de la metodología OCTAVE se tomará en cuenta pues

desarrolla un modelo de gestión de riesgos de seguridad de la información con base en el estándar ISO/IEC 27005.

Torcoroma, Castro y Pérez, en un estudio realizado el año 2015, presentan una investigación para la formulación de un modelo de gestión de riesgos en proyectos con una aproximación a los proyectos de TI [29] basándose en el ciclo PHVA (planificar, hacer, verificar y actuar) y en el marco de trabajo de Cobit 4.1, la metodología PMBOK, así como en diversas normas técnicas colombianas, basadas a su vez en estándares como ISO 31000, ISO 27001, ISO 27002 e ISO 27005. Como parte del estudio se define el plan estratégico de TI basado en Cobit 4.1 (PO1, PO9 y PO10) y se implementó PMBOK para la gestión de proyectos. El modelo de gestión de riesgos planteados se enfocó en los tres niveles: estratégico, táctico y operativo. Este trabajo aporta a la investigación pues ofrece una vista general o de alto nivel del alcance de un modelo de riesgos con un enfoque más integral.

El año 2017, tres investigadores de la Universidad de Cuenca, Ecuador, presentan un trabajo de investigación que propone el establecimiento de una metodología ágil para la gestión de riesgos informáticos [30]. Este estudio basa tu desarrollo en las normas ISO 31000 e ISO 27005 y propone una metodología cuya aplicación estuvo respaldada por el uso de diversas herramientas. Esta metodología utiliza como base el modelo PDCA con la finalidad de establecer un proceso de gestión enfocado en la mejora continua, y agrega mejoras y recomendaciones de otras guías y metodologías como: ISO 27001, ISO 27002, MAGERIT e ITIL. La aplicación de la metodología permitió identificar 201 activos en una empresa industrial de alimentos, de los cuales casi el 60% fueron identificados –en términos de seguridad- como "alto". Se identificaron además los riesgos (30 en total) y se generó un plan de tratamiento. Se toma en consideración este estudio por la integración de diversos estándares y como referencia para una comparativa con metodologías más formales, como Magerit.

La evolución de la cultura de gestión de riesgos en el entorno empresarial colombiano es un estudio presentado el año 2016 por tres docentes investigadores de una universidad colombiana [31]. Este estudio brinda un panorama de la gestión de riesgos y la cultura respecto a este concepto. Se abordan aspectos asociados al manejo del nivel de incertidumbre y destaca la importancia de la gestión de riesgos. Se revisan y analizan los estándares y metodologías actuales a fin de analizar e identificar riesgos corporativos. El

estudio presenta un cuadro que resume la documentación actual existente sobre gestión de riesgos corporativos y hace un análisis de cómo se lleva a cabo la gestión de riesgos en el entorno colombiano. Aunque este estudio corresponde a otro país, será tomando en consideración como parte de la cultura general sobre gestión de riesgos y sobre la realidad de un país vecino al respecto.

1.2 Base Teórico-Conceptual

1.2.1 La gestión de riesgos

La frase "gestión de riesgos" es un oxímoron, es decir, figura lógica que consiste en usar dos conceptos de significado opuesto en una sola expresión, que genera un tercer concepto. Aunque "gestión de riesgos" es el término que utilizamos, lo que estamos haciendo realmente es establecer un proceso para la toma de decisiones o elecciones que, se espera, darán como resultado una disminución del nivel de riesgo. [7]

La palabra riesgo tiene sus raíces en la vieja palabra francesa risqué, que significa "peligro, en el cual hay un elemento de oportunidad". [7, p. 1]

Los hitos históricos son de ayuda para ilustrar su evolución. La gestión de riesgos moderna se inició después de 1955. Desde los inicios de los años 70, el concepto de gestión de riesgos financieros evolucionó considerablemente. De manera notable, la gestión del riesgo ya no se limita solamente al mercado de los seguros, ahora es considerada una herramienta de protección que complementa otras muchas actividades de la gestión del riesgo. Luego de la Segunda Guerra Mundial, grandes compañías empezaron a desarrollar auto-seguros contra los riesgos. La mitigación del riesgo, ahora utilizada frecuentemente para reducir las consecuencias financieras de catástrofes naturales, es una forma de auto-aseguramiento. [8].

En su libro de 1998 Against the Odds (Contra Viento y Marea), Peter Bernstein describe cómo el pensamiento acerca del riesgo evoluciona en parte debido a los cambios en los sistemas de numeración matemática, un entendimiento de las bases estadísticas de la probabilidad, y el aumento de la popularidad de los juegos de azar.

El dinero y los intereses financieros condujeron al pensamiento temprano del tema del riesgo. Aristóteles, en su tratado Politics, discute el concepto de opciones - un instrumento financiero que permite a los individuos comprar y vender bienes con precios previamente establecidos. Las opciones fueron tratadas en los Estados Unidos en la década de 1970 en lo que luego se convertiría en el NYSE (New York Stock Exchange) [7, p. 1-2]

1.2.2 Preocupación por los riesgos tecnológicos

La revolución industrial despertó preocupación sobre los riesgos que podrían ser causados por la tecnología. Específicamente, fue la invención de los motores de vapor que cambió cómo la sociedad y el gobierno veían y controlaban los riesgos.

Las máquinas de vapor, particularmente aquellas utilizadas en barcos, tenían el potencial de causar un gran número de muertes.

En 1838, el Congreso de los Estados Unidos, luego de años de debate del rol que el gobierno federal debería haber tenido en la regulación de los motores de vapor, dio pasos para proteger al público aprobando la primera ley regulatoria de la industria.

Desde la Revolución Industrial, la naturaleza de los peligros y riesgos ha cambiado. Los agentes de peligro han crecido tanto más grande -puentes, aviones, tanques de combustible, rascacielos, por ejemplo- como más pequeño -pesticidas, agentes activos biológicos, partículas subatómicas, y electrones moviéndose a través de circuitos integrados, por ejemplo. [7, p. 3-4]

1.2.3 La gestión de riesgos y su aporte a la continuidad del negocio

En el artículo de investigación publicado por Ramírez y Ortiz, "Gestión de riesgos tecnológicos basado en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios", en el ítem 4. Gestión de riesgo y continuidad de negocio, con respecto a la evaluación de riesgos y su relación con la gestión de continuidad de negocio, manifiesta:

> "Parte fundamental de la continuidad de negocios es la gestión de incidentes y a su vez está se relaciona con la gestión de riesgos. La adecuada gestión de incidentes evita que sean activados los planes de continuidad de negocios, por ello es importante que las respuestas a incidentes sean efectivas y se tengan claros los riesgos que pueden estar asociados" [6, p. 63]

Además indica que la valoración de los riesgos tecnológicos es parte de la gestión de la continuidad del negocio, argumentando:

"Cuando se realiza la valoración de riesgos dentro de la gestión de continuidad se tiene en cuenta la valoración del riesgo tecnológico y su efecto sobre los activos de información." [6, p. 63]

Menciona posteriormente algunos ejemplos acerca de los riesgos y su impacto en la continuidad, para concluir afirmando:

"Los ejemplos anteriores, muestran que la gestión de riesgos debe ser vista como soporte a la gestión de continuidad de negocios y la recuperación ante desastres." [6, p. 65]

El artículo publicado por Chris Goodwin, "Integrating Business Continuity Management with IT risk management", cita parte de la publicación de Gartner Research, "Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2013", que en su página 49 describe cómo la evaluación de riesgos como parte de la gestión de continuidad de negocio no era un aspecto tomando seriamente y cómo los estándares y herramientas de gestión han cambiado dicha visión errada:

> "La planificación de un modelo de continuidad de negocio (BMC) fue conducida históricamente con un nivel muy superficial de evaluación de riesgo, o incluso sin ésta. Aunque siempre se ha comprendido que la evaluación de riesgos es un componente necesario del planeamiento de un modelo de continuidad, los gerentes a veces la consideran como una actividad que consume mucho tiempo y recursos. Esta opinión ha estado justificada por una ausencia general de métodos y herramientas efectivos de evaluación de riesgos, a menudo exacerbada por el uso inapropiado de éstos. Además, debido a que la planificación del modelo de continuidad está generalmente orientado a eventos

de baja probabilidad y alto impacto, el énfasis de la evaluación de riesgos se centra típicamente en planificar con base en la posibilidad de un evento catastrófico, más que por la probabilidad de su ocurrencia.

Sin embargo, las expectativas de mejores niveles en la práctica se han incrementado, promovidas principalmente por los estándares, tales como ITIL, COBIT y las ISO 22301, 27001 y 31000. Esto se ha reforzado por una comprensión de que las evaluaciones de riesgo juegan un rol valioso en la identificación, valoración y prevención de eventos que podrían resultar en la activación innecesaria de planes de recuperación. Esto es, la evaluación de riesgos se enfoca no solo en los riesgos sobre los cuales las empresas tienen un pequeño control (tales como desastres naturales y terrorismo) sino también sobre aquellos en los que tiene más control (por ejemplo, fallas en las instalaciones, complejidad en la cadena de suministros, pobre gestión de cambio, debilidades en controles de seguridad y error humano)

Hoy, la evaluación de riesgos es recomendada en todos los marcos de trabajo de modelos de continuidad de negocio y las herramientas están siendo incluidas e integradas en módulos individuales en los conjuntos de herramientas para planificación BMC" (traducido de [23, p.49]

Para reforzar lo anteriormente descrito, la publicación de Gartner Research incluye el gráfico correspondiente (pág. 5) donde se aprecia cómo la aparición de estándares y marcos de trabajo permiten que la gestión de riesgos y la gestión de continuidad de negocios sean aspectos estrechamente relacionados y que han logrado consolidar los procesos de gestión dentro de las organizaciones.

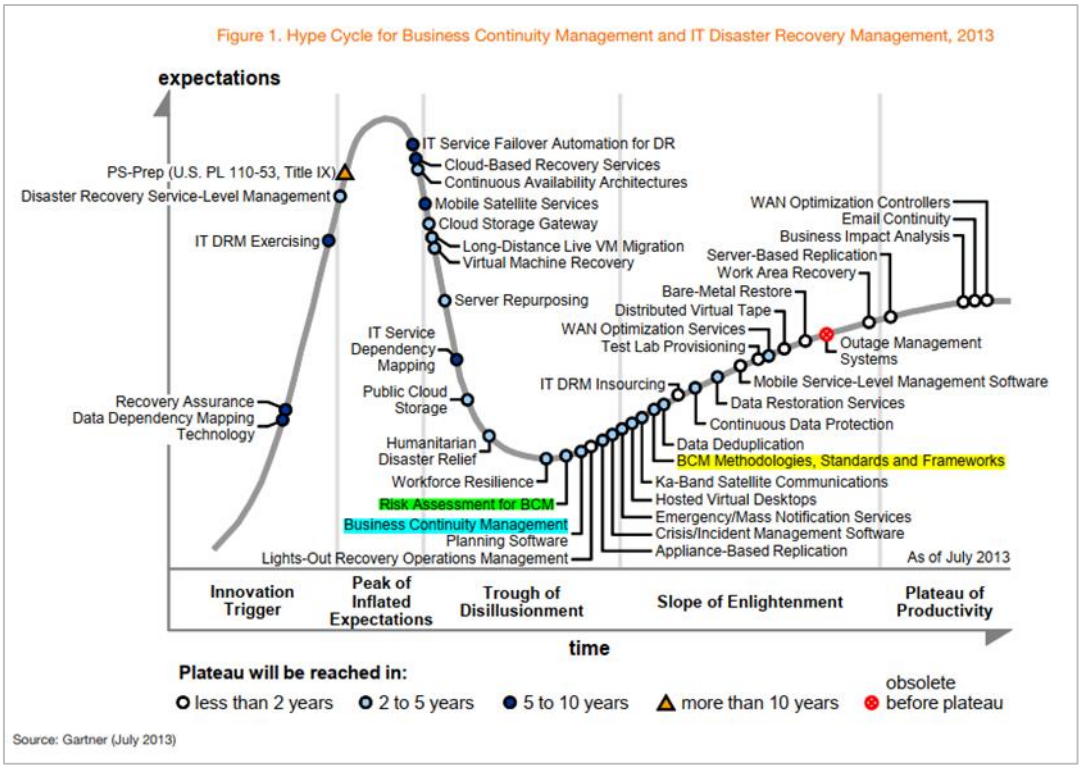


Figura 3.Ciclo de sobre-expectación de la gestión de continuidad de negocio y gestión de recuperación de desastres.

Fuente: Gartner Research [23, p.5]

El autor además argumenta que los equipos responsables tanto de la gestión de riesgos como de continuidad de negocio tienen ahora una oportunidad de integrar sus actividades haciendo uso de herramientas:

> "Aun cuando los equipos de BMC han estado hablando de evaluación de riesgos por un largo periodo, la realidad es que muchas de estas evaluaciones adolecen de madurez y calidad. Existe ahora la oportunidad de integrar a los equipos de BMC con los equipos de TI y de seguridad de la información para conformar una plataforma común que provea una técnica refinada y consistente de la evaluación, análisis y gestión" (Traducido de [24])

1.2.4 Cobit 5 para Riesgos

Cobit es un marco de referencia creado por ISACA (Information Systems Audit and Control Association, Asociación de control y auditoría de sistemas de información) y el Instituto de Administración de las tecnologías de la información (ITGI IT Governance Institute creado por ISACA en 1992) para la gestión y el gobierno de TI. Cobit (Control Objectives for Information Systems and related Technology, Objetivos de control para los sistemas de información y tecnología relacionada) tiene cinco versiones. Cobit 1 (publicado en 1996) fue la primera versión del marco de trabajo, Cobit 2 (publicado en 1998) que incluía temas de control, Cobit 3 (publicado en 2000) que incluía nuevas guías de gestión, Cobit 4 (publicado en 2005), Cobit 4.1 (publicado en 2007), Cobit 5 (publicado en 2012) que integraba Cobit 4.1, ValIT 2.0 y el marco de trabajo RiskIT. [14]

"Cobit 5 for Risk se construye sobre el marco de trabajo de Cobit 5 enfocándose en los riesgos de TI y proporcionando una guía más detallada y práctica para los profesionales de riesgos y otras partes interesadas en todos los niveles de una empresa" [15].

Presenta dos perspectivas para un contexto de riesgo: Perspectiva de función de riesgo y perspectiva de gestión de riesgo. La perspectiva de función de riesgo se enfoca en qué es necesario para construir y sostener la función del riesgo dentro de la organización. La perspectiva de gestión de riesgo describe cómo el proceso de gestión de riesgo puede ser apoyado por los habilitadores de Cobit 5. El alcance de Cobit 5 para riesgos se enfoca en utilizar los habilitadores para la gestión de riesgos por parte del gobierno, de una forma efectiva y eficiente. Provee además una guía de alto nivel para identificar, analizar y responder a los riesgos; se alinea con la gestión de riesgos corporativos y establece un enlace entre escenarios de riesgo y los habilitadores para la mitigación de riesgos. Uno de los aspectos más destacables de Cobit 5 for Risk es que provee veinte categorías de escenarios de riesgos, cubriendo más de 100 tipos de riesgos. Finalmente, Cobit 5 for Risk se alinea perfectamente con otros estándares y marcos de trabajo; cubre, por ejemplo, todos los principios de ISO 31000:2009 e incluye guías para áreas no cubiertas por este último, como Gobierno y gestión de riesgos de TI. Con respecto a ISO/IEC 27005:2011, cubre todo el proceso e incluye áreas adicionales como Gobierno del riesgo y reacción a

eventos. Cubre además los ocho componentes definidos en COSO y extiende algunos de ellos.

1.2.5 Estándares para la gestión de riesgos

ISO 31000:2018: En la categoría de riesgos, ISO ha publicado la norma ISO 31000:2018 (en), la cual provee guías para la gestión de riesgos que las organizaciones enfrentan. Esta norma provee una técnica común para gestionar cualquier tipo de riesgo pues no es específica a ningún sector o industria, pudiendo utilizarse durante el ciclo de vida de la organización y aplicado a cualquier actividad, incluyendo la toma de decisiones a todo nivel. Esta versión de la norma cancela la vigencia de la primera edición (ISO 31000:2009)

Entre los principales cambios de esta nueva versión de la norma podemos mencionar: se revisan los principios de la gestión del riesgo, los cuales son criterios claves para su éxito; resalta el liderazgo de la alta dirección así como la integración a la gestión del riesgo, comenzando por el gobierno de la organización; da mayor énfasis a la naturaleza iterativa de la gestión del riesgo, destacando que las nuevas experiencias, conocimiento y análisis pueden liderar la revisión de los elementos de los procesos, las acciones y controles en cada fase de dicho proceso; finalmente, incrementando el enfoque en un modelo de sistemas abiertos para ajustarse a múltiples necesidades y contextos. [9]

ISO 27005:2018: ISO (International Organization for Standardization, Organización Internacional para la Estandarización) es una organización mundial de estándares cuya elaboración está a cargo de comités técnicos. ISO colabora muy de cerca con la IEC (International Electrotechnical Commission, Comisión Internacional Electrotécnica) para todo lo que respecta a estandarización electrotécnica.

ISO 27005, publicada en junio del 2011, es una norma que provee una guía para la gestión de riesgos de seguridad de la información. Esta norma está diseñada para asistir a la implementación exitosa de seguridad de la información basada en una técnica de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tienen la intención de gestionar riesgos que podrían comprometer la seguridad de la información de la organización [10]. El 9 de julio de 2018 se ha publicado la más reciente versión de la norma.

1.2.6 Metodologías para la gestión de riesgos

MAGERIT: MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, ha sido elaborado y es promovido por el Consejo Superior de Administración Electrónica de España como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos.

La siguiente tabla muestra la evolución de MAGERIT:

EVOLUCIÓN DE MAGERIT		
Fecha	**Versión**	**Descripción**
1997	1.0	Ha resistido en su mayor parte el paso del tiempo, ratificándose en lo conceptual, mas no con respecto a los detalles técnicos.
2005	2.0	Revisión constructiva, adaptándola al tiempo presente e incorporando experiencia de esos años.
2012	3.0	Nueva adaptación. Tiene en cuenta no sólo la experiencia práctica sino también la evolución de las normas internacionales.

Tabla 1. Evolución de MAGERIT

MAGERIT responde a lo que se denomina "proceso de gestión de los riesgos", sección 4.4 de la norma ISO 31000, centro del "marco de gestión de riesgos". MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

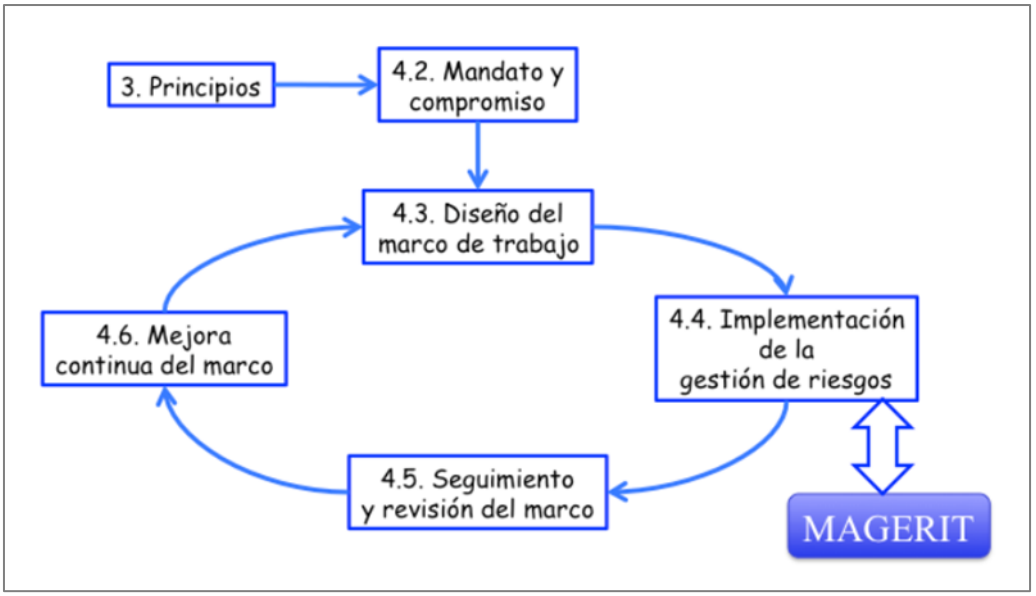


Figura 4. Marco de trabajo para la gestión de riesgos ISO 31000

MAGERIT persigue los siguientes objetivos:

Directos:

- Concientizar acerca de la existencia de los riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático de análisis de riesgos derivados del uso de las TIC.
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación. [12]

Al igual que la versión 2, la versión 3 se ha estructurado en 3 libros: El Método, el Catálogo de Elementos y la Guía de Técnicas.

El Método describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos.

El Catálogo de Elementos ofrece pautas y elementos estándar en cuanto a: tipos de activos, dimensiones de valoración de los activos, criterios de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger los sistemas de información.

La Guía de Técnicas proporciona algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos: técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi. [13]

OCTAVE

OCTAVE (Evaluación de la Amenaza Operacionalmente Crítica, Activos y Vulnerabilidad; Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología para la identificación y evaluación de los riesgos de seguridad de la información. Su intención es ayudar a las organizaciones a:

- Desarrollar criterios de evaluación cualitativa de riesgos que describa las tolerancias a riesgos operacionales de la organización.
- Identificar activos que sean importantes para la misión de la organización.
- Identificar vulnerabilidades y amenazas a los activos.
- Determinar y evaluar las consecuencias potenciales de la organización si las amenazas se materializan.

El marco de trabajo conceptual fue formado sobre las bases del enfoque original OCTAVE publicada por el Instituto de Ingeniería de Software (SEI, Software Engineering Institute) de la Universidad Carnegie Mellon en 1999.

EVOLUCIÓN DE OCTAVE	
Fecha	**Título de la Publicación**
Setiembre 1999	Marco de trabajo OCTAVE, versión 1.0
Setiembre 2001	Marco de trabajo OCTAVE, versión 2.0
Diciembre 2001	OCTAVE Criteria, versión 2.0
Setiembre 2003	OCTAVE-S versión 0.9
Marzo 2005	OCTAVE-S versión 1.0
Junio 2007	Introducción a OCTAVE Allegro, versión 1.0

Tabla 2. Evolución de OCTAVE [11]

Existen ahora 3 metodologías distintivas de OCTAVE disponibles para el público: el Método OCTAVE, OCTAVE-S y OCTAVE Allegro.

El Método OCTAVE fue la primera metodología introducida consistente con OCTAVE. La técnica está definida por una guía de implementación (procedimientos, guías, hojas de trabajo, catálogos de información) y entrenamiento. El método es ejecutado en una serie de sesiones de trabajo conducidas y facilitadas por un equipo de análisis interdisciplinario perteneciente a diversas unidades de negocios de la organización (gerente, jefes operacionales y personal) y miembros del departamento de TI.

El público objetivo del método OCTAVE son grandes organizaciones con 300 o más empleados. Más específicamente, fue diseñado para organizaciones que:

- Tienen una jerarquía multinivel.
- Mantienen su propia infraestructura tecnológica.
- Tienen la capacidad de ejecutar herramientas de evaluación de vulnerabilidades.
- Tienen la habilidad de interpretar los resultados de las evaluaciones de vulnerabilidades.

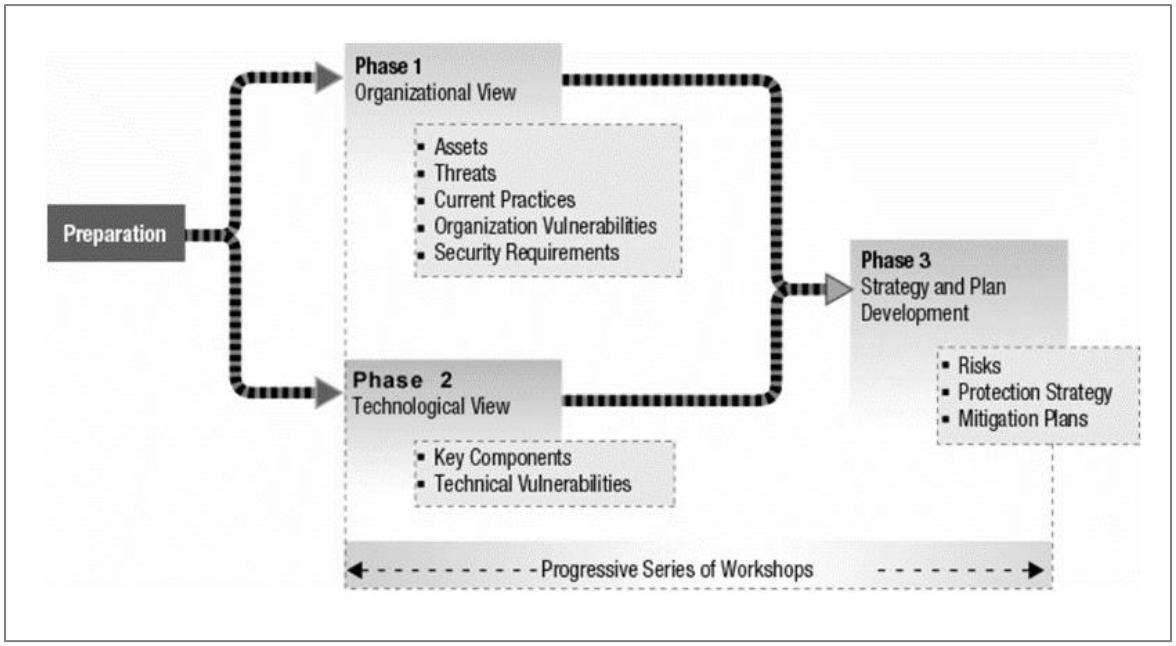


Figura 5. Fases del método OCTAVE [11]

El desarrollo de OCTAVE-S fue respaldado por el Programa de Inserción Tecnológica, Demostración y Evaluación (TIDE, Technology Insertion, Demonstration and Evaluation) del SEI con el objetivo de brindar una técnica basada en OCTAVE para pequeñas organizaciones manufactureras. La más reciente versión del enfoque OCTAVE-S, versión 1.0, está específicamente diseñada para organizaciones con 100 empleados o menos.

Consistente con el criterio OCTAVE, OCTAVE-S consiste de tres fases similares. Sin embargo, OCTAVE-S es ejecutado por un equipo de análisis que tiene un amplio conocimiento de la organización. Así, OCTAVE-S no confía en los talleres formales de obtención de conocimiento para obtener información pues se asume que el equipo de análisis (conformado generalmente por 3 a 5 personas) tiene ya conocimiento de los activos importantes relacionados a la información, requerimientos de seguridad, amenazas, y prácticas de seguridad de la organización.

Otra diferencia significativa es que OCTAVE-S es más estructurado que el método OCTAVE. Los conceptos de seguridad están incluidos en las hojas de trabajo y guías, permitiendo a los profesionales con menor experiencia en riesgos y seguridad manejar un amplio rango de riesgos con los cuales podrían no estar familiarizados. Una diferencia

final es que requiere menos revisión de la infraestructura de información de la organización debido a que las pequeñas organizaciones no tienen los recursos para adquirir y ejecutar herramientas de vulnerabilidad.

El enfoque de OCTAVE Allegro está diseñado para permitir una amplia evaluación del entorno de riesgos operacionales de la organización con el objetivo de producir resultados más robustos sin la necesidad de un conocimiento extenso de la evaluación de riesgos. Este enfoque difiere de los anteriores pues se enfoca principalmente en los activos de información, en el contexto en que son utilizados, dónde son almacenados, transportados y procesados, y cómo son expuestos a amenazas, vulnerabilidades, y disrupciones como resultado. Al igual que en los métodos previos, OCTAVE Allegro puede ser ejecutado bajo el estilo de sesiones de trabajo, entorno colaborativo, y está soportado con guías, hojas de trabajo y cuestionarios. Sin embargo, OCTAVE Allegro está pensado también para ser utilizado por personas que quieren hacer evaluación de riesgos que no están muy involucrados con la organización o tienen poca experiencia.

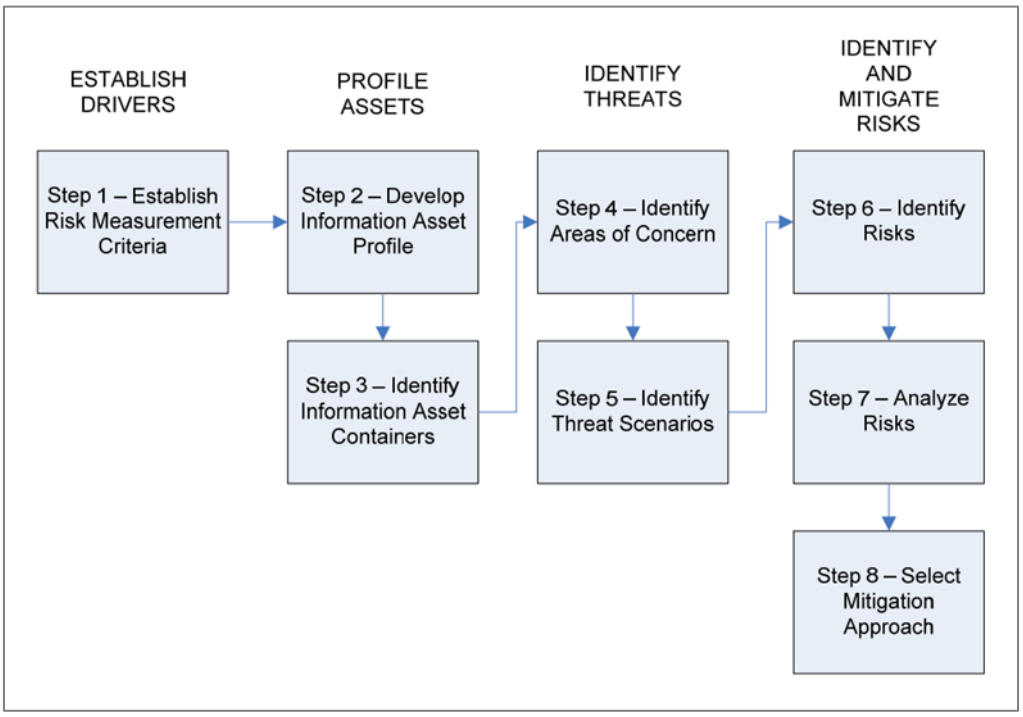


Figura 6. Hoja de ruta de OCTAVE Allegro.

OCTAVE Allegro consiste de 8 pasos organizados en 4 fases, tal como se ilustra en la figura anterior. [11]

CAPÍTULO II. MATERIALES Y MÉTODOS

2.1. Diseño de investigación

El Tipo y nivel de investigación es Cuantitativa – Experimental. *Cuantitativa*, pues es un tipo de investigación concluyente en su propósito al buscar la medición del problema y evitar todo juicio de valor o subjetivo. La cuantificación del problema permite su proyección a una población mayor mediante el uso de métodos estadísticos y matemáticos. *Experimental*, pues la aplicación del modelo a proponer (experimento) permitirá hacer un cambio en la variable independiente (*modelo de gestión de riesgos de TI*) a fin de observar el cambio en la variable dependiente (*apoyo en la continuidad del negocio*) y así poner a prueba la hipótesis planteada.

El Diseño de investigación es Pre-test / Post-test con un grupo.

$G = O_1 \; X \; O_2$
G: Grupo de estudio. *O_1: Observación o medida registrada antes de la aplicación del tratamiento en la variable dependiente (variable dependiente: apoyo a la continuidad del negocio)* *X: Tratamiento (variable independiente: Modelo de gestión de riesgos)* *O_2: Observación o medida registrada después de la aplicación del tratamiento en la variable dependiente (variable dependiente: apoyo a la continuidad del negocio)* [21]

2.2. Población y muestra

Se ha considerado un total de 04 empresas para el estudio, todas con sede en Europa y con giros de negocio y tamaños similares.

2.3. Métodos y técnicas de recolección de datos

Las técnicas e instrumentos de recolección de datos utilizados son:

Método	Técnicas e instrumento
Entrevista	Comunicación abierta. Preguntas para el directorio y área de TI (ver Anexo 1)
Encuesta	Elaboración de preguntas para el área de TI y usuarios (ver Anexo 2)
Observación	Documentación a revisar (ver listado en Anexo 3)

Tabla 3. Técnicas e instrumentos de recolección de datos. Fuente: Elaboración propia.

2.4. Procesamiento de datos

Se utiliza como herramienta Microsoft Excel 2013, para procesamiento de encuestas y generación de gráficos estadísticos.

El plan de procesamiento y análisis de datos, involucra las siguientes actividades:

- Recolección de datos.
- Procesamiento utilizando Microsoft Excel (gráficos, cuadros, tablas, etc.)
- Análisis e interpretación.
- Presentación de resultados.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Diagnóstico del sector

Un total de cuatro empresas han participado para poder realizar un diagnóstico del sector. Luego de analizar la situación individual de cada empresa, se han detectado características y necesidades comunes. La base de estas características comunes es que son similares en cuanto al sector donde se encuentran, su tamaño y número de empleados y el tipo de servicios que ofrecen. Son compañías de pocos empleados donde por lo general no existen jerarquías en la práctica, manejándose como una organización horizontal. Todas son empresas que brindan software como servicio, en rubros similares o relacionados. Ninguna cuenta actualmente con un área dedicada a la gestión de riesgos, aunque tienen políticas generales y personas que velan por su aplicación, y en algunos casos, es un esfuerzo común entre los empleados, aunque esto, no está formalmente establecido. Todas estas empresas se encuentran en proceso de adecuación a la norma europea de protección de datos personales (GDPR) como parte de la exigencia normativa de la Unión Europea. Esto trae muchos beneficios asociados a la protección y seguridad de los datos personales, aunque, por otro lado, ha exigido que las empresas impongan ciertas restricciones y controles adicionales para sus empleados que no trabajan dentro de los límites geográficos de la UE. Para ver mayor información acerca de las empresas participantes, diríjase al Anexo 1: Hoja resumen de empresas participantes.

3.2. Armonización de estándares

Los estándares, marcos de trabajo y metodologías consideradas en este análisis son las siguientes:

- ISO 31000:2018 – Directrices para la gestión de riesgos.
- ISO/IEC 27005:2018 – Tecnologías de la información – Técnicas de seguridad – Gestión de riesgos de la seguridad de la información.

- Cobit 5 for Risk – Marco de trabajo para la gestión de riesgos.
- MAGERIT v3.0 – Metodología de análisis y gestión de riesgos de los sistemas de información.
- ISO 22301:2012 – Seguridad de la sociedad: sistemas de continuidad del negocio – requisitos.

El análisis completo de los marcos y metodologías se encuentre en el Anexo 5: Cuadro de análisis de estándares, marcos de trabajo y metodologías.

3.3. Estructura del modelo

El modelo propuesto ha sido resultado del análisis de los estándares, marcos y metodologías citadas en el apartado anterior. El estándar ISO 31000:2018 se ha tomado como eje para la elaboración del modelo propuesto.

El modelo propuesto consta de 6 fases:

- FASE I: Alcance, contexto y criterios.
- FASE II. Valoración del riesgo.
- FASE III. Análisis de impacto del negocio (BIA)
- FASE IV. Tratamiento del riesgo.
- FASE V. Seguimiento y revisión.
- FASE VI. Comunicación y consulta.

MODELO PARA LA GESTIÓN DE RIESGOS DE TI		
FASE	**Actividades**	**Instrumentos**
FASE I: Alcance, contexto y criterios. Objetivo: Definir el alcance de la gestión de riesgos.	1.1 Definición de la visión, misión, objetivos, metas y alcance de la gestión de riesgos.	▪ Reuniones. ▪ Entrevistas. ▪ Revisión de información histórica relacionada a eventos de riesgo y su gestión.
	1.2 Establecer el contexto externo e interno. - Análisis FODA - Contexto externo: o Relación con los clientes. o Contexto socio-cultural. o Contexto económico. o Contexto regulatorio-normativo. o Competencia. o Relación con proveedores. - Contexto interno: o Objetivos y estrategias. o Estructura organizacional. o Capacidades. o Ambiente laboral.	• Manual de organización y funciones. • Manual de procedimientos. • Plan estratégico. • Cualquier otra documentación interna relacionada a las operaciones de la organización. • Normatividad vigente. • Políticas y procedimientos.

	1.3 Criterios de aceptación del riesgo. Niveles de aceptación del riesgo.	Formato para el establecimiento de criterios de aceptación del riesgo (ver anexo 6> 6.1) Formato para el establecimiento de los niveles de aceptación del riesgo (ver anexo 6 > 6.2)
	1.4 Organización y responsabilidades del proceso de gestión del riesgo: Se establecen quienes conformarán el comité de gestión de riesgos, así como sus principales funciones.	Guías: 1. RiskIT > 5. Fundamentos de Gobierno de Riesgo > Figura 8. Responsabilidades y rendición de cuentas de los riesgos de TI. [33] 2. Cobit 5 for Risk > Appendix B > B.3. Enabler: Organisational Structures. [15] 3. Magerit v3 > Libro 1 > Capítulo 5. Proyectos de análisis de riesgo > Ítem 5.1. Roles y funciones. [12] Formato para describir los roles y funciones del comité de riesgos (ver anexo 6 > 6.3). Matriz RACI de actividades y funciones (ver anexo 6 > 6.4).
FASE II. Valoración del riesgo. Objetivo: identificar y evaluar el riesgo a fin de determinar cuáles tienen significancia para la organización.	2.1 Identificación del riesgo ▪ Identificación de los activos. ▪ Valoración de los activos. ▪ Identificación de las amenazas y vulnerabilidades.	Formato de identificación de activo (ver anexo 6 > 6.5) Escala de valoración de los activos (ver anexo 6 > 6.6) Tabla de valoración de los niveles de criticidad (ver anexo 6 > 6.7) Formato de valoración de los activos (ver anexo 6 > 6.8) Formato de identificación de amenazas y vulnerabilidades (ver anexo 6 > 6.9)
	2.2 Análisis del riesgo ▪ Evaluar la probabilidad de ocurrencia. ▪ Evaluar las consecuencias/impacto. ▪ Determinar el nivel de riesgo (estimar el riesgo)	Escala de valoración de la probabilidad de ocurrencia de un evento de riesgo (ver anexo 6 > 6.10) Escala de valoración del impacto de un evento de riesgo (ver anexo 6 > 6.11) Tabla de mapeo cualitativo (mapa de calor) (ver anexo 6 > 6.12) Formato para la determinación del nivel de riesgo (ver anexo 6 > 6.13)

	2.3 Evaluación del riesgo de TI ▪ Priorizar el riesgo. ▪ Establecer los niveles de apetito y tolerancia.	(Ubicación de los riesgos valorados en el mapa de calor) Tabla de nivel de criticidad del riesgo inherente (ver anexo 6 > 6.14) Tabla de valorización de la tolerancia al riesgo. (ver anexo 6 > 6.15)
FASE III. Análisis de impacto del negocio (BIA) Objetivo: determinar qué procesos son críticos y sus tiempos de recuperación.	3.1 Identificación de las funciones y procesos/servicios.	Formato de identificación de funciones y procesos (ver anexo 6 > 6.16)
	3.2 Establecimiento del nivel de criticidad de las funciones y procesos/servicios	Esquema de valoración de la criticidad (ver anexo 6 > 6.17) Formato para el establecimiento del nivel de criticidad de las funciones y procesos (ver anexo 6 > 6.18)
	3.3 Evaluación del impacto ▪ Evaluación del impacto por área. ▪ Evaluación del impacto. Consolidación.	Tabla de escalas de impacto por área (ver anexo 6 > 6.19) Formato de valoración del impacto por área y escala de tiempo (ver anexo 6 > 6.20) Formato para el establecimiento de los grados de importancia de las áreas (ver anexo 6 > 6.21)
	3.4 Evaluación de tiempos (MTD, RTO, WRT, RPO)	Definiciones de los tipos de tiempos de recuperación (ver anexo 6 > 6.22) Formato para el establecimiento de los tiempos de recuperación (ver anexo 6 > 6.23) Formato para el registro de incidentes (si fuera aplicable) (ver anexo 6 > 6.23b)
	3.5 Identificación de los procesos alternos.	Formato para la descripción de los procesos alternos (ver anexo 6 > 6.24)
	3.6 Generación de informe de impacto de negocio.	Estructura del informe de impacto (ver anexo 6 > 6.25)

FASE IV. Tratamiento del riesgo. Objetivo: proponer planes de tratamiento de riesgo	4.1 Seleccionar las opciones para el tratamiento del riesgo.	Formato para el tratamiento de riesgos (ver Anexo 6 > 6.26)
	4.2 Proposición de planes de tratamiento de riesgo.	Formato para el establecimiento de planes de tratamiento de riesgos (ver Anexo 6 > 6.27)
FASE V. Seguimiento y revisión. Objetivo: monitorear los planes de tratamiento planteados.	5.1 Seguimiento, revisión y responsables.	Formato para el seguimiento y revisión de los planes de acción (ver anexo 6 > 6.28)
FASE VI. Comunicación y consulta. Objetivo: proponer estrategias de comunicación como parte del proceso de gestión.	6.1 Lineamientos para la comunicación y consulta.	Formato para el establecimiento de acciones de comunicación (ver anexo 6 > 6.29)

Tabla 4. Descripción del Modelo Propuesto. Fuente: Elaboración propia.

3.4. Implementación del modelo

FASE I. Alcance, Contexto y Criterios

1.1. Misión, Visión, Objetivos y Metas de la gestión de riesgos

Visión

Apoyar la continuidad del negocio a través de la gestión efectiva del riesgo de TI.

Misión

Formular un modelo cuya aplicación permita anticiparnos a la ocurrencia de eventos de riesgo de TI a través de su identificación, priorización, gestión y monitoreo.

Objetivos

- Construir y mejorar nuestra capacidad de responder efectivamente a los eventos de riesgo.
- Desarrollar un entendimiento común del riesgo para todas las funciones y en todas las unidades de negocio.
- Desarrollar una cultura de gestión de riesgos menos correctiva y más preventiva, reduciendo las vulnerabilidades.

Metas de la implementación

- Conocer y comprender el entorno.
- Identificar los procesos, productos y servicios de TI cuya interrupción o ausencia pudiera poner en riesgo la continuidad del negocio.
- Identificar los riesgos, su probabilidad e impacto, así como los controles a aplicar.

- Implementar planes de acción para enfrentar eventos de riesgo.
- Ejecutar un programa de capacitación y concientización sobre los riesgos de TI y su gestión.

Alcance de la implementación

- Abarcará la organización en su totalidad, debido a su tamaño, número de empleados y procesos.
- Se centrará en la gestión de riesgos de TI que dan soporte a los procesos de negocio.
- Su ejecución estará a cargo de un equipo conformado para tal fin.

1.2. Contexto externo e interno

ANÁLISIS FODA		
INTERNOS	**FORTALEZAS**	**DEBILIDADES**
	• Relativa facilidad para adaptarse al cambio (organizacional y de negocio) • Calidad de servicio y excelente relación con los clientes (NPS=75) • Independencia de tiempo y ubicación. • Posicionamiento en el mercado. • Amplia experiencia en el sector. • Aplicaciones Web fáciles de utilizar. • Rápida solución a los problemas.	• Presupuesto limitado. • Algunos procesos no están formalizados. • Desarrollo de software parcialmente estandarizado. • Cambio frecuente de elementos distintivos de la empresa.
EXTERNOS	**OPORTUNIDADES**	**AMENAZAS**
	• Creciente adopción de uso de herramientas de evaluación de niveles de satisfacción de cliente, a través de encuestas NPS. • Frecuentes requerimientos por parte de clientes para desarrollo de software a medida. • Modalidad de trabajo remoto cada vez más extendida a nivel mundial.	• Riesgos de seguridad de información en Internet. • Cultura cada vez más generalizada de corta permanencia como empleados en las organizaciones. • Crecientes niveles de ciberdelincuencia.
	POSITIVOS	NEGATIVOS

Fuente: Elaboración propia.

Contexto externo

- Relación con los clientes: aspecto que ha mejorado a través del tiempo y se da mediante la aplicación de encuestas NPS en los últimos 4 años. Se ha pasado de tener un NPS de 54 a 75. La empresa tiene una relación cercana con los clientes, asistiéndolos rápidamente ante cualquier duda o problema. Se utilizan diversos canales: foro de consultas y problemas, sistema de ayuda Web y videos tutoriales (a demanda), comunicación telefónica, chat y video conferencia por Skype y visitas presenciales.

- Socio cultural: De acuerdo a la Eurostat, que es la oficina de estadísticas de la Unión Europea (https://ec.europa.eu/eurostat), Europa mantiene uno de los niveles educativos más altos a nivel mundial. En el 2018, el 81% de la población estudiantil entre 25-54 años había completado el nivel de educación secundario y más del 40% de personas entre 30-34 años había completado el nivel de educación superior, llegando Dinamarca y Reino Unido casi al 50%. Con respecto al dominio de una lengua extranjera, más del 80% de la población económicamente activa conoce al menos un idioma extranjero, mientras que Dinamarca ocupa el 3er lugar con 96% y Reino Unido, a la zaga, con 35%. Esto revela la preponderancia del idioma inglés como lengua preferida por los habitantes de la UE. En promedio, el 94% de los egresados en educación secundaria en la UE deciden aprender el idioma inglés como lengua extranjera. Los habitantes de la UE tienen una alta participación en la vida cultural de sus países, se acuerdo a Eurostat, en el 2015, dos tercios de la población de la UE participa o está involucrada en alguna actividad cultural, esto, favorecido además por el hecho que muchas de las ciudades más importantes de la UE son cosmopolitas. Estas actividades tiene un impacto económico significativo pues se dichas actividades generaron un movimiento económico de 8.6 billones de euros en 2017. Por otro lado, las estadísticas relacionadas a la sociedad digital muestran avances notorios. En el 2017, casi la mitad de las empresas de la UE hacen uso intensivo de las redes sociales y el acceso a Internet en los hogares ha alcanzado el 87%, siendo el 85% conexiones de banda ancha. La proporción

de personas entre 16-74 años que han comprado a través de Internet alcanzó el 57% en el 2017.

- Económico: La Unión Europea es la segunda economía a nivel mundial, luego de los Estados Unidos. El mercado de bienes y servicios alcanzó los 18.8 trillones de dólares en el 2018, representando el 22% de la economía global. A nivel familiar, en el 2016, el porcentaje de ahorro llegó a casi 11%, y el de inversión a casi 8%.

- Regulatorio/Normativo: Las empresas que gestionan datos personales de habitantes de la UE se encuentran desde el 25 de mayo de 2018 bajo la Regulación General de Protección de Datos (General Data Protection Regulation, GDPR), la cual ha tenido un impacto significativo en los negocios, especialmente en negocios SaaS. Cabe indicar que esta normativa se aplica a cualquier negocio de bienes y servicios que tiene operaciones o gestiona información de habitantes de la UE. En el caso de las empresas SaaS, estas no solamente deben cumplir la regulación, deben ayudar a sus clientes a cumplirla. La mayoría de los requerimientos se encuentran en los artículos 12, 13 y 14.

- Competencia: la empresa tiene competencia directa tanto en las ciudades donde opera como a nivel internacional en general. Debido que sus clientes son de diversas partes del mundo la competencia se extiende también a dichos países. En algunos casos, la naturaleza global del cliente extiende la competencia que la empresa tiene, siempre dentro del ámbito de la creación, distribución y procesamiento de encuestas NPS. Entre otras empresas de la competencia podemos citar: Enalyzer, SurveyMonkey, SmartSurvey y ActiveCampaign.

- Relación con proveedores: la empresa terceriza varios servicios, entre los cuales podemos mencionar: el servicio de hosting, a cargo de la empresa TDC; el envío masivo de correos electrónicos, a cargo de la empresa SendGrid; el

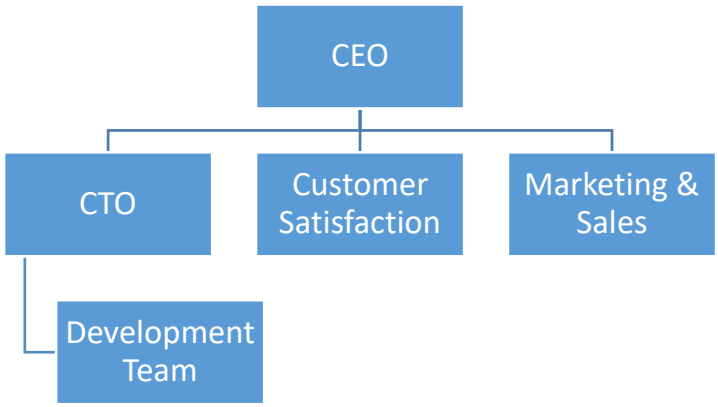
envío de mensajes de texto a celulares, a cargo de empresas como: Twilio (Canadá/EEUIU), SMS Broadcast (Australia), TNZ (Nueva Zelanda), Worldtext (Portugal).

Contexto interno

- Objetivos y estrategias:

  Misión: inspirar e influenciar en las relaciones de las compañías con sus clientes. Queremos que las empresas tengan más clientes embajadores que promuevan sus productos.

- Estructura organizacional:



Roles y responsabilidades:

ROLES Y RESPONSABILIDADES	
Rol	**Responsabilidad**
CEO	• Representa a la empresa. • Toma las decisiones. • Elabora los planes de negocio. • Dirige y controla la ejecución de los planes de negocio. • Monitorea y coordina con las diversas áreas de la empresa.

	• Establece relación directa con clientes existentes y potenciales y proveedores.
CTO	• Dirige y coordina las estrategias tecnológicas. • Fomenta la cultura tecnológica. • Evalúa de manera constante las soluciones tecnológicas brindadas a los clientes a fin de encontrar nuevas maneras de hacerlas más eficaces.
Personal del área: Customer Satisfaction	• Orientar al cliente durante todo el proceso de adopción de las soluciones tecnológicas. • Ayudar al cliente en la realización de tareas. • Ayuda el cliente en la solución de los problemas. • Controla y reporta el estado del NPS cada mes.
Personal del área: Marketing & Sales	• Contactar nuevos potenciales clientes. • Mantener actualizado el contenido de los sitios Web. • Conducir el proceso de integración de nuevas cuentas.
Personal del área: Development team	• Mantenimiento de los sistemas Web de la organización. • Desarrollo de nuevos sistemas, módulos o funcionalidades. • Mantenimiento de los sitios Web. • Tareas de mantenimiento y optimización de las bases de datos.

Tabla 5. Roles y responsabilidades en la organización. Fuente: Elaboración propia.

- Capacidades: la empresa cuenta con 8 empleados distribuidos en 5 países, los cuales coordinan sus actividades de manera remota. La mayoría de empleados se encuentran físicamente en Londres. La empresa cuenta con dos sistemas propietarios: un CRM para la gestión de clientes y otro para la gestión de proyectos y tareas, y registro de actividades. Cuenta actualmente con dos soluciones tecnológicas ofrecidas a los clientes, ambas son aplicaciones Web: RSS, para el diseño, distribución y procesamiento de boletines electrónicos, y RLS, para el diseño, distribución y procesamiento de encuestas por Internet.

- Ambiente laboral: existe un buen clima laboral, potenciado principalmente por las características en la forma en que se lleva a cabo el trabajo, los empleados valoran la libertad de poder disponer de su tiempo cuando se trabaja por objetivos. El único aspecto que a veces trae ciertos inconvenientes es la diferencia horaria, pero la empresa ha establecido los horarios de contacto y coordinación entre los empleados a fin de poder tener rangos de horas donde coincida la mayoría, sobre todo para las llamadas grupales y reuniones virtuales. La alta rotación en algunos puestos de trabajo en el último año se ha debido principalmente a la costumbre que los empleados tienen, principalmente en Europa, de no permanecer mucho tiempo en un puesto específico por mucho tiempo, con mayor incidencia en empresas pequeñas como la que es objeto de estudio.

1.3. Criterios de aceptación del riesgo

La empresa ha establecido los siguientes criterios para la aceptación del riesgo:

CRITERIOS DE ACEPTACIÓN DE RIESGO	
Aspecto	**Criterio**
Económico	No se acepta una pérdida mayor a los 30000 USD.
Operativo	No se acepta una interrupción de los servicios (sistemas Web) mayor a 08 horas.
Regulatorio	No se acepta el incumplimiento regulatorio que pueda dar origen a sanción.
información	No se acepta la pérdida total o parcial de datos, mayor a 6 horas de antigüedad.
Continuidad	No se acepta interrupciones generales en las operaciones mayores a 24 horas.

NIVELES DE ACEPTACIÓN DE RIESGO				
Nivel de riesgo		**Nivel de aceptación**	**Descripción**	**Estrategia(s)**
	Bajo	Aceptable (Apetito)	Se asume el riesgo y se gestionará por medio de los procedimientos establecidos. Se registrará y se monitoreará 2 veces al año.	Aceptar
	Moderado	Tolerable (Tolerancia)	Se buscará reducir su probabilidad de ocurrencia mediante la proposición de controles preventivos. Se registrará y tendrá un seguimiento trimestral.	Mitigar
	Alto	No aceptable	Se establecerán medidas de control preventivas y correctivas para tratar de evitar su ocurrencia. Se efectuará su registro y tendrá un seguimiento mensual.	Aceptar, Mitigar, Evitar, Compartir/Transferir

Fuente: Elaboración propia.

Lineamientos:

- Deben evitarse los riesgos que permitan dicho tratamiento.
- Deben reducirse los riesgos en todos los casos aplicables.
- Los efectos de los eventos de riesgo deben ser contenidos dentro de los límites establecidos.
- El desarrollo a futuro no debería traer consigo un riesgo incremental.

1.4. Organización y responsabilidades del proceso de gestión de riesgos:

La empresa ha decidido conformar un comité para la gestión de riesgos conformado por el CTO y dos miembros del staff, uno del área de desarrollo y uno del área de gestión de clientes. Las principales responsabilidades de este comité son:

- Diseñar e implementar el proceso de gestión de riesgo para la empresa.

- Valoración de los riesgos, analizando los riesgos actuales e identificando nuevos riesgos potenciales.
- Establecer el nivel de riesgo que la empresa está dispuesta a aceptar.
- Preparar el presupuesto para la gestión de riesgos.
- Elaborar reportes que permitan que la dirección conozca sobre los riesgos más significativos.
- Asegurar que todos los miembros de la empresa logren entender y asumir su propia responsabilidad en la gestión de riesgos.
- Crear planes de continuidad del negocio basado en la gestión de riesgos.

A continuación se establecen las responsabilidades específicas de cada uno de los miembros del equipo de gestión de riesgos:

COMITÉ DE GESTIÓN DE RIESGO	
Rol	**Función**
Responsable de TI	Promoción, alineación de TI y estrategias organizacionales y la planificación, la asignación de recursos y la gestión de la prestación de servicios de TI. Coordina la labor del equipo y contribuye en todas las fases del proceso. Participa en el establecimiento de una visión común del riesgo.
Responsable de riesgos	Encargado de la evaluación del riesgo: recopilación de datos, análisis y mantenimiento del perfil de riesgos. Elabora y mantiene los planes de control. Es, en resumen, el responsable de la conducción del proceso de gestión de riesgos.
Responsable de cumplimiento y auditoría	Supervisa el cumplimiento de los planes de control de riesgos. Colabora en el mantenimiento y actualización del catálogo de riesgos y planes de control. Responsable además, de las tareas de comunicación, en coordinación con el responsable de riesgos.

MATRIZ RACI DE ACTIVIDADES Y FUNCIONES PARA EL PROCESO DE GESTIÓN DE RIESGOS							
Funciones		Comité riesgos			Otras áreas		
Actividades	CEO	CTO	Responsable de riesgos	Responsable cumplimiento	Customer Satisfaction	Marketing & Sales	Development Team
Misión, visión, objetivos y metas de GR	A	A/C	R	I			
Establecimiento del contexto		A	R				
Criterios de aceptación	C/I	A/C	R	C/I			
Identificar el riesgo		A	R		C	C	C
Análisis de riesgos		A/C	R	C			
Evaluación de riesgos	I	A/C	R	I	C	C	C
BIA. Identificación de funciones, procesos y servicios.		A/C	R		C	C	C
BIA. Establecimiento del nivel de criticidad	C	A	R	C			
BIA. Evaluación del impacto		A	R	C			
BIA. Evaluación de los tiempos		A	R		C	C	C
BIA. Identificación de los procesos alternos	I	A/C	R	I	C	C	C
Generación del informe de impacto de negocio	I	A	R	I			
Proposición de planes para el tratamiento del riesgo	C/I	A/C	R	C/I	C	C	C
Seguimiento y revisión		A	I	R			
Comunicación y consulta	I	A	C/I	R	I	I	I

R: Responsable, es quien efectivamente realiza la tarea.

A: Aprobador, responsable de que la tarea se realice y rinde cuentas sobre su ejecución.

C: Consultado, posee información o capacidad necesaria para la realización de la tarea.

I: Informado, debe ser informado del avance y los resultados de la ejecución de la tarea.

FASE II. Valoración del riesgo

2.1. Identificar el riesgo

- Identificación de los activos de TI

Entrada: Información sobre los activos de TI.

Salida: Lista categorizada de activos de TI.

Procedimiento:

El responsable de riesgos elaboró una lista inicial de los activos de TI cuya categorización se basó inicialmente en lo descrito en el libro 2 de Magerit v3.0 [12] y luego se adecuó de acuerdo a los hallazgos. Dicha lista fue distribuida con anticipación al inicio de las reuniones. Se llevaron a cabo reuniones con los miembros de cada una de las áreas involucradas a fin de depurar o ampliar la lista inicial, se modificaron algunas descripciones y se asignaron los códigos correspondientes. Durante el proceso se excluyeron algunos activos, ya sea por su tamaño, porque no estarían en uso o no se aplicarían en el futuro.

> **Nota**: Para la codificación de los activos, se consideró inicialmente la nomenclatura sugerida en el libro 2 de Magerit v3.0, pero luego se varió el formato, considerando un prefijo, correspondiente a la categoría del activo y luego las iniciales del nombre del activo o letras relacionadas al mismo.
>
> La numeración o el orden en que se listan los activos no determinan su importancia o relevancia para la organización.

IDENTIFICACIÓN DE ACTIVOS de TI - HOJA RESUMEN					
Clasificación: Procesos de negocio (PN)					
Elaborado por		JMRC		**Fecha**	/ /
Nr.	**Código**	**Nombre**	**Descripción**		**Responsable**
1	PN_GCyL	Gestión de clientes y licencias	Incorporación de un cliente al sistema, registro de usuarios y configuración. Inducción. Creación del plan de distribución. Activación del plan.		Área: Customer Satisfaction
2	PN_GPyF	Gestión de pagos y facturación	Generación de las facturas de cliente mediante la integración con el servicio externo e-conomic. Registro de pagos para los empleados.		Área: Marketing & Sales
3	PN_GPD	Gestión de proyectos de desarrollo	Estimación, planificación e implementación de los proyectos de desarrollo de software (internos y externos)		CTO, Development Team
4	PN_GCS	Gestión de copias de seguridad (respaldo y restauración)	Generación y control de copias de seguridad de archivos y bases de datos, tanto de los sistemas como de los sitios Web. Restauración de bases de datos, generalmente para ayudar al cliente a resolver problemas de eliminación involuntaria de datos.		Development Team
5	PN_GAD	Gestión de adquisiciones, contrataciones y compras	Determinación de necesidades, evaluación de opciones de mercado, entrevistas y adquisición, contratación y compras, de bienes y servicios.		CEO, CTO

IDENTIFICACIÓN DE ACTIVOS de TI - HOJA RESUMEN					
Clasificación		Hardware (HW)			
Elaborado por		JMRC		**Fecha**	/ /
Nr.	**Código**	**Nombre**	**Descripción**		**Responsable**
1	HW_LAP	Laptop	04 Laptops utilizada por el CEO, CTO y 2 empleados del área de Marketing & Sales.		CTO
2	HW_USB	Dispositivos de almacenamiento USB	04 dispositivos de almacenamiento utilizados por el CEO, CTO y dos empleados del área de Marketing & Sales.		CTO

IDENTIFICACIÓN DE ACTIVOS de TI - HOJA RESUMEN					
Clasificación		Software (SW)			
Elaborado por		JMRC		**Fecha**	/ /
Nr.	**Código**	**Nombre**	**Descripción**		**Responsable**
1	SW_CRM	Customer Relationship Management	Sistema Web para gestionar actuales y potenciales clientes y licencias. Tiene integración con el servicio externo e-conomic para la gestión de facturas.		CEO
2	SW_TL	Task List	Sistema Web para la gestión de proyectos, tareas y control. Contiene módulos para la gestión de idiomas de las aplicaciones y monitoreo de actividad de cuentas de clientes.		CTO
3	SW_RNS	RW Newsletter Solution	Sistema Web para el diseño, distribución y procesamiento de boletines electrónicos.		CEO, CTO

4	SW_RLS	RW Loyalty Solution	Sistema Web para el diseño, distribución y procesamiento de encuestas NPS y eNPS	CEO, CTO
5	SW_SRVW	Servicios Windows	16 Servicios Windows para diversas tareas, relacionadas principalmente a los sistemas RLS y RNS (distribución, importación, integración, etc.)	Development Team
6	SW_SWB	Sitios Web	2 Sitios Web en WordPress, en idiomas danés e inglés.	CEO, CTO
7	SW_SOA	Sistema Operativo y aplicaciones	Sistema operativo y aplicaciones instaladas	CTO

IDENTIFICACIÓN DE ACTIVOS de TI - HOJA RESUMEN				
Clasificación	Información (INF)			
Elaborado por	JMRC		**Fecha**	/ /
Nr.	**Código**	**Nombre**	**Descripción**	**Responsable**
1	INF_BDT	Bases de datos	Bases de datos de los sistemas Web, CRM, Task List, gestión de idiomas.	CTO
2	INF_RCR	Repositorio de Credenciales	Archivo(s) que contienen las credenciales de los sistemas y servicios contratados (envío masivo de correos, campañas, servicios de SMS, Hosting, Sitios Web)	CTO
3	INF_DOC	Documentación	Documentación administrativa, contable, etc. tanto en físico como en formato digital.	CTO

IDENTIFICACIÓN DE ACTIVOS de TI - HOJA RESUMEN					
Clasificación		Servicios (SRV)			
Elaborado por		JMRC		**Fecha**	/ /
Nr.	**Código**	**Nombre**	**Descripción**		**Responsable**
1	SRV_COE	Correo electrónico	Servicio de mensajería proporcionada por Gmail (cuenta corporativa)		CTO
2	SRV_SKY	Comunicación en tiempo real vía Skype	Servicio de mensajería en tiempo real por chat, llamadas de voz o video conferencia (cuentas gratuitas)		CTO
3	SRV_TEC	Telefonía celular	Servicio de telefonía celular (personal, no corporativo)		CTO
4	SRV_INT	Internet	Servicio de acceso a Internet (compartido)		CTO
5	SRV_ALN	Almacenamiento en la nube	Servicio de almacenamiento, compartición y trabajo colaborativo proporcionado por Google Drive (cuenta corporativa)		CTO
6	SRV_SMS	Envío de SMS	Servicio de envío masivo de SMS: Twilio (Canada/US), SMS Broadcast (Australia), TNZ (Nueva Zelanda), Worldtext (Portugal, Singapur, Hungría), Inmobile (Dinamarca)		CTO
7	SRV_VPN	Red privada virtual	Servicio de red privada virtual, proporcionado por PureVPN.		CTO
8	SRV-CON	Servicios contables	Servicios de facturación, proporcionado por E-conomic.		CTO
9	SRV_HOS	Servicio de hosting	Servicio de alojamiento de sitios Web, proporcionado por TDC (para los 2 Sitios Web y los servidores Web, Base de datos y Pruebas)		CTO

10	SRV_MEN	Servicio de envío de mensajería electrónica	Servicio de envío masivo de correo electrónico, utilizado para la distribución de boletines y encuestas. Proporcionado por SendGrid.	CTO

- Valoración de los activos

Entrada: lista categorizada de activos de TI.
Salida: cuadro de valoración de activos de TI.
Procedimiento:
El responsable de riesgos elaboró el cuadro de valoración a utilizar, así como el cuadro resumen sobre el que se trabajó. Estos documentos fueron remitidos con anticipación a las áreas involucradas. Se llevó a cabo una reunión con uno de los miembros de cada área involucrada. Durante la sesión, cada miembro proporcionaba un puntaje a cada activo por cada criterio considerado. El puntaje final se obtenía por promedio simple en base a las puntuaciones parciales asignadas. Sólo en casos de notoria diferencia entre puntajes se sometían los mimos a discusión.

Los criterios considerados en la valoración se encuentran en el Anexo 6 > 6.2. La siguiente tabla muestra los resultados de la valoración:

VALORACIÓN DE ACTIVOS								
	ACTIVO			CRITERIOS			TOTAL	Nivel de Criticidad
Nr.	Clasificación	Código	Nombre	Confidencialidad	Integridad	Disponibilidad		
1	Proceso	PN_GCyL	Gestión de clientes y licencias	4	5	3	12	Alto
2	Proceso	PN_GPyF	Gestión de pagos y facturación	4	5	3	12	Alto
3	Proceso	PN_GPD	Gestión de proyectos de desarrollo	4	4	2	10	Medio
4	Proceso	PN_GCS	Gestión de copias de seguridad (respaldo y restauración)	4	5	3	12	Alto
5	Proceso	PN_GAD	Gestión de adquisiciones, contrataciones y compras	4	3	3	10	Medio
6	Hardware	HW_LAP	Laptop	4	4	4	12	Alto
7	Hardware	HW_USB	Dispositivos de almacenamiento USB	2	1	1	4	Bajo
8	Software	SW_CRM	Customer Relationship Management	4	4	4	12	Alto
9	Software	SW_TL	Task List	3	3	3	9	Medio
10	Software	SW_RNS	RW Newsletter Solution	5	4	4	13	Alto
11	Software	SW_RLS	RW Loyalty Solution	5	4	4	13	Alto
12	Software	SW_SRVW	Servicios Windows	4	4	4	12	Medio
13	Software	SW_SWB	Sitios Web	3	3	3	9	Medio

14	Software	SW_SOA	Sistema Operativo y Aplicaciones	3	3	3	9	Medio
15	Información	INF_BDT	Bases de datos	5	5	4	14	Alto
16	Información	INF_RCR	Repositorio de Credenciales	5	5	4	14	Alto
17	Información	INF_DOC	Documentación	4	4	4	12	Medio
18	Servicio	SRV_COE	Correo electrónico	5	4	4	13	Alto
19	Servicio	SRV_SKY	Comunicación en tiempo real vía Skype	3	3	3	9	Medio
20	Servicio	SRV_TEC	Telefonía celular	2	2	3	7	Medio
21	Servicio	SRV_INT	Internet	2	4	4	10	Medio
22	Servicio	SRV_ALN	Almacenamiento en la nube	3	3	2	8	Medio
23	Servicio	SRV_SMS	Envío de SMS	4	4	4	12	Alto
24	Servicio	SRV_VPN	Red privada virtual	3	4	3	10	Medio
25	Servicio	SRV-CON	Servicios contables	3	4	3	10	Medio
26	Servicio	SRV_HOS	Servicio de hosting	5	5	4	14	Alto
27	Servicio	SRV_MEN	Servicio de mensajería electrónica	4	4	4	12	Alto

- Identificación de las amenazas y vulnerabilidades

  Entrada: lista categorizada de activos de TI.

  Salida: lista de amenazas y vulnerabilidades identificadas.

Procedimiento:

El responsable de riesgos elaboró una lista inicial de amenazas y vulnerabilidades, la cual fue distribuida con anticipación. La fuente principal de información fue el cuadro de amenazas incluida en el ISO/IEC 27005:2018 [10], anexos C y D, principalmente. También se consultaron registros y notificaciones de errores y problemas, tanto en sistemas como otros, reportados por clientes. Se discutieron también aspectos relacionados a la seguridad y a los problemas que se tuvieron en la empresa y que comprometieron sus activos. Finalmente, se dio cuenta de documentación inexistente o incompleta en la empresa y cómo esto afectaría las operaciones.

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES				
ACTIVO			**Amenaza**	**Vulnerabilidad**
Nr.	**Clasificación / Código**	**Nombre**		
1	Proceso PN_GCyL	Gestión de clientes y licencias	Error en uso	Extensiones de tiempo de vigencia de licencias no formalizadas.
2	Proceso PN_GPyF	Gestión de pagos y facturación	Error en uso	No todas las cuentas han sido integradas y son procesadas manualmente.
3	Proceso PN_GPD	Gestión de proyectos de desarrollo	Mala implementación	Especificaciones poco claras o incompletas para los desarrolladores.
			Incumplimiento	Estimaciones no precisas, principalmente en grandes proyectos.
			Desinformación	Deficiente documentación de los sistemas desarrollados
			Mal funcionamiento	Deficiente proceso de pruebas de software

			Incumplimiento	Cambios constantes de prioridades de proyectos.
4	Proceso PN_GCS	Gestión de copias de seguridad (respaldo y restauración)	Pérdida de información	Generación de una copia única.
				Proceso no formalizado.
5	Proceso PN_GAD	Gestión de adquisiciones y contrataciones	Sobretiempo	Proceso no formalizado.
6	Hardware HW_LAP	Laptop	Error en uso	Mantenimiento insuficiente.
			Degradación de rendimiento	Carencia de políticas de reemplazo.
			Pérdida	Falta de protección y cuidado.
			Acceso no autorizado	Falta de políticas de seguridad.
7	Hardware HW_USB	Dispositivos de almacenamiento USB	Uso inadecuado.	Mantenimiento insuficiente.
			Deterioro	Carencia de políticas de reemplazo.
			Pérdida.	Falta de protección y cuidado.
8	Software SW_CRM	Customer Relationship Management	Corrupción de datos	Proceso de importación de contactos no documentado.
			Abuso de derechos	Registro incompleto de pistas de auditoría.
			Desinformación	Insuficiente documentación.
9	Software	Task List	Abuso de derechos	Registro incompleto de pistas de auditoría.

	SW_TL		Desinformación	Insuficiente documentación.
10	Software SW_RNS	RW Newsletter Solution	Error en uso	Interfaz de usuario complicada.
			Abuso de derechos	Registro incompleto de pistas de auditoría.
			Desinformación	Insuficiente documentación.
11	Software SW_RLS	RW Loyalty Solution	Abuso de derechos	Registro incompleto de pistas de auditoría.
			Desinformación	Insuficiente documentación.
12	Software SW_SRVW	Servicios Windows	Mal funcionamiento	Deficiencias para notificar errores.
13	Software SW_SWB	Sitios Web	Inestabilidad	Uso indiscriminado de plug-ins no probados.
			Spam	Deficiente control de comentarios.
14	Software SW_SOA	Sistema Operativo cliente y aplicaciones	Malware, Spyware	Aplicaciones instaladas sin autorización.
			Suplantación. Abuso de derechos	Deficiente protección y control en el uso de contraseñas.
15	Información INF_BDT	Bases de datos	Degradación del rendimiento	Carencia de un plan de mantenimiento.
				Deficiente diseño de algunas tablas.
			Ineficiencia	Utilización de mapas en columnas.

			Suplantación	Contraseñas no protegidas en sistemas de uso interno.
16	Información INF_RCR	Repositorio de Credenciales	Abuso de derechos	Falta de control en la distribución/acceso.
			Desorganización	Deficiente control de cambios.
17	Información INF_DOC	Documentación	Desorganización	Deficiente control de versiones.
			Pérdida de documentación	Deficiente control de archivo.
18	Servicio SRV_COE	Correo electrónico	Malware	Apertura de enlaces sin examinar el destino.
			Espionaje	Uso de conexiones no seguras.
19	Servicio SRV_SKY	Comunicación en tiempo real vía Skype	Spam	Aceptación de usuarios desconocidos.
20	Servicio SRV_TEC	Telefonía celular	Espionaje, Robo de información	Conexión a señales de telefonía simuladas (cell-site simulators)
21	Servicio SRV_INT	Internet	Espionaje, Mala utilización	Permitir la conexión a usuarios no autorizados.
22	Servicio SRV_ALN	Almacenamiento en la nube	Desorganización	Falta de esquemas de organización de información.
23	Servicio SRV_SMS	Envío de SMS	Mal funcionamiento	Falta de control en la renovación del uso del servicio (pago de suscripción/crédito/cuota).
24	Servicio SRV_VPN	Red privada virtual	Abuso de derechos	Uso de cuentas de otros usuarios.
25	Servicio	Servicios contables	Abuso de derechos	Uso de cuentas de otros usuarios.

	SRV-CON			
26	Servicio SRV_HOS	Servicio de hosting	Malware, degradación de rendimiento	Instalación no autorizada de aplicaciones
			Ciberdelincuencia	Deficiente configuración de seguridad de servicios/aplicaciones.
27	Servicio SRV_MEN	Servicio de mensajería electrónica	Mala reputación	Deficiente configuración de autenticación de dominios.
				Carencia de un plan de control de ranking de dominio remitente.

2.2. Análisis del riesgo de TI

- Evaluación de la probabilidad de ocurrencia

  Se decidió utilizar una escala de 5 niveles debido a la variedad en la frecuencia de ocurrencia de eventos de riesgo. Esta escala de 5 niveles se aplica también en otros aspectos del estudio y en la matriz de riesgos final (5x5). Se hizo un muestreo de los eventos de riesgo ocurridos en los últimos 5 años (de aquellos que se tiene registro) con el fin de determinar los intervalos de ocurrencia.

ESCALAS DE PROBABILIDAD DE OCURRENCIA		
CATEGORIA	**ESCALA**	**FRECUENCIA**
Muy alta	5	Se espera que el evento ocurra más de dos veces al año.
Alta	4	Se espera que el evento ocurra al menos una vez en el último año.
Moderada	3	Se espera que el evento ocurra al menos una vez en los últimos dos años.
Baja	2	Se espera que el evento ocurra al menos una vez en los últimos cinco años.
Muy baja	1	No se ha presentado en los últimos cinco años.

- Escala de valoración del impacto:

  Al igual que el cuadro anterior, se hizo uso de una escala de 5 niveles. Se realizaron sesiones a fin de discutir y determinar los alcances de los impactos para cada nivel de valoración en tres aspectos: a. impacto sobre los ingresos, impacto sobre las operaciones e impacto sobre la imagen corporativa y los clientes.

VALORIZACIÓN DEL IMPACTO		
CATEGORIA	**ESCALA**	**DESCRIPCIÓN**
Muy alto	5	Impacto adverso severo o catastrófico: • Impacto económico de hasta el 80% de los ingresos. • Hay interrupción de todas las operaciones. • Pérdida significativa de clientes y serio daño a la imagen pública.
Alto	4	Pérdida o daño mayor: • Impacto económico de hasta el 50% de los ingresos. • Hay interrupción de las operaciones de los sistemas Web y de los servicios de distribución. • Pérdida significativa de clientes y daño a la imagen pública.
Moderado	3	Pérdida significativa: • Impacto económico de hasta el 20% de los ingresos. • Hay interrupción de las operaciones de los sistemas Web. • Posible pérdida de clientes.
Bajo	2	Pérdida o daño menor: • Impacto económico menor al 5% de los ingresos. • No hay interrupción de las operaciones. • Se afecta la imagen de la empresa con sus clientes.
Muy bajo	1	Impacto adverso insignificante: • No hay pérdida económica. • No hay interrupción de las operaciones.

		• No se afecta la imagen de la empresa.

La elaboración de la matriz de riesgos relaciona dos dimensiones: la probabilidad y el impacto de los eventos de riesgo. Como se aprecia en la figura siguiente, las celdas para cada par probabilidad-impacto fueron categorizadas y etiquetadas a fin de poder discriminar de mejor manera los riesgos una vez ubicados en la matriz. Como se apreciará más adelante, esta categorización sirve como entrada para el establecimiento de una correspondencia entre la matriz de riesgos y los niveles de apetito y tolerancia previamente establecidos.

MAPEO CUALITATIVO (MAPA DE CALOR)						
Impacto						
1 Muy Bajo	**2 Bajo**	**3 Moderado**	**4 Alto**	**5 Muy alto**		
Moderado	Moderado	Alto	Muy Alto	Muy Alto	**5 Muy alta**	**Probabilidad**
Bajo	Moderado	Alto	Muy Alto	Muy Alto	**4 Alta**	
Bajo	Moderado	Moderado	Alto	Alto	**3 Moderada**	
Muy Bajo	Bajo	Moderado	Moderado	Moderado	**2 Baja**	
Muy Bajo	Muy Bajo	Bajo	Bajo	Moderado	**1 Muy baja**	

- Determinación del nivel de riesgo, el cual fue determinado a criterio de la organización en base a las escalas de puntuación establecidas previamente. Se consultó información y registros de eventos anteriores a fin de establecer el nivel de probabilidad e impacto más preciso posible.

DETERMINACIÓN DEL NIVEL DE RIESGO								
ACTIVO			Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	
Nr.	Clasificación / Código	Nombre					Código	Nivel
1	Proceso PN_GCyL	Gestión de clientes y licencias	Error en uso	Extensiones de tiempo de vigencia de licencias no formalizadas.	3	2	R1	6 Moderado
2	Proceso PN_GPyF	Gestión de pagos y facturación	Error en uso	No todas las cuentas han sido integradas y son procesadas manualmente.	3	2	R2	6 Moderado
3	Proceso PN_GPD	Gestión de proyectos de desarrollo	Mala implementación	Especificaciones poco claras o incompletas para los desarrolladores.	4	3	R3	12 Alto
			Incumplimiento	Estimaciones no precisas, principalmente en grandes proyectos.	4	3	R4	12 Alto
			Desinformación	Deficiente documentación de los sistemas desarrollados	4	3	R5	12 Alto

			Mal funcionamiento	Deficiente proceso de pruebas de software	4	3	R6	12 Alto
			Incumplimiento	Cambios constantes de prioridades de proyectos.	4	3	R7	12 Alto
4	Proceso PN_GCS	Gestión de copias de seguridad (respaldo y restauración)	Pérdida de información	Generación de una copia única.	5	4	R8	20 Muy Alto
				Proceso no formalizado.	3	4	R9	12 Alto
5	Proceso PN_GAD	Gestión de adquisiciones y contrataciones	Sobretiempo	Proceso no formalizado.	3	2	R10	6 Moderado
6	Hardware HW_LAP	Laptop	Error en uso	Mantenimiento insuficiente.	3	2	R11	6 Moderado
			Degradación de rendimiento	Carencia de políticas de reemplazo.	2	2	R12	4 Bajo
			Pérdida	Falta de protección y cuidado.	1	3	R13	3 Bajo
			Acceso no autorizado	Falta de políticas de seguridad	2	3	R53	6 Moderado
7	Hardware HW_USB	Dispositivos de almacenamiento USB	Uso inadecuado.	Mantenimiento insuficiente.	2	2	R14	4 Bajo

			Deterioro	Carencia de políticas de reemplazo.	1	2	R15	2 Muy Bajo
			Pérdida.	Falta de protección y cuidado.	1	2	R16	2 Muy Bajo
8	Software SW_CRM	Customer Relationship Management	Corrupción de datos	Proceso de importación de contactos no documentado.	3	3	R17	9 Moderado
			Abuso de derechos	Registro incompleto de pistas de auditoría.	2	2	R18	4 Bajo
			Desinformación	Insuficiente documentación.	2	2	R19	4 Bajo
9	Software SW_TL	Task List	Abuso de derechos.	Registro incompleto de pistas de auditoría.	2	2	R20	4 Bajo
			Desinformación	Insuficiente documentación.	2	2	R21	4 Bajo
10	Software SW_RNS	RW Newsletter Solution	Error en uso	Interfaz de usuario complicada.	3	3	R22	9 Moderado
			Abuso de derechos	Registro incompleto de pistas de auditoría.	2	2	R23	4 Bajo
			Desinformación	Insuficiente documentación.	3	3	R24	9 Moderado

11	Software SW_RLS	RW Loyalty Solution	Abuso de derechos.	Registro incompleto de pistas de auditoría.	2	2	R25	4 Bajo
			Desinformación	Insuficiente documentación.	3	3	R26	9 Moderado
12	Software SW_SRVW	Servicios Windows	Mal funcionamiento	Deficiencias para notificar errores.	3	3	R27	9 Moderado
13	Software SW_SWB	Sitios Web	Inestabilidad	Uso indiscriminado de plug-ins no probados.	3	3	R28	9 Moderado
			Spam	Deficiente control de comentarios	1	2	R29	2 Muy Bajo
14	Software SW_SOA	Sistema Operativo y Aplicaciones	Malware, Spyware	Instalación de aplicaciones no autorizadas.	2	4	R30	8 Moderado
			Suplantación. Abuso de derechos	Deficiente protección y control en el uso de contraseñas.	3	4	R31	12 Alto
15	Información INF_BDT	Bases de datos	Degradación del rendimiento	Carencia de un plan de mantenimiento.	3	4	R32	12 Alto
				Deficiente diseño de algunas tablas.	3	4	R33	12 Alto
			Ineficiencia	Utilización de mapas en columnas.	3	4	R34	12 Alto

			Suplantación	Contraseñas no protegidas en sistemas de uso interno.	2	4	R35	8 Moderado
16	Información INF_RCR	Repositorio de Credenciales	Abuso de derechos	Falta de control en la distribución/acceso.	3	4	R36	12 Alto
			Desorganización	Deficiente control de cambios.	4	3	R37	12 Alto
17	Información INF_DOC	Documentación	Desorganización	Deficiente control de versiones.	4	3	R38	12 Alto
			Pérdida de documentación	Deficiente control de archivo.	4	3	R39	12 Alto
18	Servicio SRV_COE	Correo electrónico	Malware	Apertura de enlaces sin examinar el destino.	3	4	R40	12 Alto
			Espionaje	Uso de conexiones no seguras.	2	4	R41	8 Moderado
19	Servicio SRV_SKY	Comunicación en tiempo real vía Skype	Spam	Aceptación de usuarios desconocidos.	1	3	R42	3 Bajo
20	Servicio SRV_TEC	Telefonía celular	Espionaje, Robo de información	Conexión a señales de telefonía simuladas (cell-site simulators)	2	3	R43	6 Moderado

21	Servicio SRV_INT	Internet	Espionaje, Mala utilización	Permitir la conexión a usuarios no autorizados.	3	3	R44	9 Moderado
22	Servicio SRV_ALN	Almacenamiento en la nube	Desorganización	Falta de esquemas de organización de información.	3	3	R45	9 Moderado
23	Servicio SRV_SMS	Envío de SMS	Mal funcionamiento	Falta de control en la renovación del uso del servicio (pago de suscripción/crédito/cuota).	3	4	R46	12 Alto
24	Servicio SRV_VPN	Red privada virtual	Abuso de derechos	Uso de cuentas de otros usuarios.	3	3	R47	9 Moderado
25	Servicio SRV-CON	Servicios contables	Abuso de derechos	Uso de cuentas de otros usuarios.	3	3	R48	9 Moderado
26	Servicio SRV_HOS	Servicio de hosting	Malware, degradación de rendimiento	Instalación no autorizada de aplicaciones	2	4	R49	8 Moderado
			Ciberdelincuencia	Deficiente configuración de seguridad de servicios/aplicaciones.	1	4	R50	4 Bajo
27	Servicio SRV_MEN	Servicio de mensajería electrónica	Mala reputación	Deficiente configuración de autenticación de dominios.	3	4	R51	12 Alto
				Carencia de un plan de control de ranking de dominio remitente.	1	4	R52	4 Bajo

2.3. Evaluación del riesgo de TI

- Priorización del riesgo

Impacto						
1 Muy Bajo	**2 Bajo**	**3 Moderado**	**4 Alto**	**5 Muy alto**		
			R8		**5 Muy alta**	**Probabilidad**
		R3, R4, R5, R6, R7, R9, R37, R38, R39			**4 Alta**	
	R1, R2, R10, R11	R17, R22, R24, R26, R27, R28, R44, R45, R47, R48	R31, R32, R33, R34, R36, R40, R46, R51		**3 Moderada**	
	R12, R14, R18, R19, R20, R21, R23, R25	R43, R53	R30, R35, R41, R49		**2 Baja**	
	R15, R16, R29	R13, R42	R50, R52		**1 Muy baja**	

De acuerdo al mapa de calor resultante se presenta la siguiente tabla con las escalas de criticidad del riesgo inherente:

NIVEL DE CRITICIDAD DEL RIESGO INHERENTE		
Rango de resultados	**Nivel de riesgo**	
De 1 a 4	Bajo	
De 5 a 10	Moderado	
De 12 a 25	Alto	

- Establecimiento de los niveles de apetito y tolerancia

Impacto						
1 Muy Bajo	2 Bajo	3 Moderado	4 Alto	5 Muy alto		
					5 Muy alta	Probabilidad
					4 Alta	
					3 Moderada	
					2 Baja	
					1 Muy baja	

VALORIZACIÓN DE LA TOLERANCIA	
Nivel de riesgo	**Valorización**
Bajo	Aceptable
Moderado	Tolerable
Alto	Intolerable

FASE III. Análisis del impacto del negocio (BIA)

3.1. Identificación de las funciones y procesos/servicios

El responsable de riesgos elaboró una lista inicial de las funciones y procesos de la organización, que fue discutida y depurada en reuniones con el CEO y CTO. La nomenclatura utilizada es propia y sirvió para identificar a los procesos en los pasos subsiguientes. Se utilizó como fuente de información la "Guía para realizar el Análisis de Impacto de Negocios BIA" [38] y se consultó documentación de la empresa a fin de determinar claramente qué procesos y servicios serían finalmente considerados en el BIA, teniendo como prioridad a los procesos relacionados con el cliente (licencias, facturación, etc.) y luego a los de operación interna (control de tareas, servicios, etc.).

FUNCIONES y PROCESOS			
Función		**Proceso / Servicio**	
Cód.	**Nombre**	**Cód.**	**Nombre**
F01	Clientes	PS01	Gestión de clientes y licencias
F02	Finanzas	PS02	Gestión de pagos y facturación
F03	Operaciones	PS03	Gestión de proyectos de desarrollo
		PS04	Gestión de copias de seguridad (respaldo y restauración)
F04	Proveedores	PS05	Gestión de adquisiciones y contrataciones
F05	Aplicaciones	PS06	Customer Relationship Management
		PS07	Task List
		PS08	RW Newsletter Solution
		PS09	RW Loyalty Solution
		PS10	Servicios Windows
F06	Web	PS11	Sitios Web
F07	Comunicaciones	PS12	Correo electrónico
		PS13	Internet
F08	Servicios	PS14	Envío de SMS
		PS15	Red privada virtual

		PS16	Hosting
		PS17	Servicio de mensajería electrónica

3.2. Establecimiento del nivel de criticidad de las funciones y procesos/servicios

Se utilizará el siguiente esquema de valoración, el cual es una adaptación de [38, p. 16]:

CRITICIDAD DE LAS OPERACIONES		
Categoría	**Nombre**	**Descripción**
1	Crítico	La función del negocio no puede realizarse si no se cuenta con ésta.
2	Importante	La operación es parte del negocio y sin ella el negocio no podría operar normalmente.
3	Menor	La operación no es una parte integral del negocio.

Con la tabla descrita, se procede a establecer el nivel de criticidad de las funciones y procesos. Las valoraciones fueron establecidas a lo largo de varias reuniones con miembros de las áreas involucradas. Se determinaron los escenarios posibles y sus consecuencias para cada caso, los que se describen en la columna "Comentario":

CRITICIDAD DE FUNCIONES y PROCESOS					
Función		**Proceso / Servicio**		**Criticidad**	**Comentario**
Cód.	**Nombre**	**Cód.**	**Nombre**		
F01	Clientes	PS01	Gestión de clientes y licencias	1 – Crítico	No se podrían incorporar nuevos clientes ni renovar las licencias y cuentas próximas a expirar.

F02	Finanzas	PS02	Gestión de pagos y facturación	2 – Importante	No se podría efectuar a tiempo el pago a los empleados y proveedores, ni generar/enviar a tiempo las facturas a los clientes.
F03	Operaciones	PS03	Gestión de proyectos de desarrollo	2 – Importante	No se gestionarían de manera efectiva los proyectos de desarrollo.
		PS04	Gestión de copias de seguridad (respaldo y restauración)	2 – Importante	No se generarían las copias de seguridad de los archivos que pudieran requerirse ante un evento de riesgo que afecte a los archivos originales.
F04	Proveedores	PS05	Gestión de adquisiciones y contrataciones	3 – Menor	No se podría realizar formalmente la contratación de nuevo personal o asesores. No se podrían adquirir bienes o servicios mediante el procedimiento regular.
F05	Aplicaciones	PS06	Customer Relationship Management	2 – Importante	No se gestionarían adecuadamente las comunicaciones con potenciales clientes ni se podría mantener actualizada la información de los clientes existentes.
		PS07	Task List	3 – Menor	No se podrían registrar las tareas, progresos y horas empleadas en la ejecución de tareas.
		PS08	RW Newsletter Solution (RNS)	1 – Crítico	Los clientes no podrían utilizar el sistema.
		PS09	RW Loyalty Solution (RLS)	1 – Crítico	Los clientes no podrían utilizar el sistema.

		PS10	Servicios Windows	2 – Importante	No se ejecutarían ciertas tareas relacionadas con los sistemas RNS y RLS, tales como: importación de destinatarios/lectores, distribución de boletines/encuestas, lectura de archivos externos, sincronizaciones, etc.
F06	Web	PS11	Sitios Web	1 – Menor	Los sitios web no estarían disponibles. Son utilizados como imagen de la empresa y para publicar información (blog)
F07	Comunicaciones	PS12	Correo electrónico	2 – Importante	No se podrían atender las comunicaciones de los clientes ni enviar mensajes.
		PS13	Internet	2 – Importante	No se tendría acceso a ningún servicio que dependa de Internet.
F08	Servicios	PS14	Envío de SMS	1 – Crítico	No se podría realizar la distribución de encuestas mediante envío de SMS.
		PS15	Red privada virtual	2 – Importante	No se podría tener acceso a los servidores.
		PS16	Servidores de producción	1 – Crítico	No estarían disponibles los servidores, y por ende, los sistemas que utilizan los clientes.
		PS17	Servicio de mensajería electrónica	1 – Crítico	No se podría realizar la distribución de encuestas mediante envío de correo electrónico.

3.3. Evaluación de impacto

Para la evaluación del impacto se han considerado las siguientes áreas de impacto:

- Impacto financiero.
- Impacto en el cliente.
- Impacto en imagen y reputación.

Para todos los casos se ha considerado una escala de 5 niveles:

ESCALA DE IMPACTO POR ÁREA				
IMPACTO		**ÁREA**		
Nivel	**Categoría**	**Financiero**	**Cliente**	**Imagen / Reputación**
1	Insignificante	Si el proceso no se encuentra disponible, no hay pérdidas ni afectación de los ingresos de la empresa.	Si el proceso no se encuentra disponible, no se afecta la imagen de la empresa con los clientes.	Si el proceso no se encuentra disponible, no se afecta la imagen pública de la empresa.
2	Bajo	Si el proceso no se encuentra disponible, tiene un impacto menor en los ingresos (5% de los ingresos) que no afectaría su rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes, pero no se pierde ninguno.	Si el proceso no se encuentra disponible, la imagen pública de la empresa podría verse afectada.
3	Moderado	Si el proceso no se encuentra disponible, tiene un impacto moderado en los ingresos (20% de los ingresos) y la rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes más importantes, perdiéndose algunos de ellos.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa.
4	Significativo	Si el proceso no se encuentra disponible, tiene un impacto significativo (50% de los ingresos), afecta la rentabilidad, pero no la sostenibilidad del negocio.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa con los clientes, generándose una pérdida significativa.	Si el proceso no se encuentra disponible, se afecta significativamente la imagen de la empresa, dando ventaja competitiva a la competencia.
5	Severo	Si el proceso no se encuentra disponible, tiene un impacto severo generando pérdida económica (80% de los ingresos), afectando la rentabilidad y su continuidad en el mercado.	Si el proceso no se encuentra disponible, se afecta seriamente la imagen de la empresa y hay pérdida masiva de clientes.	Si el proceso no se encuentra disponible, afecta totalmente la imagen de la empresa, perdiendo posicionamiento.

Para el análisis del impacto se han considerado además 7 escalas de tiempo:

- 0 – 1 horas.
- 1 – 4 horas.
- 4 – 8 horas.
- 8 – 24 horas.
- 24 – 48 horas.
- 48 – 72 horas.
- +72 horas.

Nota: Las tablas siguientes muestran las escalas de impacto para cada proceso o servicio en cada escala de tiempo, es decir, cuál sería el impacto para la organización si el proceso o servicio no se lleva a cabo en el transcurso de intervalos de tiempo. Esto permite determinar el nivel de afectación para la organización conforme transcurren las horas y da luces para poder determinar más adelante qué procesos o servicios resultan críticos para la continuidad del negocio, lo que a su vez permite que se adopten medidas correctivas o se propongan procesos alternos que garanticen de alguna manera que las operaciones sostengan la continuidad.

Al igual que los casos anteriores, estas valoraciones fueron establecidas por la organización durante varias sesiones. Se consultó información disponible sobre eventos ocurridos anteriormente.

Evaluación del impacto financiero en procesos críticos:

EVALUACIÓN DEL IMPACTO FINANCIERO								
Proceso / Servicio		**TIEMPOS (horas)**						
Cód.	**Nombre**	**0 - 1**	**1 - 4**	**4 - 8**	**8 - 24**	**24 - 48**	**48 - 72**	**+72**
PS01	Gestión de clientes y licencias	1	1	1	1	2	2	3
PS08	RW Newsletter Solution (RNS)	1	1	1	2	2	3	4

PS09	RW Loyalty Solution (RLS)	1	1	1	2	2	3	4
PS14	Envío de SMS	1	1	1	1	2	2	2
PS16	Servidores de producción	1	1	1	2	3	3	4
PS17	Servicio de mensajería electrónica	1	1	1	1	2	2	3

Evaluación del impacto con los clientes en procesos críticos:

EVALUACIÓN DEL IMPACTO CON LOS CLIENTES								
Proceso / Servicio		**TIEMPOS (horas)**						
Cód.	**Nombre**	**0 - 1**	**1 - 4**	**4 - 8**	**8 - 24**	**24 - 48**	**48 - 72**	**+72**
PS01	Gestión de clientes y licencias	1	1	1	1	2	3	4
PS08	RW Newsletter Solution (RNS)	1	1	1	2	3	4	4
PS09	RW Loyalty Solution (RLS)	1	1	1	2	3	4	4
PS14	Envío de SMS	1	1	1	1	2	3	3
PS16	Servidores de producción	1	1	1	2	3	3	4
PS17	Servicio de mensajería electrónica	1	1	1	1	2	2	3

Evaluación del impacto con la imagen/reputación en procesos críticos:

EVALUACIÓN DEL IMPACTO CON LA IMAGEN / REPUTACIÓN								
Proceso / Servicio		**TIEMPOS (horas)**						
Cód.	**Nombre**	**0 - 1**	**1 - 4**	**4 - 8**	**8 - 24**	**24 - 48**	**48 - 72**	**+72**
PS01	Gestión de clientes y licencias	1	1	1	1	2	3	3

PS08	RW Newsletter Solution (RNS)	1	1	1	2	3	3	4
PS09	RW Loyalty Solution (RLS)	1	1	1	2	3	3	4
PS14	Envío de SMS	1	1	1	1	2	3	3
PS16	Servidores de producción	1	1	1	2	3	3	4
PS17	Servicio de mensajería electrónica	1	1	1	1	2	3	3

La organización estableció además un grado de importancia a cada una de las áreas de impacto:

GRADO DE IMPORTANCIA DE LAS ÁREAS	
ÁREA	**PORCENTAJE**
Financiero	30%
Clientes	50%
Imagen y reputación	20%
TOTAL	100%

Fuente: Elaboración propia

Con el análisis de los impactos en el tiempo y los porcentajes asignados, obtenemos la siguiente tabla consolidada. La puntuación final se logra calculando el promedio ponderado de las puntuaciones parciales en cada intervalo de tiempo multiplicado por el porcentaje de importancia asignado al área:

EVALUACIÓN DEL IMPACTO - CONSOLIDACIÓN								
Proceso / Servicio		**TIEMPOS (horas)**						
Cód.	**Nombre**	**0 - 1**	**1 - 4**	**4 - 8**	**8 - 24**	**24 - 48**	**48 - 72**	**+72**
PS01	Gestión de clientes y licencias	1	1	1	1	2	3	4

PS08	RW Newsletter Solution (RNS)	1	1	1	2	3	4	4
PS09	RW Loyalty Solution (RLS)	1	1	1	2	3	4	4
PS14	Envío de SMS	1	1	1	1	2	3	3
PS16	Servidores de producción	1	1	1	2	3	3	4
PS17	Servicio de mensajería electrónica	1	1	1	1	2	2	3

3.4. Evaluación de tiempos.

Los tiempos de recuperación se describen a continuación:

TIEMPOS DE RECUPERACIÓN	
Tiempo	**Descripción**
MTD (Maximum Torerable Downtime, Tiempo de inactividad máximo tolerable)	Es el tiempo máximo que un negocio puede tolerar la ausencia o indisponibilidad de una función/proceso particular de negocio. MTD = RTO + WRT
RTO (Recovery Time Objective, Tiempo de recuperación objetivo)	Es el tiempo disponible para recuperar sistemas y recursos interrumpidos.
WRT (Work Recovery Time, Tiempo de recuperación del trabajo)	Es el tiempo que toma recuperar y volver a poner en funcionamiento funciones/procesos críticos del negocio, una vez que los sistemas han sido restaurados.
RPO (Recovery Point Objective, Punto de recuperación objetivo)	Cantidad o magnitud de pérdida de datos –en términos de un período de tiempo– que puede ser tolerado por los sistemas críticos del negocio.

Teniendo como base la tabla de evaluación de impacto se establecieron los tiempos correspondientes. En algunos casos se tomó el tiempo máximo posible de la categoría de impacto más baja y en otros se optó por adicionar algunas horas más allá de este límite. La tabla se presenta a continuación.

FUNCIONES/PROCESOS CRITICOS y TIEMPOS DE RECUPERACIÓN							
Función		**Proceso / Servicio**		**TIEMPOS (horas)**			
Cód.	**Nombre**	**Cód.**	**Nombre**	**MTD**	**RTO**	**WRT**	**RPO**
F01	Clientes	PS01	Gestión de clientes y licencias	24	20	04	06
F05	Aplicaciones	PS08	RW Newsletter Solution (RNS)	12	08	04	06
		PS09	RW Loyalty Solution (RLS)	12	08	04	06
F08	Servicios	PS14	Envío de SMS	16	12	04	06
		PS16	Servidores de producción	08	06	02	06
		PS17	Servicio de mensajería electrónica	16	12	04	06

Requisitos para la implementación de procesos alternos

Debido a que los servicios brindados por la empresa son dependientes de un entorno conectado a Internet y teniendo en cuenta que la empresa no cuenta con recursos, equipos ni servicios de respaldo, se plantea la implementación, adquisición o contratación de los mismos a fin de poder trasladar la operación a un entorno de respaldo en casos donde las operaciones se vean interrumpidas.
Los recursos a implementar, adquirir o contratar se listan a continuación:

- *Implementación del módulo de creación de cuentas temporales*, en los sistemas RLS y RNS, a fin de poder permitir que un nuevo cliente puede empezar a utilizar los servicios, aun cuando el proceso de registro de cuenta y licencia no se ha concretado. Este módulo debe incluir la tarea de migrar los datos a la cuenta oficial luego de restauradas las operaciones, o de promover la cuenta existente a una cuenta pagada, incluyendo sus usuarios y cuotas de uso.

- *Contratación de hosting alterno*, para los servidores de producción: contratar el servicio de alojamiento para los servidores de bases de datos y Web. Se sugiere la contratación de un solo servidor para ambos fines pues su operación será por un periodo determinado, mientras se restituyan los servicios/equipos originales. Se presentan dos propuestas para su consideración:

COTIZACIÓN SERVICIO DE HOSTING		
Proveedor	**Plan / Características**	**Precio**
eUKHost	eUK E3 Professional CPU Model: Intel Xeon E3-1230, 3.4GHz ◆ CPU Cores/Threads: 4 Cores / 8 Threads ◆ RAM: 16GB DDR4 (Max 64GB) ◆ Hard Disk: 2 x 1TB 7.2K SATA Port Speed: 1 Gbit ◆ Monthly Bandwith: 10TB ◆ Managed: 24x7 ◆ CPU Speed: 3.4GHz / 3.8Ghz Turbo ◆ CPU Cache: 8MB CPU Cache ◆ RAID: RAID 1 ◆ Hardware Firewall: Fortigate Firewall ◆ Operating System: Windows Server 2016	USD 112.10 /month (ex VAT) x2 servidores (Web, Base de datos) USD 224.20 /month
Contabo	Contabo VPS L SSD Performance: CPU: eight cores ◆ Intel® Xeon® E5-2620v3, E5-2630v4 or 4114 processor ◆ 30 GB RAM (guaranteed) ◆ 800 GB disk space (100% SSD) ◆ 100% SSD disk space. Networking: Unlimited traffic ◆ 600 Mbit/s port ◆ DDoS protection. Operative System: Windows Server 2012R2 (64 bit) Backup space: 500GB ◆	USD 108.00/month (ex VAT) x2 servidores (Web, Base de datos) USD 216.00 /month

Fuente: Elaboración propia (la información contenida proviene de las páginas web de las empresas proveedoras del servicio y de los correos recibidos como respuesta a consultas)

- *Adquisición de una cuenta adicional para el servicio de distribución masiva de correos electrónicos*. Actualmente la empresa depende de un solo proveedor para el servicio de distribución masiva de correo electrónico (SendGrid). La adquisición de una cuenta alterna permitiría mantener el servicio operando en tiempo récord.

- *Adquisición de cuentas adicionales para los servicios de distribución masiva de mensajes de texto a teléfonos celulares*. En este caso, todas las empresas cobran bajo la modalidad de "pay as you go" (pague según consumo) de tal forma que no implicaría mayores gastos a la empresa, pues en caso de no consumo, se paga una tarifa de mantenimiento de cuenta mínimo (menor a 5 USD en la mayoría de casos)

- *Implementar el módulo de registro y seguimiento de incidentes,* a fin de poder registrar y monitorear los incidentes y poder anticipar posibles interrupciones en las operaciones. Se propone el siguiente formato, el cual sería implementado como un módulo adicional dentro del sistema TaskList. El formato se encuentra disponible en el anexo 6 > 6.23b. A continuación se muestra un caso real de registro de incidente utilizando el formato citado (*se han modificado algunos datos a efectos de mantener la confidencialidad de la información*):

REPORTE DE INCIDENTE [CÓDIGO]	
Fecha	12 / JUN / 2018
De	Jorge Rodríguez
Información de contacto	jorge@empresa.dk (+51 979651377)
Para	Steven Andersen sa@empresa.dk
El incidente fue detectado / observado / descubierto el día: 12 / JUN / 2018 a horas: 08:50 AM, en: Módulo de importación de contactos de distribución.	
Prioridad: ○ 1 = baja ● 3 = Media ○ 5 = alta	
Sistema(s) afectado(s)	RW Loyalty System
Información afectada	Información de 275 contactos de distribución nuevos importados para el cliente Cliente XYZ.
Descripción del incidente	Se revisó la configuración de la cuenta y del plan de distribución a ejecutarse en la segunda fase del programa de la empresa –a solicitud del cliente- y se detectó que había 275 contactos recientemente importados (de un total de 1244) que serían excluidos del proceso. Se

	revisó la lista de contactos excluidos y se encontró que sus datos estaban incompletos. Se procedió a revisar el archivo original utilizado en la importación y los datos están completos, razón por la cual se concluye que hubo un error o problema durante la importación.
Acciones ejecutadas	Se importaron los datos del archivo, en un grupo separado –sin asociarlos al programa de distribución. Los contactos fueron importados, pero la información de 275 contactos, de un total de 1244, está incompleta.
Acciones recomendadas	• Revisar el log del Servicio Windows de importación de contactos. • Realizar una importación parcial del archivo (100 primera filas) y determinar si el problema reside en el archivo. • Realizar una importación desde un archivo nuevo, copiando datos del archivo original (100 primeras filas). SOLO DATOS. Utilizar la función de pegado especial de Excel.
Personas a contactar	Luis Velasco (Desarrollo)
Información adicional	El cliente puede postergar la distribución hasta 2 días como máximo, esto es, hasta el 14 / JUN / 2018
Comentarios post-gestión del incidente	• El archivo contenía filas corruptas y celdas combinadas. • Contactar al cliente y recordarle acerca de los requerimientos de los archivos utilizados en los procesos de importación. • Considerar el adelanto de la fecha de activación del módulo de validación de archivos para este cliente.

Fuente: Elaboración propia

3.5. Identificación de procesos alternos

Dado que el núcleo del negocio se centra en la provisión de servicios de información a través de Internet y teniendo en cuenta que la organización no cuenta con ningún plan de gestión de crisis, se proponen los siguientes procesos alternos. Luego de la valoración de los procesos y la determinación de aquellos que resultaban críticos, el responsable de riesgos, junto al CTO y miembros de las áreas involucradas plantearon los posibles procesos alternos, teniendo en cuenta aspectos de factibilidad técnica, costos y tiempo:

PROCESOS ALTERNOS Y PROCEDIMIENTOS DE RECUPERACIÓN					
Proceso / Servicio		**Proceso alterno**			
Cód.	**Nombre**	**Descripción**	**Acciones**	**Responsables**	**Recursos**
PS01	Gestión de clientes y licencias	Registro y creación de cuenta temporal.	1. Comunicación con el cliente. 2. Realizar el registro en el formato correspondiente. 3. Establecer los tiempos de extensión de licencia como compensación. 4. Activación del sitio Web alterno de control de cuentas. 5. Creación de una cuenta temporal en el sistema correspondiente.	Customer Satisfaction	• Directorio de contactos (clientes). • Formato de registro de cliente.
PS08	RW Newsletter Solution (RNS)	Activación de aplicación Web alterna.	1. Activación de aplicación Web alterna. 2. Activar la redirección de inicios de sesión desde el Sitio Web (portal). 3. Verificar inicio de sesión. 4. Comunicar al cliente sobre el restablecimiento del servicio.	CTO, Development Team	• Credenciales de los servicios a activar.
PS09	RW Loyalty Solution (RLS)				
PS14	Envío de SMS	Activación de servicio alterno.	1. Reconfiguración del servicio de distribución. 2. Ejecución de distribución de prueba (cuenta de prueba) 3. Ejecución de distribuciones pendientes.	CTO, Development Team	• Credenciales de los servicios a activar.

					• Códigos actualizados de API.
PS16	Servidores de producción	Activación de servidor de respaldo.	1. Activación del servidor de producción alterno. 2. Verificación de la versión de los sistemas Web instalados. 3. Traslado de sistemas Web, si fuera el caso. 4. Generación de copias de seguridad y restauración de las bases de datos, o verificación del estado de replicación, si fuera el caso. 5. Pruebas de inicio de sesión y acceso. 6. Puesta en marcha del servidor de producción alterno. 7. Comunicar al cliente sobre el restablecimiento del servicio.	CTO, Development Team	• Credenciales de los servicios a activar. • Cuentas y dominios activos.
PS17	Servicio de mensajería electrónica	Activación de servicio alterno	1. Reconfiguración del servicio de distribución para los distribuidores comprometidos. 2. Ejecución de distribución de prueba para cada distribuidor comprometido (cuenta de prueba) 3. Ejecución de distribuciones pendientes.	CTO, Development Team	• Credenciales de los servicios a activar. • Número telefónicos actualizados de cuenta remitente.

3.6. Generación de informe de impacto de negocio

Se generó un reporte con el análisis realizado y los resultados obtenidos, teniendo en cuenta la siguiente estructura y formato:

INFORME DE IMPACTO DE NEGOCIO

Elaborado por: Comité de riesgos

Versión: 1.0 Fecha: / /

Dirigido a: CEO, CTO

El equipo de gestión de riesgos ha realizado el análisis de impacto de continuidad para la organización y pone a su disposición el informe resumen del proceso y sus resultados. El informe incluye 4 cuadros resumen y 3 anexos.

- Cuadro 1: Resumen de procesos y funciones de negocio, indicando su nivel de criticidad.
- Cuadro 2: Resumen de la evaluación de impacto (consolidado) en 7 rangos de tiempo.
- Cuadro 3: Resumen con los tiempos de recuperación estimados.
- Cuadro 4: Procesos alternos y procedimientos de recuperación para los procesos críticos.

Anexos:

- Anexo 1. Escala de criticidad de las operaciones.
- Anexo 2. Escala de impacto por área.
- Anexo 3. Descripción de los tiempos de recuperación.

Cuadro 1. CRITICIDAD DE FUNCIONES y PROCESOS

Función		Proceso / Servicio		Criticidad	Comentario
Cód.	Nombre	Cód.	Nombre		
F01	Clientes	PS01	Gestión de clientes y licencias	1 – Crítico	No se podrían incorporar nuevos clientes ni renovar las licencias y cuentas próximas a expirar.
F02	Finanzas	PS02	Gestión de pagos y facturación	2 – Importante	No se podría efectuar a tiempo el pago a los empleados y proveedores, ni generar/enviar a tiempo las facturas a los clientes.

	F03	Operaciones	PS03	Gestión de proyectos de desarrollo	2 – Importante	No se gestionarían de manera efectiva los proyectos de desarrollo.	
			PS04	Gestión de copias de seguridad (respaldo y restauración)	2 – Importante	No se generarían las copias de seguridad de los archivos que pudieran requerirse ante un evento de riesgo que afecte a los archivos originales.	
	F04	Proveedores	PS05	Gestión de adquisiciones y contrataciones	3 – Menor	No se podría realizar formalmente la contratación de nuevo personal o asesores. No se podrían adquirir bienes o servicios mediante el procedimiento regular.	
	F05	Aplicaciones	PS06	Customer Relationship Management	2 – Importante	No se gestionarían adecuadamente las comunicaciones con potenciales clientes ni se podría mantener actualizada la información de los clientes existentes.	
			PS07	Task List	3 – Menor	No se podrían registrar las tareas, progresos y horas empleadas en la ejecución de tareas.	
			PS08	RW Newsletter Solution (RNS)	1 – Crítico	Los clientes no podrían utilizar el sistema.	
			PS09	RW Loyalty Solution (RLS)	1 – Crítico	Los clientes no podrían utilizar el sistema.	
			PS10	Servicios Windows	2 – Importante	No se ejecutarían ciertas tareas relacionadas con los sistemas RNS y RLS, tales como: importación de destinatarios/lectores, distribución de boletines/encuestas, lectura de archivos externos, sincronizaciones, etc.	

F06	Web	PS11	Sitios Web	1 – Menor	Los sitios web no estarían disponibles. Son utilizados como imagen de la empresa y para publicar información (blog)
F07	Comunicaciones	PS12	Correo electrónico	2 – Importante	No se podrían atender las comunicaciones de los clientes ni enviar mensajes.
		PS13	Internet	2 – Importante	No se tendría acceso a ningún servicio que dependa de Internet.
F08	Servicios	PS14	Envío de SMS	1 – Crítico	No se podría realizar la distribución de encuestas mediante envío de SMS.
		PS15	Red privada virtual	2 – Importante	No se podría tener acceso a los servidores.
		PS16	Servidores de producción	1 – Crítico	No estarían disponibles los servidores, y por ende, los sistemas que utilizan los clientes.
		PS17	Servicio de mensajería electrónica	1 – Crítico	No se podría realizar la distribución de encuestas mediante envío de correo electrónico.

Cuadro 2. EVALUACIÓN DEL IMPACTO - CONSOLIDACIÓN

Proceso / Servicio		**TIEMPOS (horas)**						
Cód.	**Nombre**	**0 - 1**	**1 - 4**	**4 - 8**	**8 - 24**	**24 - 48**	**48 - 72**	**+72**
PS01	Gestión de clientes y licencias	1	1	1	1	2	3	4
PS08	RW Newsletter Solution (RNS)	1	1	1	2	3	4	4
PS09	RW Loyalty Solution (RLS)	1	1	1	2	3	4	4
PS14	Envío de SMS	1	1	1	1	2	3	3

PS16	Servidores de producción	1	1	1	2	3	3	4
PS17	Servicio de mensajería electrónica	1	1	1	1	2	2	3

Cuadro 3. FUNCIONES/PROCESOS CRITICOS y TIEMPOS DE RECUPERACIÓN

Función		**Proceso / Servicio**		**TIEMPOS (horas)**			
Cód.	**Nombre**	**Cód.**	**Nombre**	**MTD**	**RTO**	**WRT**	**RPO**
F01	Clientes	PS01	Gestión de clientes y licencias	24	20	04	06
F05	Aplicaciones	PS08	RW Newsletter Solution (RNS)	12	08	04	06
		PS09	RW Loyalty Solution (RLS)	12	08	04	06
F08	Servicios	PS14	Envío de SMS	16	12	04	06
		PS16	Servidores de producción	08	06	02	06
		PS17	Servicio de mensajería electrónica	16	12	04	06

Cuadro 4. PROCESOS ALTERNOS Y PROCEDIMIENTOS DE RECUPERACIÓN

Proceso / Servicio		**Proceso alterno**			
Cód.	**Nombre**	**Descrip.**	**Acciones**	**Respons.**	**Recursos**
PS01	Gestión de clientes y licencias	Registro y creación de cuenta temporal.	1. Comunicación con el cliente. 2. Realizar el registro en el formato correspondiente. 3. Establecer los tiempos de extensión de licencia como compensación. 4. Activación del sitio Web alterno de control de cuentas. 5. Creación de una cuenta temporal en el sistema correspondiente.	Customer Satisfaction	• Directorio de contactos (clientes). • Formato de registro de cliente.

PS08	RW Newsletter Solution (RNS)	Activación de aplicación Web alterna.	1. Activación de aplicación Web alterna. 2. Activar la redirección de inicios de sesión desde el Sitio Web (portal). 3. Verificar inicio de sesión. 4. Comunicar al cliente sobre el restablecimiento del servicio.	CTO, Development Team	• Credenciales de los servicios a activar.
PS09	RW Loyalty Solution (RLS)				
PS14	Envío de SMS	Activación de servicio alterno.	1. Reconfiguración del servicio de distribución. 2. Ejecución de distribución de prueba (cuenta de prueba) 3. Ejecución de distribuciones pendientes.	CTO, Development Team	• Credenciales de los servicios a activar. • Códigos actualizados de API.
PS16	Servidores de producción	Activación de servidor de respaldo.	1. Activación del servidor de producción alterno. 2. Verificación de la versión de los sistemas Web instalados. 3. Traslado de sistemas Web, si fuera el caso. 4. Generación de copias de seguridad y restauración de las bases de datos, o verificación del estado de replicación, si fuera el caso. 5. Pruebas de inicio de sesión y acceso. 6. Puesta en marcha del servidor de producción alterno. 7. Comunicar al cliente sobre el restablecimiento del servicio.	CTO, Development Team	• Credenciales de los servicios a activar. • Cuentas y dominios activos.
PS17	Servicio de mensajería electrónica	Activación de servicio alterno	1. Reconfiguración del servicio de distribución para los distribuidores comprometidos. 2. Ejecución de distribución de prueba para cada distribuidor comprometido (cuenta de prueba) 3. Ejecución de distribuciones pendientes.	CTO, Development Team	• Credenciales de los servicios a activar. • Número telefónicos actualizados de cuenta remitente.

Anexos:

Anexo 1. CRITICIDAD DE LAS OPERACIONES		
Categoría	**Nombre**	**Descripción**
1	Crítico	La función del negocio no puede realizarse si no se cuenta con ésta.
2	Importante	La operación es parte del negocio y sin ella el negocio no podría operar normalmente.
3	Menor	La operación no es una parte integral del negocio.

Anexo 2. ESCALA DE IMPACTO POR ÁREA				
IMPACTO		**ÁREA**		
Nivel	**Categoría**	**Financiero**	**Cliente**	**Imagen / Reputación**
1	Insignificante	Si el proceso no se encuentra disponible, no hay pérdidas ni afectación de los ingresos de la empresa.	Si el proceso no se encuentra disponible, no se afecta la imagen de la empresa con los clientes.	Si el proceso no se encuentra disponible, no se afecta la imagen pública de la empresa.
2	Bajo	Si el proceso no se encuentra disponible, tiene un impacto menor en los ingresos (5% de los ingresos) que no afectaría su rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes, pero no se pierde ninguno.	Si el proceso no se encuentra disponible, la imagen pública de la empresa podría verse afectada.
3	Moderado	Si el proceso no se encuentra disponible, tiene un impacto moderado en los ingresos (20% de los ingresos) y la rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes más importantes, perdiéndose algunos de ellos.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa.
4	Significativo	Si el proceso no se encuentra disponible, tiene un impacto significativo (50% de los ingresos), afecta la rentabilidad, pero no la sostenibilidad del negocio.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa con los clientes, generándose una pérdida significativa.	Si el proceso no se encuentra disponible, se afecta significativamente la imagen de la empresa, dando ventaja competitiva a la competencia.
5	Severo	Si el proceso no se encuentra disponible, tiene un impacto severo generando pérdida económica (80% de los ingresos), afectando la rentabilidad y su continuidad en el mercado.	Si el proceso no se encuentra disponible, se afecta seriamente la imagen de la empresa y hay pérdida masiva de clientes.	Si el proceso no se encuentra disponible, afecta totalmente la imagen de la empresa, perdiendo posicionamiento.

Anexo 3. TIEMPOS DE RECUPERACIÓN	
Tiempo	**Descripción**
MTD (Maximum Torerable Downtime, Tiempo de inactividad máximo tolerable)	Es el tiempo máximo que un negocio puede tolerar la ausencia o indisponibilidad de una función/proceso particular de negocio. MTD = RTO + WRT
RTO (Recovery Time Objective, Tiempo de recuperación objetivo)	Es el tiempo disponible para recuperar sistemas y recursos interrumpidos.
WRT (Work Recovery Time, Tiempo de recuperación del trabajo)	Es el tiempo que toma recuperar y volver a poner en funcionamiento funciones/procesos críticos del negocio, una vez que los sistemas han sido restaurados.
RPO (Recovery Point Objective, Punto de recuperación objetivo)	Cantidad o magnitud de pérdida de datos –en términos de un período de tiempo– que puede ser tolerado por los sistemas críticos del negocio.

FASE IV. Tratamiento del riesgo

La empresa ha considerado las siguientes opciones de tratamiento de riesgo:

ALTERNATIVAS DE TRATAMIENTO DE RIESGOS	
Alternativa	Descripción
Mitigar	La empresa adopta las medidas necesarias para reducir la probabilidad e impacto del evento de riesgo al mínimo posible.
Evitar	La empresa deja de realizar la actividad amenazada por el evento de riesgo o establece una forma diferente de llevarla a cabo.
Aceptar	La empresa no realiza ninguna acción para tratar el riesgo. La empresa considera esta medida apropiada en casos donde el costo de tratar el riesgo es mayor que el daño que éste pueda causar.
Compartir/Transferir	La empresa decide trasladar (tercerizar) la ejecución de la actividad a un proveedor de recursos o servicios a fin de transferir o compartir con éste los posibles efectos del evento de riesgo.

4.1. Selección de opciones para el tratamiento del riesgo

TRATAMIENTO DEL RIESGO						
Riesgo		**Activo**	**Amenaza**	**Vulnerabilidad**	**Valorización**	**Estrategia**
Código	**Nivel**	**Clasificación / Código / Nombre**				
R1	6	Proceso PN_GCyL Gestión de clientes y licencias	Error en uso	Extensiones de tiempo de vigencia de licencias no formalizadas.	Tolerable	Evitar

R2	6	Proceso PN_GPyF Gestión de pagos y facturación	Error en uso	No todas las cuentas han sido integradas y son procesadas manualmente.	Tolerable	Evitar
R3	12	Proceso PN_GPD Gestión de proyectos de desarrollo	Mala implementación	Especificaciones poco claras o incompletas para los desarrolladores.	Intolerable	Mitigar
R4	12		Incumplimiento	Estimaciones no precisas, principalmente en grandes proyectos.	Intolerable	Mitigar
R5	12		Desinformación	Deficiente documentación de los sistemas desarrollados	Intolerable	Mitigar
R6	12		Mal funcionamiento	Deficiente proceso de pruebas de software	Intolerable	Mitigar
R7	12		Incumplimiento	Cambios constantes de prioridades de proyectos.	Intolerable	Mitigar
R8	20	Proceso PN_GCS Gestión de copias de seguridad (respaldo y restauración)	Pérdida de información	Generación de una copia única.	Intolerable	Evitar
R9	12			Proceso no formalizado.	Intolerable	Evitar

R10	6	Proceso PN_GAD Gestión de adquisiciones y contrataciones	Sobretiempo	Proceso no formalizado.	Tolerable	Aceptar
R11	6	Hardware HW_LAP Laptop	Error en uso	Mantenimiento insuficiente.	Tolerable	Aceptar
R12	4		Degradación de rendimiento	Carencia de políticas de reemplazo.	Aceptable	Aceptar
R13	3		Pérdida	Falta de protección y cuidado.	Aceptable	Evitar
R53	6		Acceso no autorizado	Falta de políticas de seguridad.	Aceptable	Mitigar
R14	4	Hardware HW_USB Dispositivos de almacenamiento USB	Uso inadecuado.	Mantenimiento insuficiente.	Aceptable	Aceptar
R15	2		Deterioro	Carencia de políticas de reemplazo.	Aceptable	Aceptar
R16	2		Pérdida.	Falta de protección y cuidado.	Aceptable	Evitar
R17	9	Software SW_CRM Customer Relationship Management	Corrupción de datos	Proceso de importación de contactos no documentado.	Tolerable	Mitigar
R18	4		Abuso de derechos.	Registro incompleto de pistas de auditoría.	Aceptable	Aceptar
R19	4		Desinformación	Insuficiente documentación.	Aceptable	Aceptar

R20	4	Software SW_TL Task List	Abuso de derechos.	Registro incompleto de pistas de auditoría.	Aceptable	Aceptar
R21	4		Desinformación	Insuficiente documentación.	Aceptable	Mitigar
R22	9	Software SW_RNS RW Newsletter Solution	Error en uso	Interfaz de usuario complicada.	Tolerable	Mitigar
R23	4		Abuso de derechos	Registro incompleto de pistas de auditoría.	Aceptable	Aceptar
R24	9		Desinformación	Insuficiente documentación.	Tolerable	Mitigar
R25	4	Software SW_RLS RW Loyalty Solution	Abuso de derechos.	Registro incompleto de pistas de auditoría.	Aceptable	Aceptar
R26	9		Desinformación	Insuficiente documentación.	Tolerable	Mitigar
R27	9	Software SW_SRVW Servicios Windows	Mal funcionamiento	Deficiencias para notificar errores.	Tolerable	Mitigar
R28	9	Software SW_SWB Sitios Web	Inestabilidad	Uso indiscriminado de plug-ins no probados.	Tolerable	Evitar
R29	2		Spam	Deficiente control de comentarios	Aceptable	Mitigar
R30	8	Software SW_SOA	Malware. Spyware.	Instalación de aplicaciones no autorizadas.	Tolerable	Evitar

R31	12	Sistema Operativo cliente y Aplicaciones	Suplantación. Abuso de derechos.	Deficiente protección y control en el uso de contraseñas.	Intolerable	Evitar
R32	12	Información INF_BDT Bases de datos	Degradación del rendimiento.	Carencia de un plan de mantenimiento.	Intolerable	Mitigar
R33	12			Deficiente diseño de algunas tablas.	Intolerable	Mitigar
R34	12		Ineficiencia	Utilización de mapas en columnas.	Intolerable	Mitigar
R35	8		Suplantación	Contraseñas no protegidas en sistemas de uso interno.	Tolerable	Mitigar
R36	12	Información INF_RCR Repositorio de Credenciales	Abuso de derechos.	Falta de control en la distribución/acceso.	Intolerable	Mitigar
R37	12		Desorganización	Deficiente control de cambios.	Intolerable	Mitigar
R38	12	Información INF_DOC Documentación	Desorganización	Deficiente control de versiones.	Intolerable	Evitar
R39	12		Pérdida de documentación	Deficiente control de archivo.	Intolerable	Evitar
R40	12	Servicio SRV_COE Correo electrónico	Malware	Apertura de enlaces sin examinar el destino.	Intolerable	Evitar
R41	8		Espionaje	Uso de conexiones no seguras.	Tolerable	Mitigar

R42	3	Servicio SRV_SKY Comunicación en tiempo real vía Skype	Spam.	Aceptación de usuarios desconocidos.	Aceptable	Aceptar
R43	6	Servicio SRV_TEC Telefonía celular	Espionaje. Robo de información.	Conexión a señales de telefonía simuladas (cell-site simulators)	Tolerable	Mitigar
R44	9	Servicio SRV_INT Internet	Espionaje. Mala utilización.	Permitir la conexión a usuarios no autorizados.	Tolerable	Mitigar
R45	9	Servicio SRV_ALN Almacenamiento en la nube	Desorganización	Falta de esquemas de organización de información.	Tolerable	Mitigar
R46	12	Servicio SRV_SMS Envío de SMS	Mal funcionamiento	Falta de control en la renovación del uso del servicio (pago de suscripción/crédito/cuota).	Intolerable	Evitar
R47	9	Servicio SRV_VPN Red privada virtual	Abuso de derechos.	Uso de cuentas de otros usuarios.	Tolerable	Mitigar
R48	9	Servicio SRV-CON Servicios contables	Abuso de derechos.	Uso de cuentas de otros usuarios.	Tolerable	Aceptar

R49	8	Servicio SRV_HOS Servicio de hosting	Malware, degradación de rendimiento	Instalación no autorizada de aplicaciones	Tolerable	Evitar
R50	4		Ciberdelincuencia.	Deficiente configuración de seguridad de servicios/aplicaciones.	Aceptable	Evitar
R51	12	Servicio SRV_MEN Servicio de mensajería electrónica	Mala reputación	Deficiente configuración de autenticación de dominios.	Intolerable	Evitar
R52	4			Carencia de un plan de control de ranking de dominio remitente.	Aceptable	Mitigar

4.2. Proposición de planes de tratamiento del riesgo

De los riesgos que se encuentran en el nivel ALTO, se han seleccionado los riesgos asociados a 3 procesos críticos, para los cuales se proponen planes de acción:

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-001
RIESGOS A TRATAR	R3, R4, R5, R6, R7
ACTIVO ASOCIADO	Proceso - PN_GPD - Gestión de proyectos de desarrollo
PLAN DE ACCIÓN	Adopción de Scrum como marco de trabajo ágil para la gestión de los proyectos de desarrollo. Uso de herramientas de control de código fuente.
DESCRIPCIÓN	Formalizar el proceso de desarrollo y mantenimiento de los sistemas mediante la adopción del marco de trabajo ágil SCRUM. Esto facilitará la gestión de los proyectos a través de períodos cortos controlados de desarrollo, prueba, revisión y entrega, lo que permitirá proveer entregables de mejor calidad. Esto beneficia directamente al cliente, mejora la reputación de la organización y ahorra costos. De manera simultánea, se hará uso de herramientas formales de control de código fuente a fin de subsanar las deficiencias actuales respecto a la fase de programación.
COSTO	Tiempo de adecuación del sistema TaskList: Nro. De personas x tiempo x costo/hora: 1 x 22 x 14.00 = 308.00 USD. Evaluación y selección de herramientas de control de código: Nro. De personas x tiempo x costo/hora: 1 x 16 x 14.00 = 224.00 USD Costo de las herramientas de control de código: = 0.00 USD (< 5 usuarios) Capacitación: Nro. De personas x tiempo x costo/hora: = 5 x 2 x 14.00 = 140.00 USD COSTO TOTAL: 672.00 USD
PRESUPUESTO ASIGNADO	750.00 USD
RESPONSABLES	CTO, Development team

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-002
RIESGOS A TRATAR	R8, R9
ACTIVO ASOCIADO	Proceso - PN_GCS - Gestión de copias de seguridad (respaldo y restauración)
PLAN DE ACCIÓN	Contratación del servicio de generación de copias de seguridad y restauración de archivos
DESCRIPCIÓN	Servicio proporcionado por la empresa de hosting. Inicialmente se tenía contratado solamente el alquiler de tres servidores (Web, Base de datos y Pruebas). Incluir, como parte del servicio contratado, la generación y restauración de copias de seguridad de archivos permitirá que este proceso se realice de una manera mucho más segura y programada. Esto evitará la necesidad de generar manualmente las copias de seguridad, ahorrará tiempo y reducirá la ocurrencia de errores en el proceso.
COSTO	Costo del servicio contratado: Almacenamiento: 0.80 USD/GB/mes Restauración: 0.30 USD/GB/mes Tamaño aproximado de todos los archivos a respaldar: 112 GB = 112 * 0.80 + 40^{1} * 0.30 = 89.60 + 12.00 COSTO TOTAL: 101.60 USD/mes (1: tamaño aproximado mensual a ser restaurado)
PRESUPUESTO ASIGNADO	101.60 USD/mes
RESPONSABLES	CTO

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-003
RIESGOS A TRATAR	R32, R33, R34
ACTIVO ASOCIADO	Información - INF_BDT - Bases de datos
PLAN DE ACCIÓN	Elaboración y ejecución de un plan de optimización del rendimiento de las bases de datos.
DESCRIPCIÓN	Elaboración de un plan integral de optimización del rendimiento de las bases de datos, priorizando las bases de datos de los sistemas RNS y RLS, a fin de mejorar su desempeño. Etapas: - Etapa 1: normalización y desnormalización, optimización de columnas. - Etapa 2: eliminación de mapas en columnas, optimización de índices - Etapa 3: tablas históricas, partición. - Etapa 4: optimización de procedimientos almacenados y funciones - Etapa 5: creación de trabajos de mantenimiento periódico.
COSTO	Actividades: Elaboración del plan: Nro. Personas x tiempo x costo/hora: = 2 x 40 x 14.00 = 1120.00 USD Ejecución del plan (etapas 1 a 5): E1 = 2 x 40 x 14.00 = 1120.0 USD E2 = 2 x 24 x 14.00 = 672.0 USD E3 = 2 x 16 x 14.00 = 448.0 USD E4 = 2 x 40 x 14.00 = 1120.0 USD E5 = 2 x 8 x 14.00 = 224.0 USD COSTO TOTAL: 3584.00 USD
PRESUPUESTO ASIGNADO	4000.00 USD
RESPONSABLES	CTO, Development Team

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-004
RIESGOS A TRATAR	R36, R37
ACTIVO ASOCIADO	Información – INF-RCR – Repositorio de credenciales
PLAN DE ACCIÓN	Repositorio único de credenciales
DESCRIPCIÓN	Crear un repositorio único de credenciales y evitar su distribución/duplicación por parte del personal. Establecer políticas de modificación de contraseñas y gestionar permisos de acceso.
COSTO	Integración de la información: 2h x 14.00 = 28.00 USD Establecimiento de políticas de modificación y control de acceso: 4h x 14.00 = 56.00 USD COSTO TOTAL: 28.00 + 56.00 = 84.00 USD
PRESUPUESTO ASIGNADO	84.00 USD
RESPONSABLES	CTO

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-005
RIESGOS A TRATAR	R38, R39
ACTIVO ASOCIADO	Información – INF_DOC – Documentación
PLAN DE ACCIÓN	Creación de un repositorio único de documentación.
DESCRIPCIÓN	Módulo implementado como parte del sistema TaskList. Requerimientos funcionales: - Carga de documentos. - Organización de documentos en categorías. - Búsqueda, visualización y archivamiento. Gestión de acceso y permisos.

COSTO	Análisis, diseño e implementación: Nro. Personas x tiempo x costo/hora: 1 x 40 x 14.00 = 560.00 USD Carga de documentación y organización: Nro. Personas x tiempo x costo/hora: 1 x 4 x 14.00 = 56.00 USD Capacitación: = 4 x 1 x 14 = 56.00 USD COSTO TOTAL: 560.0 + 56.0 + 56.0 = 672.00 USD
PRESUPUESTO ASIGNADO	750.00 USD
RESPONSABLES	CTO, Development Team, Customer Satisfaction

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-006
RIESGOS A TRATAR	R46
ACTIVO ASOCIADO	Servicio – SRV_SMS – Envío de SMS
PLAN DE ACCIÓN	Evitar la interrupción del servicio de distribución masiva de SMS mediante renovación automática o mediante alerta.
DESCRIPCIÓN	Opción 1. Activación de la opción de cobro automático de servicio por cuota de consumo. El servicio permite el cobro automático al medio de pago asociado de acuerdo a la cuota de consumo establecida. Opción 2. Creación de alerta de correo/SMS cuando se alcance un valor mínimo de crédito establecido. El pago se efectuaría manualmente a través del sistema del proveedor.
COSTO	0.00 USD
PRESUPUESTO ASIGNADO	0.00 USD
RESPONSABLES	CTO

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	RW-PTR-007
RIESGOS A TRATAR	R51
ACTIVO ASOCIADO	Servicio – SRV_MEN – Servicio de mensajería electrónica
PLAN DE ACCIÓN	Automatizar la configuración de la autenticación de los dominios remitentes.
DESCRIPCIÓN	Cada nuevo cliente cuenta con uno o varios dominios desde los cuales desea remitir encuestas o boletines de forma masiva a sus clientes. Para que el envío sea exitoso (el correo no sea puesto en cuarentena o enviado a la bandeja de correo no deseado) deben crearse y configurarse registros que permitan la autenticación del dominio y convertirlo así en un dominio que autoriza a la empresa a remitir correos en su nombre. A este proceso se le denomina “white labeling”. El API del proveedor permite este tipo de automatización.
COSTO	Costo de implementación y pruebas: Nr. Personas x tiempo x costo/hora: 1 x 6h x 14.00 = 84.00 USD
PRESUPUESTO ASIGNADO	84.00 USD
RESPONSABLES	CTO, Development team

FASE V. Seguimiento y revisión

5.1. Seguimiento, revisión y responsables

SEGUIMIENTO y REVISIÓN DE PLANES DE ACCIÓN			
Proyecto	**Detalle**	**Variable a controlar**	**Indicador**
Proyecto P01: Adopción de Scrum como marco de trabajo ágil para la gestión de los proyectos de desarrollo. Uso de herramientas de control de código fuente.	Avance: 70% Presupuesto asignado/ejecutado: 750.00 USD / 610.00 USD Estado: En progreso Fecha objetivo: 23 de julio (con retraso por cambio de prioridades) Responsable: CTO	Desviación en las estimaciones.	Número de tareas estimadas con margen de error mayor a 25%.
		Valor total de tareas en desarrollo.	Número de puntos de tareas en desarrollo.
		Errores encontrados en etapas luego de la etapa de desarrollo.	Número de errores reportados en etapa de prueba.
			Número de errores encontrados luego de pase a producción.
		Historias completadas por iteración.	Número de historias completadas por iteración.
Proyecto P02: Contratación del servicio de generación de copias de seguridad y restauración de archivos.	Avance: 100% Presupuesto asignado/ejecutado: 101.60 USD/mes Estado: Concluido Fecha objetivo: 30 mayo (fecha proyectada) / 12 junio (fecha oficial, luego	Copias de seguridad completas.	Número de copias de seguridad completas.
		Restauraciones satisfactorias (sin errores o incompletas)	Número de restauraciones satisfactorias.

	de realización de pruebas de respaldo y recuperación) Responsable: CTO		
Proyecto P03: Elaboración y ejecución de un plan de optimización del rendimiento de las bases de datos.	Avance: 20% Presupuesto asignado/ejecutado: 4000.00 USD / 860.00 USD Estado: En progreso Fecha objetivo: 15 de diciembre (se dedican algunas horas los viernes por la tarde, según disponibilidad) Responsable: CTO	Desempeño de procesos de base de datos (mediana y gran complejidad)	Tiempo promedio de respuesta –en minutos/segundos- que cada proceso demora en completarse.
		Eficacia de los índices.	Cuota de participación de los índices en la ejecución de una consulta.
		Capacidad de respuesta de la base de datos.	Número de interrupciones causadas por problemas de base de datos.

En todos los casos, supervisado por el CTO, mediante reuniones semanales o reportes registrado en el sistema Task List.

FASE VI. Comunicación y consulta

6.1. Lineamientos para la comunicación y consulta

Se tendrán en cuenta los siguientes lineamientos:

- Se brindará comunicación a lo largo de todo el proceso de gestión de riesgos a todo el personal de la organización, para lo cual se identifican 3 fases de comunicación para un evento de riesgo:

ACCIONES DE COMUNICACIÓN			
Fase	**Acción de comunicación**	**Descripción**	**Instrumentos**
Antes	Educación	Brindar conocimientos básicos de riesgos, cómo enfrentarlos, acciones preventivas. Fomentar la investigación y el auto-conocimiento	Recursos de Internet (páginas, videos, etc.)
	Capacitación	Orientación en el uso de los activos de TI a fin de prevenir eventos de riesgo.	Actividades con el personal de la organización: Chat y video-conferencia vía Skype, videos instructivos.
	Información	Brindar información adicional o complementaria, sobre todo si se detectan variantes en los riesgos o la inclusión de un nuevo activo.	Notificaciones vía correo electrónico, boletines informativos en formato PDF.
Durante	Información	Brindar información sobre cómo actuar y los procedimientos a seguir para el tratamiento.	El instrumento es diverso y variará en función a la urgencia de atención del evento de riesgo en curso.
Después	Información	Compartir lecciones aprendidas. Comunicar la efectividad del tratamiento aplicado.	Chat y video-conferencia vía Skype
	Capacitación	Orientación en el uso de los activos de TI a fin de prevenir eventos de riesgo.	Actividades con el personal de la organización: Chat y video-conferencia vía Skype, videos instructivos.

	Promoción	Fomentar una cultura de gestión de riesgos e interiorizarlo en el personal.	Chat y video-conferencia vía Skype, notificaciones vía correo electrónico.

- Se asegurará que la toma de decisiones esté alineada con los resultados obtenidos luego de la aplicación del proceso de gestión de riesgos.
- Revisar periódicamente si el marco de gestión de riesgos y los planes establecidos son aún aplicables y están actualizados.

Por otro lado, se formuló un programa de capacitación como actividad formal en la organización con un plan de contenidos a desarrollar. Esta actividad constituye una de las estrategias de prevención a fin de fomentar una cultura y concientización frente al riesgo. El plan de contenidos aborda aspectos relacionados a los riesgos identificados en las fases anteriores, su tratamiento y control. El programa se detalla a continuación:

PROGRAMA DE CAPACITACIÓN	
PROGRAMA	Plan de capacitación sobre riesgos asociados al uso de tecnología y seguridad de la información.
DIRIGIDO A	CEO, CTO, Customer Satisfaction (2 personas), Marketing & Sales (2 personas) Development Team (3 personas), Diseñador Web (1 persona)
RECURSOS	• Diapositivas. • Guías, documentación en formato PDF. • Videos complementarios. • Encuestas. • Skype o Google Hangouts (llamada de voz/video)
FACILITADOR	• Comité de riesgos.
CONTENIDO	PARTE I. Conocimientos generales SESION 1

	• ¿Qué es el riesgo? • ¿Qué es la gestión de riesgos? • Riesgos asociados al uso de tecnología. • Uso apropiado de Internet. SESIÓN 2 • Identificación de correos electrónicos sospechosos. • El Malware. Spam. • Ingeniería Social. SESIÓN 3 • Seguridad en el puesto de trabajo. • Resguardo y recuperación de información (personal y laboral) PARTE II. Políticas de la organización SESIÓN 4 • Políticas organizacionales relacionadas con la seguridad de la información. • Políticas organizacionales relacionadas al uso de software y hardware. • Roles y responsabilidades en la empresa. SESIÓN 5 • Sanciones por incumplimiento de políticas. • Gestión de incidentes.
COSTO	Las sesiones se llevarán a cabo dentro de los horarios regulares de trabajo. El costo se calcula en función al tiempo invertido en el proceso multiplicado por el número de personas involucradas y el pago por hora. Adicionalmente, se asigna un costo por elaboración de materiales bajo la misma mecánica de cálculo. Sesiones x Personas x Tiempo x Costo/hora 5 x 8 x 1 x 14.00 = 560.00 USD Material: 100.00 USD COSTO TOTAL: 660.00 USD
MONITOREO	Se aplicarán encuestas para evaluar la sesión, el contenido impartido y el nivel de comprensión de los temas tratados.
MÉTRICAS	• Número de asistentes a las sesiones. • Nivel de participación y preguntas. • Número de personas que contestaron satisfactoriamente las encuestas. • Incidentes de seguridad posteriores a la capacitación.

	• Número de sanciones por incumplimiento de políticas posteriores a la capacitación.

El resumen con los resultados del programa de capacitación se puede consultar en el anexo 6.B

Asimismo, se elaboró una guía para el establecimiento de políticas para el trabajo remoto, que incluye definiciones, criterios y responsabilidades, así como una serie de consideraciones a partir de las cuales la organización puede elaborar e implementar su propio documento de políticas. Esta guía se encuentre disponible en el anexo 6.C.

3.5. Evaluación del modelo aplicado (juicio experto)

El proceso de validación del modelo propuesto involucró la utilización de los siguientes instrumentos:

a. Validación por juicio experto: se solicitó a cuatro (4) expertos realizar la validación del modelo propuesto a través de un formato de evaluación que permitió la calificación de todas las actividades de las fases comprendidas en el modelo mediante la valoración de 6 indicadores (ver Anexos 7 y 8). Los resultados obtenidos determinaron que ***el modelo planteado es aceptable***.

b. Determinación del nivel de confiabilidad del instrumento: las calificaciones proporcionadas por los expertos fueron sometidos a la aplicación del Alfa de Cronbach. Los resultados se muestran a continuación:

ESTADÍSTICAS DE CONFIABILIDAD	
Alpha de Cronbach	Nro. de ítems
0.841	17

De acuerdo la investigación de Karen Harkness y otros [32], los rangos para determinar el nivel de aceptación para el Alfa de Cronbach son los siguientes:

NIVELES DE ACEPTABILIDAD PARA EL COEFICIENTE ALFA DE CRONBACH	
Coeficiente Alfa	**Nivel de Confiabilidad**
Menor a 0.60	Inaceptable
Entre 0.60 y 0.65	No deseable
Entre 0.65 y 0.70	Mínimamente aceptable
Entre 0.70 y 0.80	Respetable
Entre 0.80 y 0.90	**Muy buena**
Mayor a 0.90	Considere acortar la escala

Tomando en cuenta el coeficiente obtenido para elementos estandarizados (0.722) concluimos que ***el instrumento aplicado se encuentra en el nivel de confiabilidad Muy Buena***.

c. Determinación del nivel de concordancia de las evaluaciones: se hizo uso del Coeficiente de Concordancia de Kendall (W), con los parámetros estándar exigidos por el método. Debido a que el coeficiente puede variar entre 0 y 1 se plantean dos hipótesis:

H0 ($W = 0$): no existe concordancia entre los expertos.
H1 ($W > 0$): existe concordancia entre los expertos.

La siguiente tabla muestra los resultados obtenidos:

COEFICIENTE DE KENDALL							
	Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	GLOBAL
N	17	17	17	17	17	17	17
Coeficiente de Kendall (α)	0.353	0.176	0.118	0.216	0.147	0.039	0.214
Chi-cuadrado (x^2)	18.00	9.00	6.00	11.00	7.50	2.00	10.904
Grados de libertad (gl)	3	3	3	3	3	3	3
Valor de probabilidad (p)	0.000	0.029	0.112	0.012	0.058	0.572	0.012

En base a los resultados obtenidos se concluye que:

- La hipótesis nula (H0) queda eliminada.
- Existe concordancia entre los expertos.
- La concordancia entre los evaluadores no se debe a las probabilidades ($p \leq \alpha$)

CONCLUSIONES

La investigación realizada y la aplicación del modelo permiten formular las siguientes conclusiones:

Se elaboró un modelo para la gestión de riesgos de TI adecuado para organizaciones que brindan servicios de información bajo la modalidad de suscripción que fue el resultado del análisis, comparación y armonización de diferentes estándares y marcos de trabajo dedicados a la gestión de riesgos.

Se estableció un procedimiento para la determinación de los procesos críticos en la organización que constituyen parte fundamental en la continuidad del negocio.

Se formuló y aplicó un plan de capacitación y concientización que permitió a los miembros de la organización conocer y aplicar medidas de protección y asumir una posición de prevención frente al riesgo asociado al uso de tecnología.

El modelo propuesto y ajustado fue sometido a validación de expertos con la finalidad de determinar su aplicabilidad, para permitir a la organización resguardar sus activos, aplicar de manera efectiva el proceso de gestión de riesgos y mantener su continuidad.

Se ha logrado que la organización comprometa sus esfuerzos en llevar a cabo la gestión de riesgos como un proceso intrínseco, más allá de la gestión básica cotidiana que había llevado hasta antes de la realización de este trabajo.

REFERENCIAS BIBLIOGRÁFICAS

[1] World Economic Forum, "The Global Risk Report 2018, 13th Edition". World Economic Forum. Geneva, Italy. 2018.
Disponible en: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[2] Deloitte, "Global Risk Management Survey, 10th Edition". Deloitte Development LLC. United States. 2017.
Disponible en:
https://www2.deloitte.com/content/dam/insights/us/articles/3654_Global-risk-mgmt-survey-10/DUP_Global-risk-management-survey-10th-ed.pdf

[3] Del Carpio Gallegos, Javier, "Gestión de riesgos en proyectos de tecnología de información en el Perú", Revista "Industrial Data" de la Facultad de Ingeniería Industrial, vol. 11, Núm. 2, pp 45-51 (2008) UNMSM. Octubre 2008.
Disponible en: http://www.redalyc.org/pdf/816/81619829006.pdf

[4] Numa Arellano, "La gestión de riesgos como pilar del Gobierno Corporativo". Artículo que resume los resultados de la encuesta "Gobierno, riesgo y cumplimiento 2015" de EY. Perú 2016.
Disponible en: https://www.ey.com/pe/es/newsroom/newsroom-am-gestion-riesgos-gobierno-corporativo

[5] M. Arangurí, R. Imán, G. León, "Modelo de gestión de riesgos Ti para procesos que contribuyen la generación de valor en las universidades privadas", Flumen vol. 9, no. 1, pp. 25-36. USAT 2016.
Disponible en:
http://publicaciones.usat.edu.pe/index.php/flumen/article/view/391/396

[6] Ramírez y Ortiz, "Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios". Revista Ingeniería, Vol. 16, No. 2, pág. 56-66.
Disponible en: https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

[7] James Vesper, "Risk Assessment and Risk Management in the Pharmaceutical Industry. Clear and Simple". United States. Davis Healthcare International Publishing, LLC. 2006.

[8] Georges Dionne, "Risk Management: History, Definition and Critique". HEC Montreal - Department of Finance. 2013.
Disponible en: https://ssrn.com/abstract=2231635 ó http://dx.doi.org/10.2139/ssrn.2231635

[9] ISO, ISO 31000:2018(es) Risk management — Guidelines. USA; ISO, 2018
Disponible en: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[10] ISO, ISO/IEC 27005:2011. Information technology -- Security techniques -- Information security risk management. USA; ISO, 2018
Disponible e: https://www.iso.org/standard/56742.html

[11] A. Caralli, J. Stevens, L. Young, W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process". CERT Program. Software Engineering Institute. Carnegie Mellon University. United States. 2007.
Disponible en: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[12] Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, "MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método". Secretaría de Estado de Administraciones Públicas. Gobierno de España. 2012.
Disponible en: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

[13] Blanca Duque, "Metodologías de Gestión de Riesgos (OCTAVE, MAGERIT, DAFP)". Universidad de Caldas. Facultad de Ingeniería. Colombia. 2010.
Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

[14] ISACA, Twenty years of the Cobit framework. USA: ISACA, 2018.
Disponible en: http://www.isaca.org/COBIT/Pages/COBIT-20th-Anniversary.aspx#years

[15] ISACA, Cobit 5 for Risk. USA. ISACA 2013, p. 9.

[16] S. Laguna, C. Caballero-Uribe, V. Lewis, S. Mazuera, J. Salamaca, W. Daza, A. Fourzali, "Consideraciones éticas en la publicación de investigaciones científicas". Publicado en Salud Uninorte. Vol. 23, No. 1. Colombia, 2007. Disponible en: http://ciruelo.uninorte.edu.co/pdf/salud_uninorte/23-1/8_Consideraciones%20eticas.pdf

[17] Paulino Rivero, "Diseño de un modelo de gestión del riesgo aplicado a una empresa manufacturera de autopartes". Tesis de Maestría. Instituto Politécnico Nacional. Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas. México, 2017.
Disponible en:
http://148.204.210.201/tesis/1506975002735TESISTERMINADA.pdf

[18] María Fernanda Molina Miranda, "Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral". Trabajo de fin de Máster. Universidad Politécnica de Madrid. Escuela Técnica Superior de Ingenieros en Telecomunicación. Departamento de Ingeniería de Sistemas Telemáticos. España. 2015.
Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

[19] Paulino José Rivero Meléndez, "Diseño de un Modelo de Gestión del Riesgo aplicado a una empresa manufacturera de autopartes".
Tesis de maestría. Instituto Politécnico Nacional. Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas. México. 2017.
Disponible en:
http://148.204.210.201/tesis/1506975002735TESISTERMINADA.pdf

[20] Hanim Maria Astuti, Feby Artwodini Muqtadiroh, Eko Wahyu Tyas Darmaningrat, Chitra Utami Putri, "Risk Assessment of Information Technology Processes Based on COBIT 5 Framework. A Case Study of ITS Service Desk". Artículo – Caso de Estudio Publicado por ScienceDirect. ELSEVIER. Presentado en la 4ta Conferencia Internacional de Sistemas de Información 2017. Bali – Indonesia.

Instituto Tecnológico Sepuluh Nopember (ITS) Facultad de Tecnología de la Información y Comunicaciones. Departamento de Sistemas de Información. Indonesia. 2017.
Disponible en:
https://www.sciencedirect.com/science/article/pii/S1877050917329599

[21] Carlos Monje, "Metodología de la investigación cuantitativa y cualitativa. Guía didáctica". Universidad Surcolombiana, Facultad de Ciencias Sociales y Humanas. Colombia, 2011.

[22] Oskar Liuksiala, "The use of the risk management standard ISO 31000 in Finnish organizations". Tesis de maestría. Escuela de Administración. Universidad de Tampere. Finland, 2012.

[23] John P Morency, Roberta J. Witty, "Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2013". Gartner Research. USA, 2013.
Disponible en:
http://infota.siss.cl/concesiones/empresas/ESSAL/06%20Informaci%C3%B3n%20entregada%20por%20la%20empresa/INFORMACION%20EXCEPCIONAL/TICA/inf%20adicional/informacion%20excepcional/Documentos%20Inf%20Excepcional/Gartner/Calidad/hype_cycle_for_business_cont_247328.pdf

[24] Chris Goodwin, "Integrating business continuity management with IT risk management". Publicado por CSO. IDG Communications. USA. 2013.

[25] Cabello S.D., Kuna H.D. "Análisis y Gestión de Riesgo en Proyectos Software. Un nuevo modelo integrando la metodología SEI y Magerit". Tesis de Maestría. Universidad Nacional de Misiones. Artículo presentado en el XX Workshop de Investigadores en Ciencias de la Computación. Argentina. Abril 2018.
Disponible en:
http://sedici.unlp.edu.ar/bitstream/handle/10915/67916/Documento_completo.pdf-PDFA.pdf?sequence=1

[26] Ernesto Celi Arévalo, "La gestión de riesgo de TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las

pequeñas entidades financieras de Lambayeque". Pueblo Continente, Nr. 1, Vol. 27, pp. 73-84. Febrero 2016.
Disponible en:
http://journal.upao.edu.pe/PuebloContinente/article/view/395/360

[27] Francisco Valencia, Carlos Marulanda y Marcelo López, "Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional". Gerencia Tecnológica Informática GTI, Nr. 41, Vol. 5, pp. 65-77. Colombia, 2016.
Disponible en:
http://revistas.uis.edu.co/index.php/revistagti/article/view/5911/6185

[28] García J., Huamani S., Lomparte R., "Modelo de Gestión de Riesgos de Seguridad de la Información para PYMES peruanas". Revista Peruana de Computación y Sistemas, Nr. 1 Vol. 1. pp, 47-56. Perú, 2018.
Disponible en:
http://revistasinvestigacion.unmsm.edu.pe/index.php/rpcsis/article/view/14856/13008

[29] Torcoroma Velásquez, Hugo F. Castro y Yesica M. Pérez, "Modelo de gestión de riesgos en proyectos. Aproximación conceptual para proyectos de TI". Revista INGENIO UFPSO. Vol. 8, pp. 93-100. Colombia, 2015.
Disponible en:
http://revistas.ufpso.edu.co/index.php/ringenio/article/viewFile/227/142

[30] Arévalo, Cedillo y Moscoso, "Metodología Ágil para la Gestión de Riesgos Informáticos". Tevista Killkana Técnica. Nr. 2, Vol. 1, pp.31-42. Ecuador, mayo-agosto 2017.
Disponible en:
http://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/download/81/122/

[31] Gabriel Jaime Correa Henao, Eliana María Ríos-González y Julio César Acevedo-Moreno, "Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano". Journal of Engineering and Technology. Nr. 1, Vol. 6. Pp. 22-45. Colombia, 2016.

Disponible en:
http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1397/pdf

[32] Karen Harkness, Heather Arthur & Robert McKelvie; "The Measurement of Uncertainty in Caregivers of Patients With Heart Failure". Journal of Nursing Measurament. Vol. 21. Num. 1. Pp. 23-42. Canadá. November 2013. Disponible en:
https://www.researchgate.net/publication/261015950_The_Measurement_of_Uncertainty_in_Caregivers_of_Patients_With_Heart_Failure_Harkness_Karen_RN_PhD_Arthur_Heather_RN_PhD_FESC_McKelvie_Robert_MD_PhD_FRCPC_Journal_of_Nursing_Measurement211_2013_23-42#pf8

[33] ISACA; "Risk IT - Basado en COBIT". USA, ISACA 2009; p. 19.

[34] Vásquez, Fátima; Alva, Juliana; "Modelo de Gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la Región Lambayeque". Tesis de Maestría. Universidad Católica Santo Toribio de Mogrovejo. Perú. 2018.
Disponible en:
http://tesis.usat.edu.pe/bitstream/20.500.12423/1373/1/TM_VasquezVelasquezFatima_AlvaZapataJuliana.pdf

[35] Ministerio de Economía y Finanzas; "Metodología de Gestión de riesgos de seguridad de la información". Oficina de Gobierno de Tecnologías de la Información. Perú, 2016.
Disponible en:
https://www.mef.gob.pe/es/normatividad-interna/14172-05-rdn-006-2012-pip-transporte-estudios-en-paquete-mod-anexo-snip-09-10-y-16-2-2-final-871/file

[36] M. Arangurí, R. Imán, G. León, "Modelo de gestión de riesgos Ti para procesos que contribuyen la generación de valor en las universidades privadas", Tesis de Maestría. Universidad Católica Santo Toribio de Mogrovejo. Perú. 2016.
Disponible en:
http://tesis.usat.edu.pe/bitstream/20.500.12423/1444/3/TL_AranguriGarciaMaria_ImanEspinozaRicardo_LeonTenorioGregorio.pdf

[37] Dávila, Juan; "Gestión de Riesgos de Tecnologías de la Información (TI)". Universidad Católica Santo Toribio de Mogrovejo. Perú. 2018.

[38] Dirección de Estándares y Arquitectura de la Información. "Guía para realizar el Análisis de Impacto de Negocios BIA". Ministerio de Tecnologías de la Información y las Comunicaciones. Colombia, 2015.
Disponible en:
https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

[39] Días, Paul, Mariño, Olga, Sierra, Flor; "Elaboración del Análisis de Impacto al Negocio (BIA) como parte fundamental del plan de continuidad de negocio de la Cadena Radial". Trabajo de Grado. Facultad de Ingeniería. Universidad Piloto de Colombia. Colombia, 2016.
Disponible en:
http://polux.unipiloto.edu.co:8080/00002972.pdf

ANEXOS

Anexo 1: Hoja resumen de empresas participantes

EMPRESAS PARTICIPANTES			
Empresa	**Descripción**	**Misión**	**Valores**
Empresa 1 (Servicios de TI) Creación: 2001	Empresa que brinda SaaS para la creación, distribución y procesamiento de encuestas NPS y eNPS	Inspire and influence companies' relationships with their customers. We want companies to get more customer ambassadors that will promote the company and their products.	Ten core values 1. Be the Best; 2. Put Relationship First; 3.Never Stop Learning; 4. Keep it Simple; 5. Work With a smile; 6. Embrace Change and Challenges; 7. Work as A Team; 8. Focus On The Goal; 9. Stay Passionate; 10. Hard Work and Discipline.
Empresa 2 (Servicios de TI) Creación: 2013	We develop rapid response tools for the development of software according to your needs, which will allow you to quickly manage your projects, products, people, services and finances through a complete set of functionalities.	We deliver high-quality products that provides measurable business results to organizations around the world and profitable customer relationships.	We rely on principles of social responsibility providing volunteer work. Of continuous improvement of the Quality and care of the Environment reducing the consumption of natural resources and internal recycling programs. Improving and developing occupational health and safety practices achieving a safe and pleasant work environment.
Empresa 3 (Servicios de TI) Creación: 1993	Private Bulgarian company founded in 1993. The company is specialized in the design and development of integrated information systems (ERP systems) for the management of dynamic companies.	We develop innovative, adaptive and optimized solutions that are easy to adapt. We believe that the key to our success is the close cooperation with the customer during implementation.	

Empresa 4 (Servicios de TI) Creación: 2005	We develop innovative, fast and intuitive products to send emails, sms, web and email through smtp that will help you grow your business and increase the visibility of your products and services.	Our company has been built based on the trust and commitment to help our clients increase their productivity and expand their businesses.	We constantly seek to innovate and improve. We are dedicated to helping our clients connect with their users.

Tabla 6. Hoja resumen de empresas participantes

Anexo 2: Encuestas de diagnóstico aplicadas

UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
RESEARCH ABOUT IT RISK MANAGEMENT IN SaaS COMPANIES
- MASTER THESIS -
Research conductor: Jorge Rodríguez Castro
Master Degree Program. Student Code 172PG74617
jorgerodcas@hotmail.com - (+51) 979651370

IT RISK MANAGEMENT - DIAGNOSTIC SURVEY

Applied to: IT Risk Manager, IT Leader, TCO or similar

COMPANY _____

NAME _____

ROLE _____

EMAIL _____

Objective

This survey has the purpose of get an overview about the current state of the Risk IT Management in the small SaaS companies in Europe.

Non-disclosure agreement

The research conductor is committed to not to reveal any information about the respondent, the company or any other confidential information provided for the respondent. The data provided in this survey will be exclusively used to make an analysis about the current state of IT Risk Management in the SaaS companies in Europe.

Instructions

Please underline or check the option you consider fits better for each question.

Nr.	QUESTION
1	A framework -standard or proprietary- for IT risk management is applied in the company Yes | Partially | No | Don't know
2	There is an area or employee responsible for the IT risk management Yes | Partially | No | Don't know
3	The IT risk strategy is aligned with the corporate risk strategy Yes | Partially | No | Don't know

4 The company has a method to collect, classify and analyze the data related with IT risk
Yes | Partially | No | Don't know

5 The company has an inventory of the assets related to IT
Yes | Partially | No | Don't know

6 The company has an inventory of the processes related to IT
Yes | Partially | No | Don't know

7 The risk appetite has been determined for the IT risks
Yes | Partially | No | Don't know

8 A common language/vocabulary about IT risks is used in the company
Yes | Partially | No | Don't know

9 There is an inventory about known IT risks, their characteristics, resources, priorities and control activities
Yes | Partially | No | Don't know

10 A cost-benefit analysis about response options for potential risks is done regularly
Yes | Partially | No | Don't know

11 The results of the risk analysis are delivered on time to all affected stakeholders
Yes | Partially | No | Don't know

12 The results of the risk analysis are reported using useful terms and formats for decision making
Yes | Partially | No | Don't know

13 The company provides the necessary resources for the IT risk management
Yes | Partially | No | Don't know

14 The board is really engaged in IT risk management.
Yes | Partially | No | Don't know

15 IT risks - and their possible consequences - are taken into account for decision making
Yes | Partially | No | Don't know

16 The performance in IT risk management is monitored regularly
Yes | Partially | No | Don't know

17 Response plans are applied to minimize the impact of a IT risk incident
Yes | Partially | No | Don't know

18 A risk culture is promoted in the company
Yes | Partially | No | Don't know

19 The employees are conscious about the potential IT risks
Yes | Partially | No | Don't know

20 In a 0-10 range, please rate your level of knowledge about ISO 31000 standard
0 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10

21 In a 0-10 range, please rate your level of knowledge about ISO ISO/IEC 27005 standard
0 - 1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10

22 The company has a BIA (Business Impact Analysis)
Yes | Partially | No | Don't know

23 The company has a Business Continuity Plan
Yes | Partially | No | Don't know

24 There is an analysis about the threats that can have an impact in the business continuity

Yes | Partially | No | Don't know

Additional comments

_____

_____

_____

_____

_____

Signature

_____

Many thanks for your cooperation!

UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
RESEARCH ABOUT IT RISK MANAGEMENT IN SaaS COMPANIES
- MASTER THESIS -
Research conductor: Jorge Rodríguez Castro
Master Degree Program. Student Code 172PG74617
jorgerodcas@hotmail.com - (+51) 979651370

IT RISK MANAGEMENT - DIAGNOSTIC SURVEY

Applied to: IT users

COMPANY _____

NAME _____

ROLE _____

EMAIL _____

Objective

This survey has the purpose of get an overview about the current state of the Risk IT Management in the small SaaS companies in Europe.

Non-disclosure agreement

The research conductor is committed to not to reveal any information about the respondent, the company or any other confidential information provided for the respondent. The data provided in this survey will be exclusively used to make an analysis about the current state of IT Risk Management in the SaaS companies in Europe.

Instructions

Please underline or check the option you consider fits better for each question.

Nr.	QUESTION
1	I know the definition of "IT Risk" Yes | No
2	I know the definition of "IT Risk Management" Yes | No
3	The company I work has policies/rules/directives about risks management related to IT Yes | No | Don't know

4 If yes in question 3: The company applies regularly those policies to prevent or face risk events to happen.
Yes | No | Don't know

5 If yes in question 3: I consider those policies are good enough to prevent or face risk events.

Yes | No | Don't know

6 I know which are some of the risk related to IT at work

Yes | No

7 I experimented in the past risk events related with IT at work
Yes | No

8 In the computer I use at work is installed an anti-malware software
Yes | No | Don't know

9 The software in the computer I use at work is always updated (operative system, applications, etc.)
Yes | No | Don't know

10 I keep protected my sensitive/confidential information at work (passwords, security codes, confidential documents, etc.)
Yes | No

11 Finally, please provide some ideas/comments you can give to improve the security related with the use of technology in your company and reduce the occurrence of risk events related to IT

_____

_____

_____

_____

Signature _____

Many thanks for your cooperation!

Anexo 3: Tabla de resultados de encuestas

El cuadro siguiente muestra la categorización de las preguntas en función a su promedio ponderado.

Categoría	Aspecto	Cód.	REF: 2.13
EDM03 - ASEGURAR LA OPTIMIZACION DEL RIESGO	Marco de trabajo	P1	1.20
	Persona responsable	P2	1.07
	Alineamiento	P3	1.60
	Apetito de riesgo	P7	0.33
	Lenguaje común	P8	1.07
	Provisión recursos	P13	1.20
	Cultura	P18	1.20
	Concientización	P19	1.20
APO12 - GESTIONAR EL RIESGO	Recolección datos	P4	1.33
	Inventario activos	P5	1.47
	Inventario procesos	P6	0.93
	Inventario riesgos	P9	1.20
	Análisis costo-beneficio	P10	0.87
	Comunicación análisis	P11	0.87
	Formato comunicación	P12	0.60
	Compromiso Directorio	P14	1.13
	Toma decisiones	P15	1.47
	Monitoreo desempeño	P16	1.47
	Planes respuesta	P17	1.47
GESTIÓN CONTINUIDAD	BIA	P22	0.53
	Plan contingencia	P23	0.73
	Amenazas a la continuidad	P24	1.07
ESTÁNDARES ISO *	ISO 31000:2018	P20	
	ISO 27005:2018	P21	

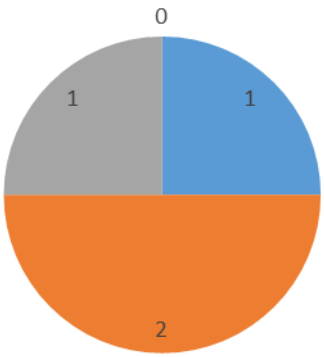
Tabla 7. Categorías, preguntas, promedios y códigos de color.

Fuente: elaboración propia. (*) No incluyen ponderación pues las preguntas cuentan con su propia escala y serán interpretadas independientemente.

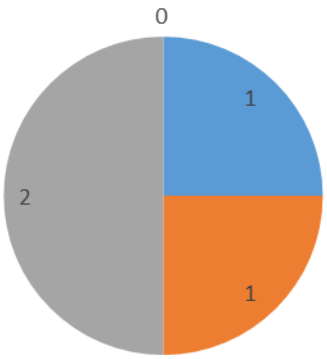
Anexo 4: Tabulación de resultados

Resultados de la encuesta de diagnóstico aplicada a los directores/líderes de TI

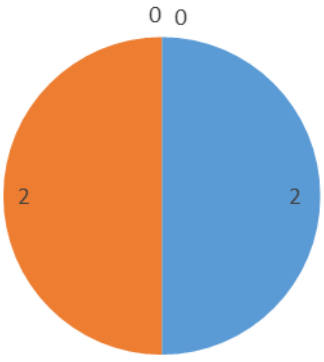
Q1. A framework -standard or proprietary- for IT risk management is applied in the company			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	1	25%
	Don't know	0	0%
	Total	**4**	**100%**



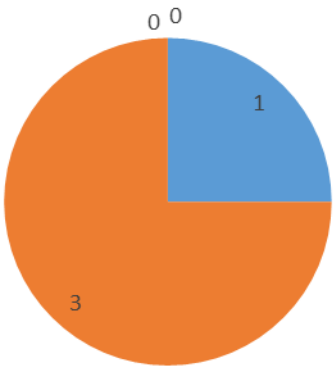
Q2. There is an area or employee responsible for the IT risk management			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	1	25%
	No	2	50%
	Don't know	0	0%
	Total	**4**	**100%**



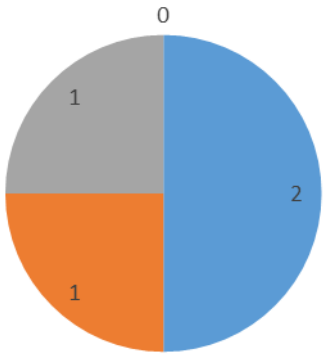
Q3. The IT risk strategy is aligned with the corporate risk strategy			
Options		Frequency	Percentage
	Yes	2	50%
	Partially	2	50%
	No	0	0%
	Don't know	0	0%
	Total	**4**	**100%**



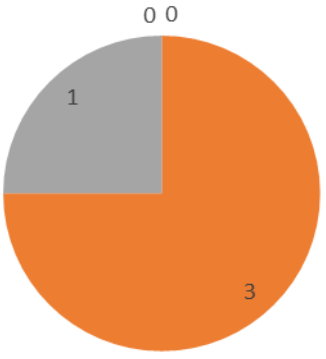
Q4. The company has a method to collect, classify and analyze the data related with IT risk			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	3	75%
	No	0	0%
	Don't know	0	0%
	Total	**4**	**100%**



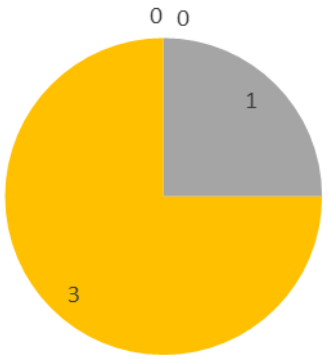
Q5. The company has an inventory of the assets related to IT			
Options		Frequency	Percentage
	Yes	2	50%
	Partially	1	25%
	No	1	25%
	Don't know	0	0%
	Total	**4**	**100%**



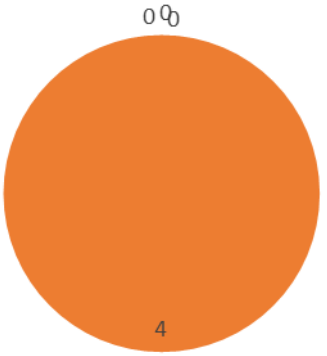
Q6. The company has an inventory of the processes related to IT			
Options		Frequency	Percentage
	Yes	0	0%
	Partially	3	75%
	No	1	25%
	Don't know	0	0%
	Total	**4**	**100%**



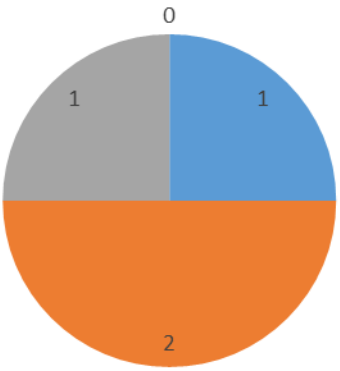
Q7. The risk appetite has been determined for the IT risks			
Options		Frequency	Percentage
	Yes	0	0%
	Partially	0	0%
	No	1	25%
	Don't know	3	75%
	Total	**4**	**100%**



Q8. A common language/vocabulary about IT risks is used in the company			
Options		Frequency	Percentage
	Yes	0	0%
	Partially	4	100%
	No	0	0%
	Don't know	0	0%
	Total	**4**	**100%**

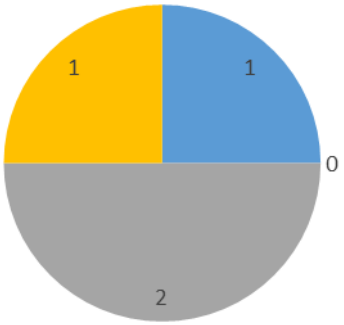


Q9. There is an inventory about known IT risks, their characteristics, resources, priorities and control activities			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	1	25%
	Don't know	0	0%
	Total	**4**	**100%**



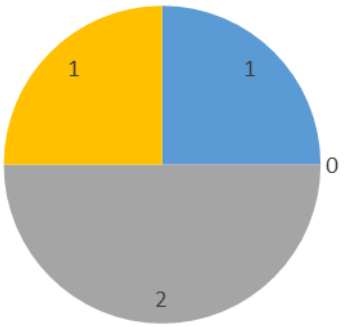
Q10. A cost-benefit analysis about response options for potential risks is done regularly

Options	Frequency	Percentage
Yes	1	25%
Partially	0	0%
No	2	50%
Don't know	1	25%
Total	**4**	**100%**



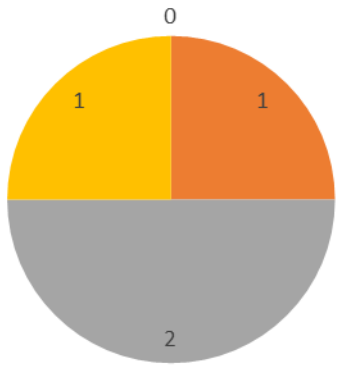
Q11. The results of the risk analysis are delivered on time to all affected stakeholders

Options	Frequency	Percentage
Yes	1	25%
Partially	0	0%
No	2	50%
Don't know	1	25%
Total	**4**	**100%**

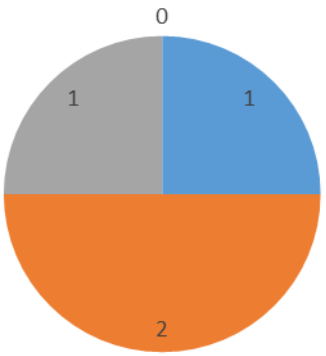


Q12. The results of the risk analysis are reported using useful terms and formats for decision-making

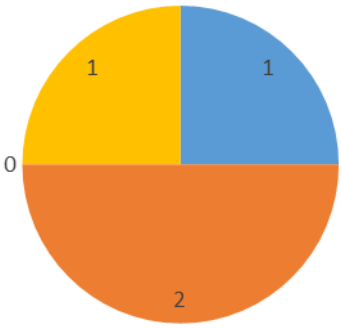
Options	Frequency	Percentage
Yes	0	0%
Partially	1	25%
No	2	50%
Don't know	1	25%
Total	**4**	**100%**



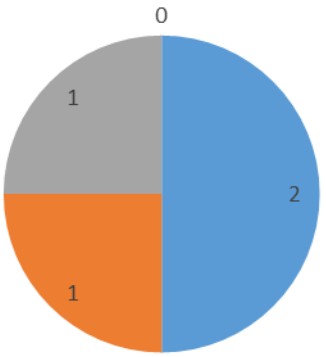
Q13. The company provides the necessary resources for the IT risk management			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	1	25%
	Don’t know	0	0%
	Total	**4**	**100%**



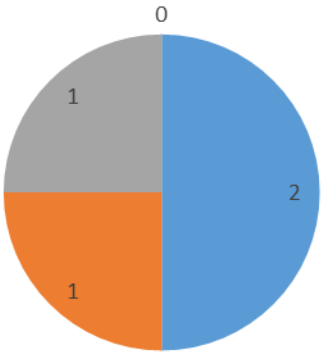
Q14. The board is really engaged in IT risk management.			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	0	0%
	Don’t know	1	25%
	Total	**4**	**100%**



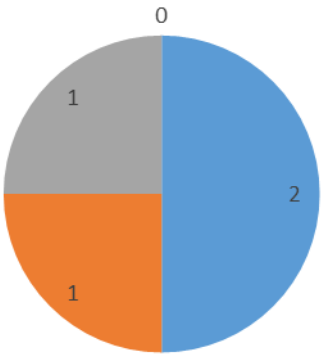
Q15. IT risks - and their possible consequences - are taken into account for decision making			
Options		Frequency	Percentage
	Yes	2	50%
	Partially	1	25%
	No	1	25%
	Don’t know	0	0%
	Total	**4**	**100%**



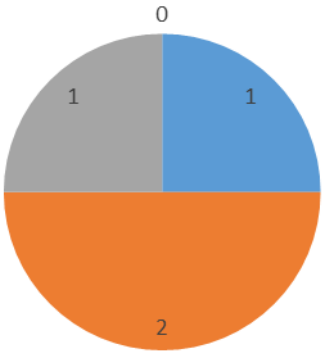
Q16. The performance in IT risk management is monitored regularly			
Options		Frequency	Percentage
	Yes	2	50%
	Partially	1	25%
	No	1	25%
	Don’t know	0	0%
	Total	**4**	**100%**



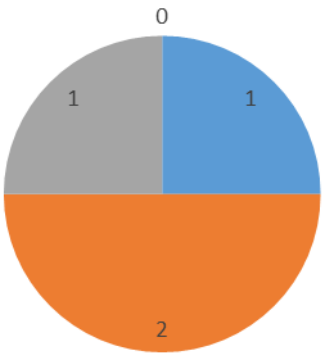
Q17. Response plans are applied to minimize the impact of a IT risk incident			
Options		Frequency	Percentage
	Yes	2	50%
	Partially	1	25%
	No	1	25%
	Don’t know	0	0%
	Total	**4**	**100%**



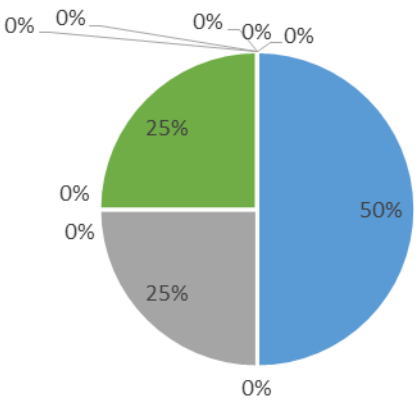
Q18. A risk culture is promoted in the company			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	1	25%
	Don’t know	0	0%
	Total	**4**	**100%**



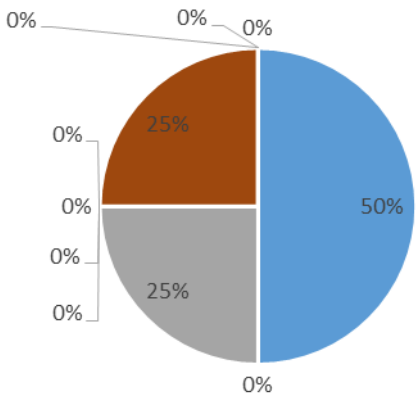
Q19. The employees are conscious about the potential IT risks			
Options		Frequency	Percentage
	Yes	1	25%
	Partially	2	50%
	No	1	25%
	Don't know	0	0%
	Total	**4**	**100%**



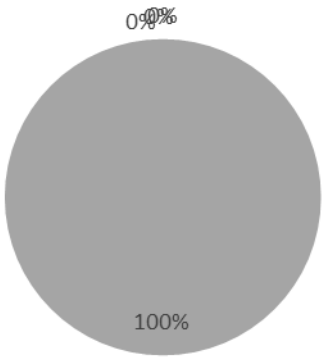
Q20. In a 0-10 range, please rate your level of knowledge about ISO 31000 standard			
Options		Frequency	Percentage
	0 – I have no clue	2	50%
	1	0	0%
	2	1	25%
	3	0	0%
	4	0	0%
	5	1	25%
	6	0	0%
	7	0	0%
	8	0	0%
	9	0	0%
	10 – I know it very well	0	0%
	Total	**4**	**100%**



Q21. In a 0-10 range, please rate your level of knowledge about ISO/IEC 27005 standard			
Options		Frequency	Percentage
	0 – I have no clue	2	50%
	1	0	0%
	2	1	25%
	3	0	0%
	4	0	0%
	5	0	0%
	6	0	0%
	7	1	25%
	8	0	0%
	9	0	0%
	10 – I know it very well	0	0%
	Total	**4**	**100%**

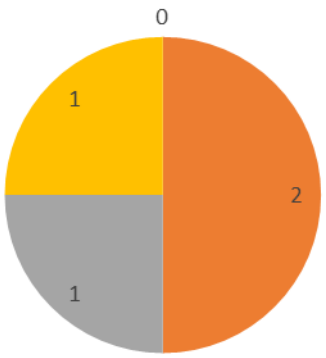


Q22. The company has a BIA (Business Impact Analysis)			
Options		Frequency	Percentage
	Yes	0	0%
	Partially	0	0%
	No	4	100%
	Don’t know	0	0%
	Total	**4**	**100%**



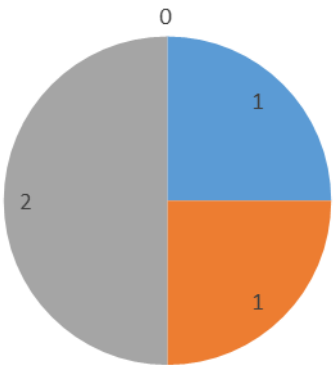
Q23. The company has a Business Continuity Plan

Options	Frequency	Percentage
Yes	0	0%
Partially	2	50%
No	1	25%
Don’t know	1	25%
Total	**4**	**100%**



Q24. There is an analysis about the threats that can have an impact in the business continuity

Options	Frequency	Percentage
Yes	1	25%
Partially	1	25%
No	2	50%
Don’t know	0	0%
Total	**4**	**100%**



Additional comments

Respondent 1

"GDPR has made us very conscious about personal data protection and IT security has recently been significantly increased in all aspects.

We have a Security Policy (attached) but it is not specifically part of an IT Risk Strategy (or at least it doesn’t appear that way to me because I'm not familiar with this specific methodology).

In the broader sense, we're all very aligned in minimizing risk by making everything as standardized as possible and as secure as possible.

Respondent 2

It's necessary to integrate the different points of views about the IT risk management in the company. We have good ideas but we need to align all our efforts. Using standards is a must and more resources are necessary. GDPR is triggering and accelerating changes in the company.

Respondent 3

- To apply a formal and complete IT risk evaluation.
- To create a catalog of all the assets and processes.
- To create a list of countermeasures and put them in practice.

Respondent 4

(No comments)

Resultados de la encuesta de diagnóstico aplicada a los usuarios de TI:

Q1. I know the definition of "IT Risk"			
Options		Frequency	Percentage
	Yes	3	75%
	No	1	25%
	Total	**4**	**100%**

Q2. I know the definition of "IT Risk Management"			
Options		Frequency	Percentage
	Yes	3	75%
	No	1	25%
	Total	**4**	**100%**

Q3. The company I work has policies/rules/directives about risks management related to IT			
Options		Frequency	Percentage
	Yes	2	50%
	No	1	25%
	Don’t know	1	25%
	Total	**4**	**100%**

Q4. I know which are some of the risk related to IT at work			
Options		Frequency	Percentage
	Yes	3	75%
	No	1	25%
	Total	**4**	**100%**

Q5. I experimented in the past risk events related with IT at work			
Options		Frequency	Percentage
	Yes	2	50%
	No	2	50%
	Total	**4**	**100%**

Q6. In the computer I use at work is installed an anti-malware software			
Options		Frequency	Percentage
	Yes	4	100%
	No	0	0%
	Total	**4**	**100%**

Q7. The software in the computer I use at work is always updated (operative system, applications, etc.)

Options		Frequency	Percentage
	Yes	3	75%
	No	1	25%
	Total	**4**	**100%**

Q8. I keep protected sensitive/confidential information at work (passwords, security codes, confidential documents, etc.)

Options		Frequency	Percentage
	Yes	3	75%
	No	1	25%
	Total	**4**	**100%**

Q9. Finally, please provide some ideas/comments you can give to improve the security related with the use of technology in your company and reduce the occurrence of risk events related to IT

Respondent 1
As a member of a small team in an European IT company I have to look at different IT issues. I am not the best candidate to provide a solution so my suggestion would be the implementation of specialized IT departments or training to fill these gaps.

Respondent 2
"Do not use free versions of antivirus and buy licenses for all the terminals. Schedule sessions to instruct employees about security and protection of sensitive data."

Respondent 3
To apply more restrictions for users, especially the new ones. In the development team, even the new employees have unlimited access to the whole databases. Creating logins/users may improve the security. It's necessary also some policies.

Respondent 4
More physical control. People can bring devices and copy information or install any software.

Anexo 5: Cuadro de análisis de estándares, marcos de trabajo y metodologías.

	ISO 31000:2018 Directrices para la Gestión de Riesgos		Cobit 5 For Risk Marco de trabajo	ISO/IEC 27005:2018 Tecnologías de la información - Técnicas de Seguridad - Gestión del riesgo de la seguridad de la información		MAGERIT v3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información		ISO 22301:2012 Seguridad de la Sociedad: Sistemas de Continuidad del Negocio – Requisitos
Propósito del estándar o metodología	Proporcionar directrices para gestionar el riesgo al que se enfrentan las organizaciones.		Ayudar a las organizaciones a crear valor óptimo desde TI manteniendo un balance entre los beneficios realizables y la optimización de los niveles de riesgo y uso de recursos	Proporcionar líneas guía para la gestión de los riesgos de seguridad de la información en una organización.		Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de TI.		
Principios	El propósito de la gestión del riesgo es la creación y protección del valor, en base a los siguientes principios: Integrada / Estructurada y exhaustiva / Adaptada / Inclusiva / Dinámica / Mejor información disponible / Factores humanos y culturales / Mejora continua		- Conocer las necesidades de las partes interesadas. - Cubrir la empresa de extremo a extremo. - Aplicar un único marco de trabajo integrado. - Habilitar un enfoque holístico. - Separar el gobierno de la gestión.			Objetivos: - Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. - Ofrecer un método sistemático para analizar los riesgos derivados del uso de TIC. - Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.		
Marco de referencia	Liderazgo y compromiso, a través de: Integración / Diseño / Implementación / Valoración / Mejora					ISO 31000:2009		
Proceso de Gestión de Riesgos	**Alcance, contexto y criterios**	**Definición del alcance** La organización debería definir el alcance de sus actividades de gestión del riesgo.	- Cuenta con un dominio llamado gobierno de riesgos para ayudar a asegurar que el enfoque de gestión de riesgo adoptado es apropiado para la situación de la organización y para el riesgo que afecta el logro de los objetivos.	**Establecimiento del contexto**	**Alcance y límites** - La organización debe definir el alcance y los límites de la gestión de riesgos de seguridad de la información. - El alcance necesita definirse para asegurar que todos los activos relevantes son tomados en cuenta en la evaluación del riesgo. - Los límites necesitan identificarse para abordar aquellos riesgos que surjan a través de estos límites.	**Método**	- Estudio de Oportunidad. Resultado: informe preliminar. - Determinación del alcance del proyecto. Resultado: Perfil de proyecto de análisis de riesgo. - Planificación del proyecto. Resultados: Plan de trabajo y procedimientos. - Lanzamiento del proyecto. Resultados: cuestionarios para las entrevistas, catálogo de tipos de activos, la relación de dimensiones de seguridad, criterios de valoración.	
		Contextos externo e interno La organización debería establecer los contextos externo e interno. Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos.	- Incluye prácticas de gestión para trabajar con las funciones de riesgo de nivel empresarial más amplias para entender el contexto externo. - Incluye prácticas de gestión para entender el contexto interno, que incluye determinar dónde y cómo los procesos organizacionales dependen de TI para el éxito y compararlos con las capacidades relacionadas de TI existentes.		**Establecimiento del Contexto** El contexto externo e interno para la gestión del riesgo de la seguridad de la información debe ser establecido.			
		Definición de los criterios del riesgo La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar, con relación a los objetivos. La organización debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones.	- Provee una guía a las empresas para desarrollar criterios de riesgos específicos, así como la medición de consecuencias, definir el impacto al negocio, establecer el apetito de riesgo y los límites de tolerancia y la agregación del riesgo.		**Criterio Básico** - Enfoque de gestión de riesgo. - Criterio de evaluación de riesgo. - Criterio de impacto. - Criterio de aceptación de riesgo.			
					Organización para la gestión de riesgos de seguridad de la información La organización y las responsabilidades para el proceso de gestión de riesgos de seguridad de la información deben ser establecidos y mantenidos.			

	Evaluación del riesgo	**Identificación del riesgo** El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que puedan ayudar o impedir a una organización lograr sus objetivos.	Incluye prácticas de gestión para identificar el riesgo asociado con los servicios y productos claves de la organización que dependen de TI y a identificar los factores de riesgo que contribuyen a eventos e incidentes históricos.	**Valoración del riesgo**	Identificación del riesgo - Identificación de los activos. - Identificación de las amenazas - Identificación de los controles existentes - Identificación de las vulnerabilidades - Identificación de las consecuencias	**Análisis de riesgos**	- Caracterización de los activos: Determinar los activos relevantes para la organización, su interrelación y su valor. - Caracterización de las amenazas: Determinar a qué amenazas están expuestos aquellos activos. - Caracterización de las salvaguardas: determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo. - Estimación del estado del riesgo: consta de dos actividades: a. Estimación del impacto; b. Estimación del riesgo.	
		Análisis del riesgo El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características, incluyendo, cuando sea apropiado, el nivel del riesgo. Las técnicas de análisis pueden ser cualitativas, cuantitativas o una combinación de éstas.	El análisis de riesgos es el proceso por el cual son estimados la frecuencia y el impacto de los escenarios de riesgo de TI.		**Análisis del riesgo** - Metodologías de análisis de riesgo - Evaluación de las consecuencias - Evaluación de la probabilidad de incidentes - Determinación del nivel de riesgo			
		Valoración del riesgo El propósito de la valoración del riesgo es apoyar a la toma de decisiones.	Aborda este paso del proceso intrínsecamente.		**Evaluación del riesgo** El nivel de los riesgos debe ser comparado contra los criterios de evaluación de riesgo y el criterio de aceptación de riesgo			
								8.4.3.3 Análisis de impacto - Indentificación de actividades que apoyan la provisión de productos y servicios. - Evaluación del impacto a través del tiempo de no estar realizando estas actividades. - Estableciendo y priorizando tiempos para reanudar estas actividades de manera específica a un nivel mínimo aceptable, tomando en consideración los impactos que tendría la no reanudación. - Identificación de dependencias y recursos de apoyo de estas actividades, incluyendo suplidores, compañeros de outsourcing y partes interesadas relevantes.
	Tratamiento del riesgo	**Selección de las opciones para el tratamiento del riesgo** La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales derivados del logro de los objetivos como costos, esfuerzo o desventajas de la implementación.	Incluye una guía de las opciones de respuesta comunes y cómo se aplican a un contexto de TI.	**Tratamiento del riesgo**	- Modificación del riesgo - Retención del riesgo - Evitación del riesgo - Compartición del riesgo	**Gestión de riesgos**	- Identificación de proyectos de seguridad (Se traducen las decisiones de tratamiento de los riesgos en acciones concretas) - Planificación de los proyectos de seguridad (ordenar temporalmente los programas de seguridad) - Ejecución del plan (alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado)	

		Preparación e implementación de los planes de tratamiento del riesgo El propósito de los planes del tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.	Define respuestas específicas a riesgos para abordar diferentes tratamientos para los riesgos. Utiliza el desarrollo de escenarios para la identificación de riesgos.					
				Aceptación del riesgo	Debe registrarse formalmente la decisión de aceptar los riesgos así como los responsables de dicha decisión.			
	Seguimiento y revisión	- El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso.	Incluye objetivos y métricas que pueden ser utilizados para medir el desempeño y un modelo de madurez para establecer una hoja de ruta para mejorar los procesos de gestión de riesgos.	**Monitoreo y revisión**	Los riesgos y sus factores (valor de los activos, impactos, amenazas, vulnerabilidades, probabilidad de ocurrencia) deberían ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa temprana, y mantener una vista general del entorno completo del riesgo. - Monitoreo y revisión de los factores de riesgo. - Monitoreo de la gestión, revisión y mejora.			
	Comunicación y consulta	Propósito: asistir a las partes pertinentes a comprender el riesgo - La comunicación busca promover la toma de conciencia. - La consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.	El habilitador "Información" incluye información específica a ser comunicada entre las partes interesadas.	**Comunicación y consulta**	La información acerca del riesgo debería ser intercambiada o compartida entre las personas que toman las decisiones y otras partes interesadas.			
	Registro e informe	- El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados.	Incluye prácticas de gestión para rastrear decisiones de riesgos claves y especifica entradas y salidas para estas prácticas de gestión.					

Anexo 5.B. Aporte de los marcos de trabajo en el modelo propuesto

MODELO PROPUESTO Y APORTE DE LOS MARCOS DE TRABAJO		
FASE	**Actividades**	**Marcos de trabajo utilizados**
FASE I: Alcance, contexto y criterios. Objetivo: Definir el alcance de la gestión de riesgos.	1.1 Definición de la visión, misión, objetivos, metas y alcance de la gestión de riesgos.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.3. Alcance, contexto y criterios. Describe las consideraciones a tener en cuenta para la determinación del alcance de las actividades de gestión de riesgos.
	1.2 Establecer el contexto externo e interno. - Análisis FODA. - Contexto externo: Relación con los clientes; Contexto socio-cultural; Contexto económico; Contexto regulatorio-normativo; Competencia; Relación con proveedores. - Contexto interno: Objetivos y estrategias; Estructura organizacional; Capacidades; Ambiente laboral.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.3. Alcance, contexto y criterios. Describe los aspectos a analizar para el establecimiento de los contextos externo e interno.

	1.3 Criterios de aceptación del riesgo. Niveles de aceptación del riesgo.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.3. Alcance, contexto y criterios. Describe la importancia en la determinación de los niveles de aceptación del riesgo y su coherencia con las políticas de la organización. ISO/IEC 27005:2018 Sección 7. Establecimiento del contexto. Ítem 7.2. Criterios básicos. Describe las consideraciones a tener en cuenta para definir los criterios de aceptación, los cuales varían en función de las políticas y objetivos. Asimismo, sugiere una lista de posibles dimensiones para las cuales deben establecerse dichos niveles.
	1.4 Organización y responsabilidades del proceso de gestión del riesgo: Se establecen quienes conformarán el comité de gestión de riesgos, así como sus principales funciones.	ISO/IEC 27005:2018 Sección 7. Establecimiento del contexto. Ítem 7.4. Organización para la gestión de riesgos de seguridad de la información. Cobit 5 For Risk Apéndice B.3 Estructura organizacional. Contiene información detallada acerca la estructura organizacional relevante para la función de riesgo.
FASE II. Valoración del riesgo. Objetivo: identificar y evaluar el riesgo a fin de determinar	2.1 Identificación del riesgo ▪ Identificación de los activos. ▪ Valoración de los activos. ▪ Identificación de las amenazas y vulnerabilidades.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.4.2. Identificación del riesgo. Encontrar, reconocer y describir los riesgos que ayuden o impidan el logro de los objetivos.

cuáles tienen significancia para la organización.		ISO/IEC 27005:2018 Sección 8. Evaluación del riesgo de seguridad de la información. Ítem 8.2.2. Identificación de los activos, Ítem 8.2.3. Identificación de las amenazas, Ítem 8.2.5. Identificación de las vulnerabilidades.
	2.2 Análisis del riesgo ▪ Evaluar la probabilidad de ocurrencia. ▪ Evaluar las consecuencias/impacto. ▪ Determinar el nivel de riesgo (estimar el riesgo)	ISO 31000:2018 Sección 6. Proceso. Ítem 6.4.3. Análisis del riesgo. ISO/IEC 27005:2018 Sección 8. Evaluación del riesgo de seguridad de la información. Ítem 8.2.6. Identificación de las consecuencias.
	2.3 Evaluación del riesgo de TI ▪ Priorizar el riesgo. ▪ Establecer los niveles de apetito y tolerancia.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.4.4. Valoración del riesgo.
FASE III. Análisis de impacto del negocio (BIA) Objetivo: determinar qué procesos son críticos y sus tiempos de recuperación.	3.1 Identificación de las funciones y procesos/servicios.	ISO 22301:2012 Sección 8.4.3.3 Análisis de impacto. Identificación de actividades que apoyan la provisión de productos y servicios. Evaluación del impacto a través del tiempo. Requerimientos de tiempos de recuperación. Estableciendo y priorizando tiempos. Identificación de procesos alternos.
	3.2 Establecimiento del nivel de criticidad de las funciones y procesos/servicios	
	3.3 Evaluación del impacto ▪ Evaluación del impacto por área. ▪ Evaluación del impacto. Consolidación.	
	3.4 Evaluación de tiempos (MTD, RTO, WRT, RPO)	

	3.5 Identificación de los procesos alternos.	
	3.6 Generación de informe de impacto de negocio.	
FASE IV. Tratamiento del riesgo. Objetivo: proponer planes de tratamiento de riesgo	4.1 Seleccionar las opciones para el tratamiento del riesgo.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.5. Tratamiento del riesgo. Selección de opciones de tratamiento. Preparación e implementación de los planes de tratamiento. Cobit 5 For Risk Capítulo 5. Respuesta al riesgo. Opciones de respuesta al riesgo. Selección y priorización.
	4.2 Proposición de planes de tratamiento de riesgo.	
FASE V. Seguimiento y revisión. Objetivo: monitorear los planes de tratamiento planteados.	5.1 Seguimiento, revisión y responsables.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.6. Seguimiento y revisión. Tiene como finalidad la mejora de la calidad y la eficacia del diseño. ISO/IEC 27005:2018 Sección 12. Monitoreo y revisión de riesgos de seguridad de la información. Describe aspectos a considerar para el procesos de monitoreo de los planes de acción
FASE VI. Comunicación y consulta.	6.1 Lineamientos para la comunicación y consulta.	ISO 31000:2018 Sección 6. Proceso. Ítem 6.2. Comunicación y consulta.

Objetivo: proponer estrategias de comunicación como parte del proceso de gestión.		Difusión de información a las partes interesadas. Promover la toma de conciencia y la comprensión del riesgo. ISO/IEC 27005:2018 Sección 11. Comunicación y consulta de riesgos de seguridad de la información. Describe la importancia del intercambio de información con quienes toman decisiones y otras partes interesadas,

Fuente: Elaboración propia.

Anexo 6: Instrumentos a aplicar para el modelo propuesto

6.1 Formato para el establecimiento de criterios de aceptación del riesgo

CRITERIOS DE ACEPTACIÓN DE RIESGO	
Aspecto	Criterio
Mencione aquí los aspecto para los cuales se establecerá un criterio de aceptación (ejemplo: económico, operativo, etc.)	Describa aquí el criterio de aceptación. Ejemplos: La empresa declara que no acepta una pérdida mayor a X soles) La empresa declara que no acepta una interrupción de sus servicios mayor a X horas.
…	…

6.2 Formato para el establecimiento de los niveles de aceptación del riesgo

CRITERIOS DE ACEPTACIÓN DE RIESGO			
Nivel de riesgo	Nivel de aceptación	Descripción	Estrategias
Establezca aquí el nivel de riesgo a considerar. Ejemplo: Alto, Moderado, Bajo. Puede asignar un color diferenciador para cada nivel establecido.	Establezca aquí el nivel de aceptación del riesgo. Ejemplo: Aceptable, Tolerable, No aceptable.	Describa aquí qué significa para la empresa el nivel de aceptación establecido en la columna anterior.	Establezca aquí la estrategia a aplicar para cada nivel de riesgo y aceptación. Ejemplo: Aceptar, Mitigar, Evitar, etc.
…	…	…	…

Fuente: Elaboración propia

6.3 Formato para describir los roles y funciones del comité de riesgos

COMITÉ DE GESTIÓN DE RIESGOS	
Rol	Función
Definir los roles de cada uno de los integrantes del equipo (ejemplo: Responsable de Riesgos, Responsable de Cumplimiento, etc.)	Describir las funciones del rol definido en la columna anterior.
…	…

Fuente: Adaptado de [15]. Anexo B.3.

6.4 Matriz RACI de actividades y funciones (ver anexo

MATRIZ RACI DE ACTIVIDADES Y FUNCIONES PARA EL PROCESO DE GESTIÓN DE RIESGOS					
Función					
Actividades	CEO	CTO	Responsable de riesgos	Otra función	Función N
Definir las actividades que forman parte del proceso de gestión de riesgos.	(*)	(*)	(*)	(*)	(*)
…					

(*) Establecer la responsabilidad de cada función para cada actividad mediante los valores R, A, C, I:

R: Responsable, es quien efectivamente realiza la tarea.

A: Aprobador, responsable de que la tarea se realice y rinde cuentas sobre su ejecución.

C: Consultado, posee información o capacidad necesaria para la realización de la tarea.

I: Informado, debe ser informado del avance y los resultados de la ejecución de la tarea.

Fuente: Adaptado de [15]. Anexo B.3.

6.5: Formato de identificación de activo

IDENTIFICACIÓN DE ACTIVOS - HOJA RESUMEN					
Clasificación: Especifique aquí la categoría a la que pertenece el activo: Proceso, Hardware, Software, etc.					
Elaborado por		Escriba aquí el nombre de las personas que llenaron el formato.		**Fecha**	Indique la fecha de elaboración, o rango de fechas si fuera necesario
Nr.	**Código**	**Nombre**	**Descripción**		**Responsable**
1	Indique aquí el código asignado al activo	Indique aquí el nombre completo del activo	Describa el activo de forma concreta y breve. Puede proporcionar información adicional si considera necesario, a fin de evitar ambigüedades o malas interpretaciones.		Indique aquí el nombre de la persona o área responsable del activo.
2					
3					
…					

Tabla 8. Formato de identificación de activo. Fuente: Adaptado de [34, p. 76]

6.6 Escala de valoración de los activos.

Utilice esta escala para valorar los activos catalogados a fin de determinar en qué nivel de cada dimensión se encuentra. Esta valoración es fundamental para ayudar a establecer el nivel de criticidad de un activo.

ESCALA DE VALORACIÓN DE LOS ACTIVOS			
Valor	**Confidencialidad**	**Disponibilidad**	**Integridad**
5 Muy alto	La información asociada al activo es solo accedida por el personal de alto rango, pues su divulgación afectaría irreversiblemente a la organización.	Se requiere que el activo nunca esté indisponible, pues su carencia afectaría irreversiblemente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 0%, pues la vulneración de su integridad afectaría irreversiblemente a la organización.
4 Alto	La información asociada al activo es restringida y solo personal de un proyecto específico puede acceder a ella, pues su divulgación afectaría gravemente a la organización.	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 15%, pues la vulneración de su integridad afectaría gravemente a la organización.
3 Medio	La información asociada al activo es confidencial y sólo el personal de algunas áreas internas puede acceder a ella, pues su divulgación afectaría considerablemente a la organización.	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 50%, pues la vulneración de su integridad afectaría considerablemente a la organización.
2 Bajo	La información asociada al activo es de uso interno y sólo el personal de la organización puede acceder a ella, pues su divulgación afectaría parcialmente a la organización.	Se considera que como máximo el activo puede estar indisponible por una semana, pues se carencia afectaría parcialmente a la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 85%, pues la vulneración de su integridad afectaría parcialmente a la organización.

1 Muy bajo	La información asociada al activo es pública y cualquiera puede acceder a ella, pues no impacta a la organización.	Se considera que como máximo el activo puede estar disponible por tiempo indefinido, pues su carencia no impacta en la organización.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un 100%, pues la vulneración de su integridad no impacta a la organización.

Tabla 9. Escala de valoración de los activos. Fuente: Adaptado de [35, p. 5] Tabla 5.

6.7 Tabla de valoración de los niveles de criticidad de los activos

VALORACIÓN DE LOS NIVELES DE CRITICIDAD	
Rango (resultado de la suma de los criterios de confidencialidad, disponibilidad e integridad)	**Nivel de criticidad**
De 1 a 5	Bajo
De 6 a 10	Medio
De 11 a 15	Alto

Tabla 10. Tabla de rangos para la valoración de los niveles de criticidad. Fuente: Adaptado de [36, p.53]

6.8 Formato de valoración de los activos

VALORACIÓN DE ACTIVOS								
	ACTIVO			CRITERIOS			TOTAL	Nivel de Criticidad
Nr.	Clasificación	Código	Nombre	Confidencialidad	Integridad	Disponibilidad		
1	Nombre de la clasificación del activo	Código asignado al activo	Nombre del activo	Puntuación de acuerdo a la escala del anexo 6>6.2			Suma de las puntuaciones	Nivel de criticidad de acuerdo a la tabla del anexo 6>6.3
2								
3								
…								

Tabla 11. Valoración de activos. Fuente: Adaptado de [34, p.82]

6.9 Formato de identificación de amenazas y vulnerabilidades

IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES				
ACTIVO			**Amenaza**	**Vulnerabilidad**
Nr.	**Clasificación / Código**	**Nombre**		
1	Clasificación y código del activo	Escriba aquí el nombre del activo	Describa aquí la amenaza que podría afectar al activo.	Describa aquí la vulnerabilidad que expone al activo a la amenaza.
2				
3				
…				

Tabla 12. Identificación de amenazas y vulnerabilidades. Fuente: Adaptado de [34, p.82] y [36, p.54]

6.10 Escala de valoración de la probabilidad de ocurrencia de un evento de riesgo

ESCALAS DE PROBABILIDAD DE OCURRENCIA		
CATEGORIA	**ESCALA**	**FRECUENCIA**
Muy alta	5	Describa la frecuencia de ocurrencia de un evento de riesgo para cada escala. Ejemplo: Se espera que el evento ocurra más de dos veces al año.
Alta	4	…
Moderada	3	…
Baja	2	…
Muy baja	1	…

Tabla 13. Escala de valoración de probabilidad de ocurrencia de un evento de riesgo. Fuente: Elaboración propia.

6.11 Escala de valoración del impacto de un evento de riesgo

VALORIZACIÓN DEL IMPACTO		
CATEGORIA	**ESCALA**	**DESCRIPCIÓN**
Muy alto	5	Describa lo que para la empresa significaría cada nivel de impacto. Ejemplo: Impacto adverso severo o catastrófico: • Impacto económico de hasta el 80% de los ingresos. • Hay interrupción de todas las operaciones. • Pérdida significativa de clientes y serio daño a la imagen pública.
Alto	4	…
Moderado	3	…
Bajo	2	…
Muy bajo	1	…

Tabla 14. Escala de valoración del impacto de un evento de riesgo. Fuente: Elaboración propia.

6.12 Tabla de mapeo cualitativo (mapa de calor)

MAPEO CUALITATIVO (MAPA DE CALOR)						
Impacto						
1 Muy Bajo	**2 Bajo**	**3 Moderado**	**4 Alto**	**5 Muy alto**		
Moderado	Moderado	Alto	Muy Alto	Muy Alto	**5 Muy alta**	**Probabilidad**
Bajo	Moderado	Alto	Muy Alto	Muy Alto	**4 Alta**	
Bajo	Moderado	Moderado	Alto	Alto	**3 Moderada**	
Muy Bajo	Bajo	Moderado	Moderado	Moderado	**2 Baja**	
Muy Bajo	Muy Bajo	Bajo	Bajo	Moderado	**1 Muy baja**	

Tabla 15. Tabla de mapeo cualitativo (mapa de calor). Fuente: Adaptado de [37, p. 53]

6.13 Formato para la determinación del nivel de riesgo

DETERMINACIÓN DEL NIVEL DE RIESGO								
ACTIVO			**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**	
Nr.	**Clasificación / Código**	**Nombre**					**Código**	**Nivel**
1	Clasificación y código del activo	Nombre del activo	Descripción de la amenaza	Descripción de la vulnerabilidad	Valor de la probabilidad de ocurrencia (anexo 6 > 6.6)	Valor del impacto (anexo 6 > 6.5)	Código del evento de riesgo	Resultado de multiplicar los valores de probabilidad e impacto. Indicar además la descripción del nivel.
2								
3								
…								

Tabla 16. Determinación del nivel de riesgo. Fuente: Adaptado de [3, p.54]

6.14 Tabla de nivel de criticidad del riesgo inherente.

NIVEL DE CRITICIDAD DEL RIESGO INHERENTE		
Rango de resultados	**Nivel de riesgo**	
De 1 a 4	Bajo	
De 5 a 10	Moderado	
De 12 a 25	Alto	

Tabla 17. Nivel de criticidad del riesgo inherente. Fuente: Adaptado de [36, p.53]

6.15 Tabla de valorización de la tolerancia al riesgo.

VALORIZACIÓN DE LA TOLERANCIA	
Nivel de riesgo	**Valorización**
Bajo	Aceptable
Moderado	Tolerable
Alto	Intolerable

Tabla 18. Valorización nominal de la tolerancia al riesgo. Fuente: Elaboración propia.

6.16 Formato de identificación de funciones y procesos:

FUNCIONES y PROCESOS			
Función		**Proceso/Servicio**	
Cód.	**Nombre**	**Código**	**Nombre**
Código de la función	Nombre de la función (ejemplo: Operaciones, Servicios, Comunicaciones, etc.)	Código del proceso/servicio	Nombre del proceso/servicio

Tabla 19. Identificación de funciones y procesos. Fuente: Adaptado de [38, p. 16]

6.17 Esquema de valoración de la criticidad

CRITICIDAD DE LAS OPERACIONES		
Categoría	**Nombre**	**Descripción**
1	Crítico	La función del negocio no puede realizarse si no se cuenta con ésta.
2	Importante	La operación es parte del negocio y sin ella el negocio no podría operar normalmente.
3	Menor	La operación no es una parte integral del negocio.

Tabla 20. Valoración de la criticidad. Fuente: Adaptado de [38, p. 18]

6.18 Formato para el establecimiento del nivel de criticidad de las funciones y procesos

FUNCIONES y PROCESOS					
Función		**Proceso/Servicio**		**Criticidad**	**Comentario**
Cód.	**Nombre**	**Código**	**Nombre**		
Código de la función	Nombre de la función (ejemplo: Operaciones, Servicios, Comunicaciones, etc.)	Código del proceso/servicio	Nombre del proceso/servicio	Indique aquí la categoría y nombre de la valoración de criticidad asignada	Escriba aquí un comentario que sustente la valoración asignada

Tabla 21.Establecimiento del nivel de criticidad de las funciones y procesos. Fuente: Elaboración propia (integración de tablas 19 y 20)

6.19 Tabla de escalas de impacto por área

ESCALA DE IMPACTO POR ÁREA				
IMPACTO		**ÁREA**		
Nivel	**Categoría**	**Financiero**	**Cliente**	**Imagen / Reputación**
1	Insignificante	Si el proceso no se encuentra disponible, no hay pérdidas ni afectación de los ingresos de la empresa.	Si el proceso no se encuentra disponible, no se afecta la imagen de la empresa con los clientes.	Si el proceso no se encuentra disponible, no se afecta la imagen pública de la empresa.
2	Bajo	Si el proceso no se encuentra disponible, tiene un impacto menor en los ingresos que no afectaría su rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes, pero no se pierde ninguno.	Si el proceso no se encuentra disponible, la imagen pública de la empresa podría verse afectada.
3	Moderado	Si el proceso no se encuentra disponible, tiene un impacto moderado en los ingresos y la rentabilidad.	Si el proceso no se encuentra disponible, se afecta la imagen con los clientes más importantes, perdiéndose algunos de ellos.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa.
4	Significativo	Si el proceso no se encuentra disponible, tiene un impacto significativo, afecta la rentabilidad, pero no la sostenibilidad del negocio.	Si el proceso no se encuentra disponible, se afecta la imagen de la empresa con los clientes, generándose una pérdida significativa.	Si el proceso no se encuentra disponible, se afecta significativamente la imagen de la empresa, dando ventaja competitiva a la competencia.
5	Severo	Si el proceso no se encuentra disponible, tiene un impacto severo generando pérdida económica, afectando la rentabilidad y su continuidad en el mercado.	Si el proceso no se encuentra disponible, se afecta seriamente la imagen de la empresa y hay pérdida masiva de clientes.	Si el proceso no se encuentra disponible, afecta totalmente la imagen de la empresa, perdiendo posicionamiento.

Tabla 22. Escalas de impacto por área. Fuente: Adaptado de [39, p.34, 35 y 37]

6.20 Formato de valoración del impacto por área y escala de tiempo.

VALORACIÓN DEL IMPACTO								
Proceso/Servicio		**TIEMPOS (horas)**						
Código	**Nombre**	0 - 1	1 - 4	4 - 8	8 - 24	24 - 48	48 - 72	+72
Código del proceso/servicio	Nombre del proceso/servicio	(*)	(*)	(*)	(*)	(*)	(*)	(*)

Tabla 23. Valoración del impacto por área y escala de tiempo.

(*) Valoración del impacto (anexo 6 > 6.19) para cada escala de tiempo por cada área considerada

Fuente: [39, p. 47]

6.21 Formato para el establecimiento de los grados de importancia de las áreas.

GRADO DE IMPORTANCIA DE LAS ÁREAS	
ÁREA	**PORCENTAJE**
Nombre del área a considerar en la evaluación de impacto (ejemplo: financiero, clientes, imagen, etc.)	Indique aquí el porcentaje asignado
…	…
TOTAL	100%

Tabla 24. Establecimiento de grado de importancia de las áreas. Fuente: Adaptado de [39, p.55]

6.22 Definiciones de los tipos de tiempos de recuperación

TIEMPOS DE RECUPERACIÓN	
Tiempo	**Descripción**
MTD (Maximum Torerable Downtime, Tiempo de inactividad máximo tolerable)	Es el tiempo máximo que un negocio puede tolerar la ausencia o indisponibilidad de una función/proceso particular de negocio. MTD = RTO + WRT
RTO (Recovery Time Objective, Tiempo de recuperación objetivo)	Es el tiempo disponible para recuperar sistemas y recursos interrumpidos.
WRT (Work Recovery Time, Tiempo de recuperación del trabajo)	Es el tiempo que toma recuperar y volver a poner en funcionamiento funciones/procesos críticos del negocio, una vez que los sistemas han sido restaurados.
RPO (Recovery Point Objective, Punto de recuperación objetivo)	Cantidad o magnitud de pérdida de datos –en términos de un período de tiempo– que puede ser tolerado por los sistemas críticos del negocio.

Tabla 25. Tipos de tiempos de recuperación. Fuente: Adaptado de [38, p.18]

6.23 Formato para el establecimiento de los tiempos de recuperación

FUNCIONES/PROCESOS CRITICOS y TIEMPOS DE RECUPERACIÓN							
Función		**Proceso/Servicio**		**TIEMPOS (horas)**			
Cód.	**Nombre**	**Cód.**	**Nombre**	**MTD**	**RTO**	**WRT**	**RPO**
Código de la función	Nombre de la función (ejemplo: Operaciones, Servicios, Comunicaciones, etc.)	Código del proceso / servicio	Nombre del proceso / servicio	(*)	(*)	(*)	(*)

Tabla 26. Establecimiento de tiempos de recuperación.

(*) Tiempo –en horas- estimado para cada uno de los tipos de tiempos de recuperación.

Fuente: Elaboración propia.

6.23b Formato de reporte de incidente

REPORTE DE INCIDENTE [CÓDIGO]	
Fecha	Fecha de registro del incidente
De	Persona que registra el incidente
Información de contacto	Correo, teléfono u otra información de contacto de la persona que registra el incidente
Para	Persona a la que se reporta el incidente
El incidente fue detectado / observado / descubierto el día: Fecha a horas: Hora, en: Lugar donde se identificó el incidente.	
Prioridad: ○ 1 = baja ○ 3 = Media ○ 5 = alta (Nivel de prioridad en la atención)	
Sistema(s) afectado(s)	Lista de sistemas o aplicaciones afectados por el incidente
Información afectada	Lista de datos, documentos e información que ha sido afectada por el incidente
Descripción del incidente	Descripción detallada del incidente. Indicar el contexto, condiciones previas y alguna otra información que dé cuenta del incidente ocurrido.
Acciones ejecutadas	Acciones que fueron ejecutadas luego de la ocurrencia del incidente y descripción de las nuevas condiciones del incidente, si fuera el caso.
Acciones recomendadas	Lista de acciones adicionales a ejecutar para el tratamiento del incidente y la recuperación del estado previo al mismo.
Personas a contactar	Personas adicionales a contactar, para ser informadas o para colaborar en la ejecución de acciones posteriores y tratamiento del incidente.
Información adicional	Cualquier información adicional asociada al incidente o a su tratamiento.
Comentarios post-gestión del incidente	Comentarios u observaciones posteriores al tratamiento del incidente. Lecciones aprendidas y buenas prácticas. Recomendaciones para la mejora de planes de tratamiento en los riesgos que puedan estar asociados o en nuevos riesgos detectados.

Tabla 27. Formato de reporte de incidente. Fuente: Elaboración propia.

6.24 Formato para la descripción de los procesos alternos

PROCESOS ALTERNOS Y PROCEDIMIENTOS DE RECUPERACIÓN					
Proceso/Servicio		Proceso alterno			
Cód.	Nombre	Descripción	Acciones	Responsables	Recursos
Código del proceso/servicio	Nombre del proceso/servicio	Descripción del proceso alterno a seguir.	Lista de acciones a ejecutar para la realización del proceso alterno.	Actores responsables y colaboradores (personas específicas, áreas, equipos, etc.)	Lista de recursos (materiales, digitales, económicos, información, etc.) que serán utilizados en el proceso.
…	…	…	…	…	…

Tabla 28. Formato para la descripción de procesos alternos. Fuente: Elaboración propia.

6.25 Estructura del informe de impacto

INFORME DE IMPACTO DE NEGOCIO	
Elaborado por:	
Versión:	Fecha: / /
Dirigido a:	

El equipo de gestión de riesgos ha realizado el análisis de impacto de continuidad para la organización y pone a su disposición el informe resumen del proceso y sus resultados. El informe incluye 4 cuadros resumen y 3 anexos.

- Cuadro 1: Resumen de procesos y funciones de negocio, indicando su nivel de criticidad.
- Cuadro 2: Resumen de la evaluación de impacto (consolidado) en 7 rangos de tiempo.
- Cuadro 3: Resumen con los tiempos de recuperación estimados.
- Cuadro 4: Procesos alternos y procedimientos de recuperación para los procesos críticos.

Anexos:

- Anexo 1. Escala de criticidad de las operaciones.
- Anexo 2. Escala de impacto por área.
- Anexo 3. Descripción de los tiempos de recuperación.

Cuadro 1. CRITICIDAD DE FUNCIONES y PROCESOS

Función		Proceso/Servicio		Criticidad	Comentario
Cód.	Nombre	Cód.	Nombre		

Cuadro 2. EVALUACIÓN DEL IMPACTO - CONSOLIDADO

Proceso/Servicio		Tiempos (horas)						
Cód.	Nombre	0 - 1	1 - 4	4 - 8	8 - 24	24 - 48	48 - 72	+72

Cuadro 3. TIEMPOS DE RECUPERACIÓN							
Función		Proceso/Servicio		Tiempos (horas)			
Cód.	Nombre	Cód.	Nombre	MTD	RTO	WRT	RPO

Cuadro 4. PROCESOS ALTERNOS Y PROCEDIMIENTOS DE RECUPERACIÓN					
Proceso/Servicio		Proceso alterno			
Cód.	Nombre	Descripción	Acciones	Responsables	Recursos

Anexos:

Anexo 1. ESCALA DE CRITICIDAD DE LAS OPERACIONES		
Categoría	Nombre	Descripción

Anexo 2. ESCALA DE IMPACTO POR ÁREA				
IMPACTO		ÁREA		
Nivel	Categoría	Financiero	Cliente	Imagen / Reputación

Anexo 3. TIEMPOS DE RECUPERACIÓN	
Tiempo	**Descripción**
MTD	
RTO	
WRT	
RPO	

Tabla 29. Estructura del informe de impacto de negocio. Fuente: Elaboración propia.

6.26 Formato para el tratamiento de riesgos.

TRATAMIENTO DEL RIESGO						
Riesgo		**Activo**	**Amenaza**	**Vulnerabilidad**	**Valorización**	**Estrategia**
Código	**Nivel**	**Clasificación / Código / Nombre**				
Código del riesgo	Nivel del riesgo	Clasificación, código y nombre del activo	Descripción de la amenaza	Descripción de la vulnerabilidad	Valorización de la tolerancia al riesgo	Estrategia de tratamiento (mitigar, evitar, aceptar, compartir)

Tabla 30. Tratamiento del riesgo. Adaptado de [34, p. 91]

6.27 Formato para el establecimiento de planes de tratamiento de riesgos

PLAN DE TRATAMIENTO DE RIESGO	
PROYECTO	Código del proyecto
RIESGOS A TRATAR	Código de los riesgos involucrados
ACTIVO ASOCIADO	Clasificación, código y nombre del activo asociado
PLAN DE ACCIÓN	Breve denominación del proyecto.
DESCRIPCIÓN	Descripción detallada del proyecto.
COSTO	Detalle de los costos: personas, tiempo, costo, etc.
PRESUPUESTO ASIGNADO	Presupuesto o recursos asignados al proyecto.
RESPONSABLES	Responsables de la ejecución del proyecto.

Tabla 31. Establecimiento de planes de tratamiento de riesgos. Adaptado de [34, p.92-93] y [36, p.65-66]

6.28 Formato para el seguimiento y revisión de los planes de acción

SEGUIMIENTO y REVISIÓN DE PLANES DE ACCIÓN				
Proyecto	**% Avance**	**Presupuesto asignado / ejecutado**	**Estado**	**Fecha objetivo**
Denominación del proyecto	Indicar el porcentaje de avance en la ejecución	Indicar el presupuesto asignado y el monto ya ejecutado.	Indicar el estado de ejecución del proyecto (ejemplo: no iniciado, en progreso, culminado, etc.)	Fechas establecidas para la culminación del proyecto. Indicar si hay retrasos o cancelaciones.
…				
…				
…				

Tabla 32. Seguimiento y revisión de los planes de acción. Fuente: Adaptado de [34, p.97]

6.29 Formato para el establecimiento de acciones de comunicación

ACCIONES DE COMUNICACIÓN			
Fase	**Acción de comunicación**	**Descripción**	**Instrumentos**
Antes	Indicar aquí la acción de comunicación (ejemplo: Educación, Capacitación, Información, etc.)	Describir aquí en que consiste la actividad, su objetivo y a quienes está dirigida.	Detalle aquí los medios o instrumentos a utilizar para cada acción de comunicación.
	Acción 2	…	…
	Acción N	…	…
Durante			
Después			

Tabla 33. Establecimiento de acciones de comunicación. Fuente: Elaboración propia.

Anexo 6.B. **Resumen de resultados del programa de capacitación**

Programa de capacitación – Reporte final. Resumen

Información

El presente informe resume los resultados de la ejecución del curso de capacitación: "*Riesgos asociados al uso de tecnología y seguridad de la información*", llevado a cabo entre los meses de Junio y Setiembre de 2019.
Participantes: CEO, CTO, Customer Satisfaction (2 personas), Marketing & Sales (2 personas) Development Team (3 personas), Diseñador Web (1 persona)

Resultados

Los participantes fueron consultados sobre el nivel de conformidad de cada criterio considerado en la encuesta aplicada a la finalización del curso.
Cada criterio evaluado tiene una ponderación de 1 a 4 y se incluye el promedio por cada ítem. El promedio global de todos los ítems ha sido 3.74/4, lo que demuestra una evaluación favorable del curso.

NIVEL DE SATISFACCIÓN DE LOS ASISTENTES AL PROGRAMA DE CAPACITACIÓN					
Criterio evaluado	En total desacuerdo	En desacuerdo	De acuerdo	Totalmente de acuerdo	Promedio
	1	2	3	4	
El curso ha sido de gran utilidad para mi actividad diaria.	0	0	1	9	3.9 / 4

El material fue claro y fácil de comprender.	0	0	5	5	3.5 / 4
Las presentaciones fueron claras e hicieron las sesiones más interesantes	0	0	4	6	3.6 / 4
El facilitador estaba bien preparado.	0	0	1	9	3.9 / 4
El facilitador sabía cómo transmitir su conocimiento.	0	0	1	9	3.9 / 4
Las sesiones dejaron tiempo suficiente para la discusión.	0	0	5	5	3.5 / 4
Recomendaría este entrenamiento a otras personas, colegas o amigos.	0	0	1	9	3.9 / 4
				Promedio global	3.74 / 4

Por otro lado, el nivel de aprovechamiento que se alcanzó fue de 81/100 en promedio. Este valor es el resultado de la consolidación de las encuestas/evaluaciones aplicadas luego de cada sesión, así como de la evaluación de la participación de los asistentes y sus preguntas. La siguiente tabla muestra el nivel de aprovechamiento por área:

NIVEL DE APROVECHAMIENTO	
(Con base en la aplicación de diversas encuestas / evaluaciones en cada sesión + participaciones y preguntas)	
Área	Nivel
Alta dirección (CEO, CTO)	82 / 100
Customer Satisfaction	76 / 100
Marketing & Sales	80 / 100
Development Team	89 / 100
Web Design	64 / 100
Promedio global	80.7 / 100

NIVEL DE ASISTENCIA	
Sesiones	Asistentes
Sesión 1	10 / 10
Sesión 2	09 / 10
Sesión 3	10 / 10
Sesión 4	08 / 10
Sesión 5 (Parte 1)	10 / 10
Sesión 5 (Parte 2)	10 / 10
Nivel asistencia	95%

Anexo 6.C. Guía para el establecimiento de políticas para el trabajo remoto

Guía para el establecimiento de políticas para el trabajo remoto

Introducción

Un trabajador podría ser considerado remoto o aislado. En situaciones particulares un trabajador podría estar solo por un corto período de tiempo, mientras en otras situaciones podría estarlo por días o semanas en una ubicación remota. Los trabajadores podrían trabajar de forma remota o aislada si ellos:

- Trabajan físicamente solos.
- Trabajan en casa o hace teletrabajo.
- Trabaja fuera durante las horas normales de trabajo.
- Viaja mucho como parte del trabajo.
- Trabaja de manera no supervisada.

Criterios generales

Las políticas que una empresa tiene para el trabajo en oficina pueden volverse más complejas al incluir la modalidad de trabajo remoto. Los siguientes criterios generales ayudarán a la organización a definir sus políticas en este escenario.

- Elegibilidad: qué cargos o posiciones son elegibles para realizarse de forma remota.
- Disponibilidad: días y horarios de trabajo y formas de contacto.
- Tiempos de respuesta: formas de comunicación, respuestas inmediatas y diferidas.
- Medición de la productividad: tiempo invertido por proyecto, número de casos resueltos, número de interacciones con clientes, etc.
- Equipamiento: qué equipos asigna la organización al trabajador remoto y qué condiciones técnicas debe satisfacer el empleado remoto en su nuevo lugar de trabajo.

- Soporte técnico: especificar el tipo de soporte técnico que tendrá el trabajador remoto y los planes de acción.
- Correcta finalización: establecer la forma en cómo se realizará la finalización del período del trabajo remoto, o la finalización del vínculo laboral.
- Entorno físico: condiciones físicas del entorno (espacio, disposición, iluminación, temperatura, etc.)
- Seguridad: medidas de seguridad, sobre todo si se trabaja en lugares públicos.
- Confidencialidad: políticas de confidencialidad para la información de la organización, de los clientes y de los empleados.

Responsabilidades del jefe

Cada jefe debe discutir con aquellos empleados que trabajan de manera remota aspectos relacionados a los siguientes temas de interés:

- Administración del desempeño: en términos de cantidad y calidad, los cuales deberán ser monitoreados.
- Salud y seguridad. Seguridad de datos y confidencialidad.
- Comunicación: formas de comunicación y medios a utilizar, así como la frecuencia, horarios y duración.
- Horarios de trabajo: establecer si se trabajará por objetivos y fechas de entrega, sin un control sobre las horas diarias dedicadas al trabajo o si se trabajará con el mismo horario de un empleado presencial u otro que se ajuste a las necesidades del contexto del trabajo.

Responsabilidades del empleado

- Ausencias: debe establecerse si las políticas de manejo de ausencias regirá sin modificaciones para los empleados remotos. El trabajo remoto no debe ser utilizado como una alternativa a las ausencias por enfermedad, por ejemplo.

- Reporte de incidentes: cualquier incidente asociado al trabajo remoto debe ser reportado de inmediato y seguir los procedimientos establecidos para su tratamiento.
- Licencias: deben seguirse los procedimientos regulares establecidos para tal fin.
- Contacto: deben indicar datos detallados de contacto en su calendario cuando no se encuentren disponibles. Adicionalmente, si el empleado cuenta con un número telefónico fijo, debe redirigir las llamadas al teléfono móvil o crear un mensaje de voz donde indique su número de contacto. De igual forma para aspectos relacionados a la correspondencia, entregas a domicilio, etc.
- Pagos por servicios e impuestos: debe analizarse, de acuerdo a la normatividad vigente si un empleado remoto puede asumir parcial o total las responsabilidades asociadas al pago de impuestos. De igual forma, llegar a un acuerdo sobre quien asume el pago de los servicios contratados para la realización del trabajo, como oficina, Internet, teléfono, etc. –si fuera el caso.
- Trabajo desde casa: el acuerdo de trabajar desde casa debe constar en un documento firmado por ambas partes. Este acto es resultado de la evaluación de la factibilidad y de su resultado satisfactorio, basados en la aplicación de la normatividad de salud y seguridad, seguridad de datos y confidencialidad.
- Reunión con clientes: los empleados remotos no deben utilizar su casa para reuniones con los clientes de la empresa, aunque es posible que –ocasionalmente- puedan haber reuniones de trabajo con colegas. Dichas reuniones deben programarse y constar en el calendario del empleado.
- Consentimiento de inspección: los empleados remotos deben permitir el acceso a sus oficinas o domicilios utilizados para el desarrollo de sus labores a fin que la organización pueda realizar una inspección del mismo y asegurarse que cumpla con las condiciones establecidas en sus políticas.

- Es responsabilidad del empleado mantener su entorno de trabajo remoto en condiciones que satisfagan las políticas establecidas por la empresa. Algunas condiciones que podrían tenerse en cuenta son:

    - Todas las laptops deben tener instalado software de encriptación en modo *"full hard disk"*.
    - Sólo deben utilizarse dispositivos de almacenamiento USB con encriptación.
    - Todas las comunicaciones deben realizarse a través de una VPN.
    - Teléfonos celulares particulares no deben ser utilizados para acceder a redes, cuentas o servicios de la organización.
    - No debe instalarse software sin autorización de la organización.
    - No debe utilizarse el correo electrónico corporativo para fines personales y viceversa.
    - Conexión segura a Internet (no compartida)
    - Contar con UPS para la laptop/PC y equipos adicionales indispensables, o en su defecto, con un estabilizador.
    - Otros que la organización considere necesarios.

Salud, seguridad y protección

- Las políticas y normatividad sobre salud y seguridad rigen por igual para todos los empleados.
- SI bien es cierto que el control ejercido sobre un trabajador remoto es limitado, éste debe adoptar las medidas necesarias que garanticen que tanto él como las personas que se vean afectadas por su actividad remota no estén expuestas a riesgos al utilizar equipamiento provisto por la organización.
- Los procedimientos asociados a la gestión de riesgos son aplicables en todos sus extremos a los empleados remotos. Es necesaria la constante supervisión e identificación de cualquier control y mejora en las condiciones que afecten la ejecución de su trabajo.

- Todos los empleados que trabajan de manera remota deben asegurarse de contar con un entorno que les garantice su concentración en el trabajo. Deben garantizar que pueden trabajar de manera libre y sin interrupciones.
- Queda prohibida la instalación no autorizada de cualquier software en las computadoras utilizadas para la ejecución del trabajo, sean o no propiedad de la organización.
- El trabajador remoto está sujeto a supervisión remota en cualquier momento, dentro de los horarios de trabajo establecidos. Cualquier incumplimiento será reportado y comunicado al jefe de línea.
- Cualquier incidente producto del uso de recursos proporcionados para el trabajo remoto debe ser reportado de acuerdo a los procedimientos establecidos por la organización.
- Deben considerarse los riesgos asociados al trabajo remoto, teniendo en cuenta eventos como:
    - Revelación de datos sensibles de la organización, empleados o clientes.
    - Pérdida o daño de datos críticos para la organización.
    - Daño a la infraestructura organizacional y servicios debido a la propagación de malware (virus, troyanos, etc.).
    - Posibilidad de sufrir ataques de hacking debido al uso de puntos de acceso a Internet no autorizados.
    - Uso incorrecto de datos debido al uso no controlado de dispositivos externos de almacenamiento.
    - Otros daños operacionales o a la reputación.

Trabajo remoto temporal

- En caso de algún desastre natural o evento que impida que los empleados realicen su trabajo en las oficinas de la organización, ésta deberá adoptar las medidas necesarias para que sus empleados puedan seguir realizando su trabajo de manera remota, por razones de continuidad de negocio. Las

políticas y procedimientos para este fin deben constar como parte del Plan de Continuidad de la organización.

- Los empleados deben tener en cuenta que es su responsabilidad asegurarse de tener acceso a su laptop de trabajo para permitirle realizar su trabajo en casos de emergencia, en la medida en que esto le sea posible.
- La organización deberá establecer la forma en que se monitoree el trabajo remoto temporal en estas circunstancias, tanto en cantidad como en calidad.
- La organización acepta que bajo las circunstancias descritas la eficiencia operacional puede verse afectada, no solamente por el hecho del trabajo remoto en sí, sino además, porque las condiciones de trabajo en el hogar son distintas y en general, menores que las ofrecidas en el centro de trabajo.

Monitoreo y revisión

- Las políticas deberán serán revisadas anualmente y deberán ajustarse a la legislación vigente y a los cambios organizacionales.

Anexo 7: Formato de evaluación del modelo (juicio experto)

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

Autor: Jorge Rodríguez Castro

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es someter a evaluación el modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, principalmente, ISO 27005, Cobit 5, Magerit) y está orientado a organizaciones que brindan servicios de gestión de información bajo la modalidad de Software como Servicio.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Grado académico y profesión
Áreas de experiencia profesional
Institución donde labora
Tiempo de experiencia

II. VALIDACIÓN

Se utilizarán los siguientes indicadores y criterios para la evaluación del modelo.

Indicador	Criterio	Valoración				
		Muy malo	Malo	Regular	Bueno	Muy bueno
CLARIDAD	El contenido se presenta utilizando un lenguaje apropiado que facilita su comprensión.	1	2	3	4	5
OBJETIVIDAD	El contenido presentado es objetivo y concreto, y está expresado en conductas observables o medibles.	1	2	3	4	5
COHERENCIA	Existe una correspondencia lógica entre el contenido presentado y la teoría.	1	2	3	4	5
PERTINENCIA	El contenido es el apropiado y acorde con la dimensión expuesta. No está fuera de lugar.	1	2	3	4	5
SUFICIENCIA	La cantidad y calidad de los elementos presentados en el contenido son suficientes.	1	2	3	4	5
RELEVANCIA	El contenido presentado es importante y determinante para lograr el entendimiento del tema.	1	2	3	4	5

III. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

FASE	Actividad	Criterios						Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos							
	Contexto externo e interno							
	Criterios de aceptación del riesgo							
	Organización y responsabilidades del proceso de gestión de riesgos							
FASE II. Valoración del riesgo	Identificar el riesgo							
	Análisis del riesgo de TI							
	Evaluación del riesgo de TI							
FASE III. Análisis del impacto del negocio (BIA)	Identificación de las funciones y procesos/servicios							
	Establecimiento del nivel de criticidad de las funciones y procesos/servicios							
	Evaluación de impacto							
	Evaluación de tiempos							
	Identificación de procesos alternos							
	Generación de informe de impacto de negocio							
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo							
	Proposición de planes de tratamiento del riesgo							
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables							
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta							
	TOTAL							

IV. RESULTADOS

Opinión:

	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

_____

Anexo 8: Resultados de evaluación por juicio de expertos

RESULTADOS DE VALIDACIÓN POR JUICIO DE EXPERTOS																									
Fase	**Actividad**	**Experto 1**						**Experto 2**						**Experto 3**						**Experto 4**					
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	Contexto externo e interno	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	4	4	5	5
	Criterios de aceptación del riesgo	4	4	4	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5
	Organización y responsabilidades del proceso de gestión de riesgos	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	4	4	4
TOTAL		**18**	**19**	**19**	**20**	**19**	**20**	**20**	**20**	**19**	**20**	**19**	**20**	**20**	**20**	**20**	**20**	**19**	**20**	**20**	**20**	**19**	**18**	**18**	**19**
FASE II. Valoración del riesgo	Identificar el riesgo	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5
	Análisis del riesgo de TI	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	Evaluación del riesgo de TI	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
TOTAL		**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**15**	**14**	**15**
FASE III. Análisis del	Identificación de las funciones y procesos/servicios	5	5	5	5	4	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5

impacto del negocio (BIA)	Establecimiento del nivel de criticidad de las funciones y procesos/servicios	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	Evaluación de impacto	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5
	Evaluación de tiempos	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	Identificación de procesos alternos	3	1	4	3	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	
	Generación de informe de impacto de negocio	3	3	3	2	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	
TOTAL		**25**	**24**	**27**	**25**	**22**	**24**	**30**	**30**	**30**	**30**	**29**	**29**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**	**29**	**28**	**30**	
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	
	Proposición de planes de tratamiento del riesgo	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	
TOTAL		**10**	**10**	**10**	**10**	**9**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**10**	**8**	**9**	**10**	
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	5	
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta	4	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
	TOTAL	**77**	**78**	**80**	**79**	**75**	**79**	**85**	**85**	**84**	**85**	**83**	**84**	**85**	**85**	**85**	**85**	**84**	**85**	**85**	**85**	**84**	**79**	**78**	**84**	

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

Autor: Jorge Rodríguez Castro

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es someter a evaluación el modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, principalmente, ISO 27005, Cobit 5, Magerit) y está orientado a organizaciones que brindan servicios de gestión de información bajo la modalidad de Software como Servicio.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
GILBERTO CORRIÓN BARCO
Grado académico y profesión
DOCTOR EN CIENCIAS PEC. COMPUTACIÓN Y SISTEMAS / INGENIERO
Áreas de experiencia profesional
INFRAESTRUCTURA TECNOLÓGICA, SEGURIDAD INFORMÁTICA
Institución donde labora
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
Tiempo de experiencia
15 AÑOS

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

FASE	Actividad	Criterios						Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos	5	5	5	5	5	5	
	Contexto externo e interno	4	5	5	5	5	5	
	Criterios de aceptación del riesgo	4	4	4	5	4	5	
	Organización y responsabilidades del proceso de gestión de riesgos	5	5	5	5	5	5	
FASE II. Valoración del riesgo	Identificar el riesgo	5	5	5	5	5	5	
	Análisis del riesgo de TI	5	5	5	5	5	5	
	Evaluación del riesgo de TI	5	5	5	5	5	5	
FASE III. Análisis del impacto del negocio (BIA)	Identificación de las funciones y procesos/servicios	5	5	5	5	4	5	
	Establecimiento del nivel de criticidad de las funciones y procesos/servicios	5	5	5	5	5	5	
	Evaluación de impacto	5	5	5	5	5	5	

	Evaluación de tiempos	4	5	5	5	5	5	
	Identificación de procesos alternos	3	1	4	3	1	2	
	Generación de informe de impacto de negocio	3	3	3	2	2	2	
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo	5	5	5	5	5	5	
	Proposición de planes de tratamiento del riesgo	5	5	5	5	4	5	
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables	5	5	5	5	5	5	
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta	4	5	4	4	5	5	
	TOTAL	77	78	80	79	75	79	

IV. RESULTADOS

Opinión:

✓	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

Autor: Jorge Rodríguez Castro

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es someter a evaluación el modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, principalmente, ISO 27005, Cobit 5, Magerit) y está orientado a organizaciones que brindan servicios de gestión de información bajo la modalidad de Software como Servicio.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Oliver Vásquez Leyva
Grado académico y profesión
Magister / Ingeniero de Sistemas.
Áreas de experiencia profesional
Gestión de TI
Institución donde labora
Universidad Señor de Sipán
Tiempo de experiencia
13 años

1

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

FASE	Actividad	Criterios						Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos	5	5	4	5	5	5	Revisar M/V.
	Contexto externo e interno	5	5	5	5	5	5	
	Criterios de aceptación del riesgo	5	5	5	5	5	5	
	Organización y responsabilidades del proceso de gestión de riesgos	5	5	5	5	4	5	Considerar el equipo humano.
FASE II. Valoración del riesgo	Identificar el riesgo	5	5	5	5	5	5	
	Análisis del riesgo de TI	5	5	5	5	5	5	
	Evaluación del riesgo de TI	5	5	5	5	5	5	
FASE III. Análisis del impacto del negocio (BIA)	Identificación de las funciones y procesos/servicios	5	5	5	5	4	5	Ampliar a todos los relevantes como mínimo.
	Establecimiento del nivel de criticidad de las funciones y procesos/servicios	5	5	5	5	5	5	
	Evaluación de impacto	5	5	5	5	5	4	Evaluar relación en costos.

	Evaluación de tiempos	5	5	5	5	5	5	
	Identificación de procesos alternos	5	5	5	5	5	5	
	Generación de informe de impacto de negocio	5	5	5	5	5	5	
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo	5	5	5	5	5	5	
	Proposición de planes de tratamiento del riesgo	5	5	5	5	5	5	
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables	5	5	5	5	5	5	
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta	5	5	5	5	5	5	
	TOTAL	85	85	84	85	83	84	

IV. RESULTADOS

Opinión:

K	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

Autor: Jorge Rodríguez Castro

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es someter a evaluación el modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, principalmente, ISO 27005, Cobit 5, Magerit) y está orientado a organizaciones que brindan servicios de gestión de información bajo la modalidad de Software como Servicio.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
Jessie Leila Bravo Jaico
Grado académico y profesión
Dra en Ciencias de la Computación y Sistemas - Ing. de Computación y Sistemas
Áreas de experiencia profesional
Gestión de Tecnologías de Información - Seguridad Informática
Institución donde labora
UNPRG - USAT
Tiempo de experiencia
25 años

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

FASE	Actividad	Criterios						Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos	5	5	5	5	5	5	
	Contexto externo e interno	5	5	5	5	4	5	Considerar evidencias de incidentes de seguridad
	Criterios de aceptación del riesgo	5	5	5	5	5	5	
	Organización y responsabilidades del proceso de gestión de riesgos	5	5	5	5	5	5	
FASE II. Valoración del riesgo	Identificar el riesgo	5	5	5	5	5	5	
	Análisis del riesgo de TI	5	5	5	5	5	5	
	Evaluación del riesgo de TI	5	5	5	5	5	5	
FASE III. Análisis del impacto del negocio (BIA)	Identificación de las funciones y procesos/servicios	5	5	5	5	5	5	
	Establecimiento del nivel de criticidad de las funciones y procesos/servicios	5	5	5	5	5	5	
	Evaluación de impacto	5	5	5	5	5	5	

	Evaluación de tiempos	5	5	5	5	5	5	
	Identificación de procesos alternos	5	5	5	5	5	5	
	Generación de informe de impacto de negocio	5	5	5	5	5	5	
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo	5	5	5	5	5	5	
	Proposición de planes de tratamiento del riesgo	5	5	5	5	5	5	
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables	5	5	5	5	5	5	
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta	5	5	5	5	5	5	
	TOTAL							

IV. RESULTADOS

Opinión:

✓	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN COMO APOYO EN LA CONTINUIDAD DEL NEGOCIO EN UNA EMPRESA QUE BRINDA SOFTWARE COMO SERVICIO

Autor: Jorge Rodríguez Castro

INFORME DE OPINION DE EXPERTO

Objetivo

El objetivo del presente informe es someter a evaluación el modelo de gestión de riesgos de TI presentado por el tesista. El modelo propuesto surge de la armonización de diversos marcos de trabajo, estándares y metodologías (ISO 31000, principalmente, ISO 27005, Cobit 5, Magerit) y está orientado a organizaciones que brindan servicios de gestión de información bajo la modalidad de Software como Servicio.

I. DATOS GENERALES del EXPERTO

Nombres y apellidos
ERNESTO KARLO CELI ARÉVALO
Grado académico y profesión
DOCTOR EN ADMINISTRACIÓN, INGENIERO EN COMPUTACIÓN Y SISTEMAS
Áreas de experiencia profesional
AUDITORÍA, CONTROL INTERNO Y GESTIÓN DE RIESGOS DE TI
Institución donde labora
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
Tiempo de experiencia
25 AÑOS

III. FICHA DE EVALUACIÓN

Instrucciones: Asigne una valoración (1 a 5) para cada criterio en cada actividad de acuerdo a la escala de valoración presentada en el ítem anterior.

FASE	Actividad	Criterios						Comentarios / Observaciones
		Claridad	Objetividad	Coherencia	Pertinencia	Suficiencia	Relevancia	
FASE I. Alcance, Contexto y Criterios	Misión, Visión, Objetivos y Metas de la gestión de riesgos	5	5	5	5	5	5	
	Contexto externo e interno	5	5	4	4	5	5	
	Criterios de aceptación del riesgo	5	5	5	5	4	5	
	Organización y responsabilidades del proceso de gestión de riesgos	5	5	5	4	4	4	
FASE II. Valoración del riesgo	Identificar el riesgo	5	5	5	5	4	5	
	Análisis del riesgo de TI	5	5	5	5	5	5	
	Evaluación del riesgo de TI	5	5	5	5	5	5	
FASE III. Análisis del impacto del negocio (BIA)	Identificación de las funciones y procesos/servicios	5	5	5	5	5	5	
	Establecimiento del nivel de criticidad de las funciones y procesos/servicios	5	5	5	5	5	5	
	Evaluación de impacto	5	5	5	5	5	5	
	Evaluación de tiempos	5	5	5	5	5	5	

	Identificación de procesos alternos	5	5	5	5	4	5	
	Generación de informe de impacto de negocio	5	5	5	4	4	5	
FASE IV. Tratamiento del riesgo	Selección de opciones para el tratamiento del riesgo	5	5	5	4	5	5	
	Proposición de planes de tratamiento del riesgo	5	5	5	4	4	5	
FASE V. Seguimiento y revisión	Seguimiento, revisión y responsables	5	5	5	4	4	5	
FASE VI. Comunicación y consulta	Lineamientos para la comunicación y consulta	5	5	5	5	5	5	
	TOTAL	85	85	84	79	78	84	

IV. RESULTADOS

Opinión:

X	FAVORABLE		DEBE MEJORAR		DESFAVORABLE

Firma:

Anexo 9. Perfil de expertos

La información detallada a continuación ha sido obtenida del Directorio Concytec: https://dina.concytec.gob.pe/appDirectorioCTI/

PERFIL DE EXPERTO	
	**Gilberto Carrión Barco** Doctor en Ciencias de la Computación y Sistemas. Maestro en Ingeniería de Sistemas, Magister en Docencia Universitaria. Ingeniero en Computación e Informática y Licenciado en Administración Pública, con Colegiatura N° 90931 por el Colegio de Ingenieros del Perú, habilitado. Con más de 12 años de experiencia en docencia universitaria en UNPRG, USS, UTP, USMP, USAT e Investigador en la línea Tecnologías de la Información, Gobierno Electrónico y Gestión por Procesos y Gestión por Resultados. Amplia experiencia como Jurado y Asesor de Investigaciones tanto en pregrado como en postgrado. Comprometido con el trabajo en equipo, proactivo y con vocación de servicio.

Datos académicos

Grado	Título	Centro de Estudios
LICENCIADO / TÍTULO	INGENIERO EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN ADMINISTRACIÓN PÚBLICA	UNIVERSIDAD SEÑOR DE SIPÁN
MAGISTER	MAESTRO EN INGENIERIA DE SISTEMAS, ESPECIALIDAD: CON MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAGISTER EN DOCENCIA UNIVERSITARIA	UNIVERSIDAD PRIVADA CÉSAR VALLEJO

DOCTORADO	DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DOCENTE ORDINARIO TIEMPO COMPLETO CATEGORÍA AUXILIAR	2008-08-01	A la actualidad
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2013-12-01	2016-01-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE AREA ADMINISTRATIVA RED TELEMÁTICA	2010-07-01	2011-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DE LABORATORIO	2010-04-01	2010-09-01
INSTITUTO DE EDUCACION SUPERIOR TECNOLOGICO PRIVADO ABACO	GERENTE DE ALTA TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA	2004-03-01	2006-01-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C. O UTP S.A.C.	Ordinario-Auxiliar	Mayo 2014	A la actualidad
UNIVERSIDAD DE SAN MARTIN DE PORRES	Ordinario-Auxiliar	Agosto 2010	Noviembre 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Agosto 2008	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Ordinario-Auxiliar	Agosto 2006	Diciembre 2009
UNIVERSIDAD SENOR DE SIPAN SAC	Ordinario-Asociado	Abril 2006	A la actualidad

Experiencia como asesor de tesis

Universidad	Tesis	Tesistas	Fecha aceptación
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Rosa America Cobeñas Sanchez	Noviembre 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guevara Chumán, Javier Gustavo	Agosto 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Rivas Estrada, Carol Meliza; Estrada Masgo, Danny Christian	Junio 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arévalo Diaz Janira; Sánchez Pérez Cinthya del Milagro	Febrero 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ramírez Arrunátegui Pamela Susanne; Rojas Muñoz Jonatan Jorge	Abril 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Apolaya Segura Carlos Eduardo; Vilchez Castillo Sylvía Susana	Junio 2018
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Palacios Ormeño, Julio César	Noviembre 2013
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Arrieta Gómez, Víctor Manuel; Camacho Aguirre, Martin Horacio	Julio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Villegas Carrasco, Carlos Alonso; Negreiros Chinchihuara, Wilfredo Martin	Octubre 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Sacravilca Narciso, Dante Gonzalo; López Alarcón, Absalón	Junio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Balcazar De Los Santos, César Augusto; Correa Villegas, Ricardo	Octubre 2013

PERFIL DE EXPERTO

Jessie Leila Bravo Jaico

Ing. de Computación y Sistemas. Primera Promoción de la Universidad Privada Antenor Orrego de Trujillo. Doctora en Ciencias de Computación y Sistemas en la USS. Magister en Informática y Multimedia en la Universidad de Los Lagos - Chile. Magister en Administración de empresas con mención en Gerencia Empresarial de la Universidad Nacional Pedro Ruiz Gallo. Especialización en Redes Informáticas, Gestión de proyectos, Auditoría y consultoría de sistemas. Asesora y Consultora de TI en empresas de la región.

Datos Académicos

Grado	Título	Centro de Estudios
MAGISTER	MAGÍSTER EN INFORMÁTICA Y MULTIMEDIA	UNIVERSIDAD SAN PEDRO
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
BACHILLER	BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
MAGISTER	MAESTRA EN ADMINISTRACION CON MENCION EN GERENCIA EMPRESARIAL	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
DOCTORADO	DOCTORA EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
SERVIMEDICOS S.A.C.	CONSULTORA TI	2006-06-01	2008-09-01
INSTITUTO DE ALTA CALIDAD DE ATENCION A LA SALUD EN LIQUIDACION	CONSULTORA TI	2005-04-01	2007-07-01

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2003-09-01	2006-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2001-05-01	2003-09-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DESARROLLO SISTEMAS	1996-06-01	2000-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECCIÓN DE ESCUELA	1997-09-01	1999-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	MIEMBRO COMITÉ DIRECTIVO	1996-12-01	1999-12-01
CIS - CATSOFT S.R.LTDA.	ANALISTA-DISEÑADORA	1996-09-01	1997-12-01
CUERPO MÉDICO HOSPITAL NACIONAL ALMANZOR AGUINAGA ASENJO	PROGRAMADORA	1993-01-01	1993-03-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Principal	Junio 2010	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Contratado	Agosto 2002	A la actualidad
UNIVERSIDAD JUAN XXIII-VALLE JEQUETEPEQUE	Contratado	Agosto 1999	Diciembre 2000
UNIVERSIDAD SAN PEDRO	Contratado	Setiembre 1998	Diciembre 1999
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Mayo 1998	Diciembre 2001
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Contratado	Octubre 1994	Abril 1998

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	CÉSAR WENCESLAO DE LA CRUZ GUERRERO y JUAN CARLOS VASQUEZ MONTENEGRO	Abril 2008
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	Santa Maria Becerra, Franck Jhonathan	Junio 2012
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	BURGA BASTO, JORGE HUMBERTO JESÚS y LEY CUÉN RODAS, CHRISTIAN ALEXIS	Abril 2011
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	RICHARD TUSET TRINIDAD y DANIEL ALEJANDRO YI RAMOS	Abril 2011
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	César Augusto López Nicolini	Junio 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Fernández Vílchez Richar Marvin	Enero 2012
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	ALARCÓN CUSMAN JOSÉ CARLOS y CHERO IZQUIERDO JULIO FRANCISCO	Mayo 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Roxana Paola Bazan becerra	Febrero 2001

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	María del Rosario Becerra Aguilar	Setiembre 2002
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guisella Lontop Vilchez/Franklin Terán/Melvy terán	Junio 2003
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Milagros Vanessa Peña Seclén/Monica Lecca Vinces	Abril 2004
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Javier Medina Campaña	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	CHANAME BALDERA, OSCAR ENRIQUE	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Chirinos Fernandez Maykol	Julio 2007
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Leiva Peña	Febrero 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	GONZALO MARTIN ROMERO ABANTO y ROBERTH CÓRDOVA OBLITAS	Noviembre 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Olano Díaz, Juan Daniel; Sánchez Aguilar, Segundo Román	Marzo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Pérez Artemio, Calderón; Vásquez Hoyos, Alvaro	Julio 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Cubas Penas, Clara Patricia	Abril 2018

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Niño Morante, Nilton Rogger	Mayo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arenas Morales, Victor Jaime / Brios Guevara, Lessly Yein	Marzo 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	LARREA DUPIS CARLO ANTONIO / HERNÁNDEZ CAMPOS ROBERT DANILO	Marzo 2019

PERFIL DE EXPERTO

Oliver Vásquez Leiva

Experiencia docente en las ciencias de la educación, ingeniería de sistemas, administración y gestión de empresas en los sectores de la ingeniería, producción y comercialización. La práctica de la mejora continua, manejo de estándares en calidad, responsabilidad social, conciencia medioambiental y la gestión procesos serán requisitos básicos en la formación y práctica profesional del siglo. Por lo que nuestro reto es trasladar la experiencia al servicio de equipos de trabajo y estudiantes.

Datos académicos

Grado	Título	Centro de Estudios
MAGISTER	MAGISTER EN ADMINISTRACION ESTRATEGICA DE EMPRESAS	PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU
LICENCIADO / TÍTULO	LICENCIADO EN EDUCACION, ESPECIALIDAD: MATEMATICA Y COMPUTACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN EDUCACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAESTRO EN CIENCIAS DE LA EDUCACION , ESPECIALIDAD: CON MENCION EN INVESTIGACION Y DOCENCIA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
LICENCIADO / TÍTULO	INGENIERO DE SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
LICENCIADO / TÍTULO	LICENCIADO EN ADMINISTRACIÓN	UNIVERSIDAD SEÑOR DE SIPÁN
BACHILLER	BACHILLER EN INGENIERIA DE SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN
BACHILLER	BACHILLER EN ADMINISTRACIÓN	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD SENOR DE SIPAN SAC	DIRECTOR DEL CENTRO DE INFORMÁTICA Y SISTEMAS	2013-12-01	A la actualidad
SOLTI SOCIEDAD ANÓNIMA CERRADA	GERENTE	2012-12-01	A la actualidad

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD CESAR VALLEJO S.A.C.	Contratado	Marzo 2016	A la actualidad
UNIVERSIDAD SENOR DE SIPAN SAC	Contratado	Marzo 2008	Mayo 2016

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ARTEAGA MONTALVO KARLA YAMILI	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ASTOLINGON NUÑEZ ARELY ESTER	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CHAMBERGO ANACLETO DAVID	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CHANAME MORI OLGA LUISA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	CRIOLLO LLACSAHUANGA LIZETH	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	FERNANDEZ PINEDO ELIZABETH	Noviembre 2016

UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	GUZMAN LLUEN JHOANNA LORENA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	HUILCA MORI KATHERINE MICHELLE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	JAVA DURAN LUZ AURORA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	JIMENEZ RIVERA MILAGROS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	MEREGILDO SALVADOR CINTHIA MABEL	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	MUÑOZ MARTINEZ JOAO JOSIMAR	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	NAVARRO HEREDIA GIAN CARLOS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	PEREZ RUIZ RAQUEL JACQUELINE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	RODRIGUEZ FLORES ANTHONY GIAMPIERRE	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ROJAS DURAN VIOLETA DEL ROCIO	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SALAZAR LLUEN IVONNE JHOSSELIN	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SANCHEZ MONTENEGRO MILAGROS	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	SEGURA GOMEZ SONIA AZUCENA	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	VASQUEZ SALDAÑA QUIN ROY JEFERSSON	Noviembre 2016

UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	VERA CAVA OSMAR ALEJANDRO	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	YAIPEN MIMBELA JONATHAN JAVIER	Noviembre 2016
UNIVERSIDAD CESAR VALLEJO S.A.C.	Bachiller	ZAVALA SIALER YASMIN STHEFANY	Noviembre 2016
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	HURTADO CHERO ARTURO JESÚS	Noviembre 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	SAAVEDRA CARBAJAL JUAN CARLOS	Enero 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ZEVALLOS LLONTOP VICTOR ENRIQUE	Mayo 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	SALAZAR GUEVARA LENIN JESUS	Abril 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ALFARO ESQUIVEL LUZ MARIA	Abril 2015
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	ESPINOZA PASTOR CESAR RAYMUNDO	Diciembre 2011

PERFIL DE EXPERTO

Celi Arévalo Ernesto Karlo

Ingeniero de Computación y Sistemas, Maestro en Ciencias con mención en Informática y Sistemas, Doctor en Administración. Experiencia profesional desarrollada en entidades del sector educativo, municipal, hospitalario y financiero, en áreas y procesos de tecnología de información, gestión operativa/administrativa, gestión de riesgos de TI, seguridad de TI, auditoría informática; realizando trabajos de planeamiento, análisis y diseño, desarrollo, implantación, soporte y administración de sistemas de información, gestión de bases de datos, gestión de proyectos informáticos, capacitación y consultoría, elaboración de expedientes técnicos, auditorías informáticas y peritajes judiciales y extrajudiciales. Trabajos profesionales e investigaciones sobre gestión de riesgos de TI usando ISO 27005, MageriIT, Octave; seguridad de la información usando ISO 27001, ISO 27002; modelamiento de procesos y servicios de TI basados en COBIT 5.0, ITIL v3, ISO 12207, ISO 15504, las TIC en el proceso enseñanza aprendizaje y gestión hospitalaria con sistemas RIS/PACs.

Datos Académicos

Grado	Título	Centro de Estudios
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
BACHILLER	BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
DOCTORADO	DOCTOR EN ADMINISTRACION	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
MAGISTER	MAESTRO EN CIENCIAS, ESPECIALIDAD: INFORMATICA Y SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2016-01-01	A la actualidad
CAJA RURAL DE AHORRO Y CREDITO CRUZ DE CHALPON (HOY CAJA SIPAN)	AUDITOR EXTERNO DE TI	2002-10-01	2015-12-01
CONSORCIO ATA - KUKOVA	PROYECTISTA PRINCIPAL	2009-11-01	2011-08-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DECANO	2008-07-01	2011-07-01
CONSORCIO ATA - KUKOVA	PROYECTISTA PRINCIPAL	2009-12-01	2011-04-01
MUNICIPALIDAD PROVINCIAL CONDORCANQUI	LIDER DE PROYECTO	2006-06-01	2006-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2001-04-01	2006-09-01
MINISTERIO DE LA PRODUCCION	ANALISTA DE PROCESOS	2004-07-01	2005-07-01
PROYECTO ESPECIAL OLMOS TINAJONES	SUPERVISOR DE ELABORACION DE EXPEDIENTE TECNICO	2002-04-01	2002-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DE OFICINA CENTRAL	2001-05-01	2001-12-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD DE LAMBAYEQUE SAC	Contratado	Marzo 2012	Julio 2017
UNIVERSIDAD SEÑOR DE SIPAN SAC	Contratado	Setiembre 2011	Diciembre 2011

UNIVERSIDAD SEÑOR DE SIPAN SAC	Contratado	Abril 2002	Diciembre 2004
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Principal	Octubre 1994	A la actualidad

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Alarcón Cubas, Flor de Avelita y Orjeda Ramírez, Juan Alberto	Enero 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arenas Villanueva, César Augusto Junior y De Los Santos Mendoza, Diana	Diciembre 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Carrasco Vilchez, Jemmy William y Cubas Villegas, Eric Fernando	Mayo 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Muñoz Delgado, Jimmy Andrés y Mocarro Trigozo, Luis Eduardo	Diciembre 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Damian Acosta, Edinson Juan y Tapia Gastelo, Robint Fernando	Enero 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Puyén Santos, Vicente Raúl y Rivas Palacios, Betty Guiliana	Febrero 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Fernández Castillo, César Augusto	Enero 2019
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Livaque Delgado, Ketty Adalí y Bernilla Mio, Erick Jean Pierre	Agosto 2018

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Salinas Farro, Maura Angélica	Abril 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ortiz Góñaz, Neill Tito	Abril 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Santa Cruz Acosta, Roberto Carlos	Mayo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Oblitas Vera, Lily	Enero 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Mija Camargo, Luis Alberto	Marzo 2018