Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

"Modelo de Gestión de Riesgos de TI que dan soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE S.A.C. basada en la metodología MAGERIT"

PARA OPTAR EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

PRESENTADO POR
Soledad Milagros Dávila Puicón

ASESORADO POR
Dr. Ernesto Karlo Celi Arévalo

LAMBAYEQUE – PERÚ
2022

Universidad Nacional Pedro Ruiz Gallo
Facultad de Ingeniería Civil, de Sistemas y Arquitectura
Escuela Profesional de Ingeniería de Sistemas

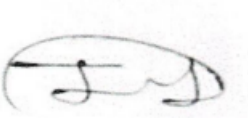
TESIS

"Modelo de Gestión de Riesgos de TI que dan soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE S.A.C. basada en la metodología MAGERIT"

PARA OPTAR EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

APROBADO POR:

Mg. Ing. Roberto Carlos Arteaga Lora	Presidente	
Mg. Ing. Juan Elias Villegas Cubas	Secretario	
Mg. Ing. Sheyla Vannina Miluska Pérez Riojas	Vocal	
Dr. Ing Ernesto Karlo Celi Arévalo	Asesor	

LAMBAYEQUE – PERÚ
2022

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
DECANATO

ACTA DE SUSTENTACIÓN VIRTUAL N° 012-2022-FICSA-D

Siendo las **10:00 am** horas del día 04 de mayo **del 2022**, se reunieron vía plataforma virtual, https://meet.google.com/pkm-uure-krk?pli=1 los miembros de jurado de la tesis titulada: **"MODELO DE GESTIÓN DE RIESGOS DE TI QUE DAN SOPORTE A LOS PROCESOS DE EVALUACIÓN, FINANCIAMIENTO Y COBRANZA DE LA EMPRESA CHANCAFE NORTE S.A.C. BASADA EN LA METODOLOGÍA MAGERIT", con código IS-2019-054,** designados por Decreto Directoral N° **252-2019-UNPRG-FICSA-UI** con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

MG. ING. ROBERTO CARLOS ARTEAGA LORA	PRESIDENTE
MG. ING. JUAN ELÍAS VILLEGAS CUBAS	SECRETARIO
MG. ING. SHEYLA VANNINA MILUSKA PÉREZ RIOJAS	VOCAL

Asesorado por el **DR. ING. ERNESTO KARLO CELI AREVALO**

El acto de sustentación fue autorizado por **OFICIO VIRTUAL No 032-2022-UIFICSA**, la tesis fue presentada y sustentada por el Bachiller: **SOLEDAD MILAGROS DÁVILA PUICÓN**, tuvo una duración de 30 **minutos**. Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

SOLEDAD MILAGROS DÁVILA PUICÓN	**18**	**DIECIOCHO**	**MUY BUENO**

Por lo que queda APTO para obtener el Título Profesional de **INGENIERA DE SISTEMAS** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las **11:50 horas**; se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

MG. ING. ROBERTO CARLOS ARTEAGA LORA
PRESIDENTE

MG. ING. JUAN ELIAS VILLEGAS CUBAS
SECRETARIO

MG. ING. SHEYLA VANNINA MILUSKA PÉREZ RIOJAS
VOCAL

DR. ING. ERNESTO KARLO CELI AREVALO
ASESOR

FACULTAD DE INGENIERIA CIVIL, SISTEMAS Y ARQUITECTURA
DECANATO

DR. ING. SERGIO BRAVO IDROGO
DECANO

REGISTRO VIRTUAL SUSTENTACIONES INGENIERIA DE SISTEMAS
IS_L001_F012

AGRADECIMIENTO

Agradecer a Dios por la vida, la salud, por permitir realizar este proyecto; por darme la fortaleza en cada momento difícil atravesado en mi vida.

A mis padres Luis y María por ser el ejemplo de perseverancia, lucha, dedicación. por sus consejos y valores inculcados.

A mi hermana Eveling por ser la mejor compañera, por sus consejos y compañía en el proceso.

A mi abuela Lucila por las risas y acompañamiento de madrugada durante mi época universitaria.

Al Dr. Ernesto Karlo Celi Arévalo por compartir sus conocimientos, amplia experiencia en el área para plasmarla en cada clase universitaria en aula; y por la asesoría en cada reunión para realizar este proyecto.

A la empresa CHANCAFE NORTE SAC por permitirme realizar el proyecto de investigación en sus instalaciones y por proporcionarme las facilidades para la misma.

DEDICATORIA

Dedico el proyecto a Dios por permitirme cumplir una de las metas más importantes en la vida.

A mi madre y hermana por sus ánimos, apoyo moral y consejos para poder culminar esta etapa.

A mi padre porque a pesar que una pandemia puede apagar un cuerpo nunca podrá con tu recuerdo; esto es por el amor tuyo que me acompaña todos los días; ha sido un orgullo ser tu hija.

A mi abuela, por tu gran compañía llena de amor, fortaleza y bondad; ha sido un orgullo ser tu nieta.

INDICE GENERAL

INDICE DE TABLA

INDICE DE GRÁFICOS

RESUMEN

Conforme la tecnología se impone como soporte a los procesos críticos, las organizaciones enfocan sus esfuerzos en proteger los activos que generen valor para el negocio por medio de controles con la finalidad de garantizar la seguridad de cada uno de ellos; siendo la información su principal activo.

CHANCAFE NORTE SAC es una empresa dedicada a la venta al crédito y contado principalmente de electrodomésticos. Los procesos críticos que soportan dicha actividad son los de evaluación, financiamiento y cobranza; en donde los activos en que se soportan dichos procesos se encuentran expuestos a riesgos accidentales, internos y externos; lo cual genera interrupciones en los mismos, perdida de información, e incluso daños económicos; todo ello afecta la imagen de la institución.

Existen métodos, estándares y modelos de referencia para el análisis y gestión de riesgo, pero el hecho de conocerlos no asegura que el proceso se lleve a cargo de forma exitosa. Es por ello que se ha diseñado y propuesto un modelo de gestión de riesgos tomando como referencia los estándares ISO/IEC (31001, 27001, 27002 y 27005) y basado en la metodología MAGERIT que en forma eficaz y eficiente aplique los marcos de referencia de manera exitosa en la labor de análisis de riesgos de tecnologías de información (TI).
El modelo desarrollado en la investigación es descriptivo propositivo no experimental porque se describirán los componentes que conforman el modelo, los procedimientos de las actividades, tareas y forma de cálculos; por lo que no se pretende modificar la realidad actual de la empresa, ya que no se va a implementar, sino que sólo se propone.

Finalmente, esta investigación evidencia como resultado que el modelo propuesto es aceptable acorde a las etapas de identificación del riesgo, análisis y evaluación del riesgo y tratamiento del riesgo bajo los criterios de suficiencia, claridad, coherencia y relevancia.

.

PALABRAS CLAVES

Gestión de riesgo de TI, activos, amenazas, salvaguardas, estado del riesgo.

ABSTRACT

As technology prevails as support for critical processes, organizations focus their efforts on protecting assets that generate value for the business through controls in order to guarantee the security of each one of them; being the information its main asset.

CHANCAFE NORTE SAC is a company dedicated to credit and cash sales mainly of household appliances. The critical processes that support this activity are those of evaluation, financing and collection; where the assets on which said processes are supported are exposed to accidental, internal and external risks; which generates interruptions in them, loss of information, and even economic damages; all this affects the image of the institution.

There are methods, standards and reference models for risk analysis and management, but knowing them does not ensure that the process is carried out successfully. For this reason, a risk management model has been designed and proposed, taking the ISO/IEC standards (31001, 27001, 27002 and 27005) as a reference and based on the MAGERIT methodology that effectively and efficiently applies the reference frameworks of successfully in the work of information technology (IT) risk analysis.

The model developed in the research is descriptive non-experimental propositional because the components that make up the model, the procedures of the activities, tasks and form of calculations will be described; Therefore, it is not intended to modify the current reality of the company, it is no longer going to be implemented, but is only proposed.

Finally, this research shows as a result that the proposed model is acceptable according to the stages of risk identification, risk analysis and evaluation, and risk treatment under the criteria of sufficiency, clarity, coherence, and relevance.

KEYWORDS:

IT risk management, assets, threats, safeguards, risk status.

INTRODUCCIÓN

La importancia de gestionar adecuadamente los riesgos de TI en las organizaciones permite proteger los activos en el cual se soportan los procesos críticos o que generan valor para el negocio.

La empresa CHANCAFE NORTE SAC atraviesa por problemas en la seguridad de la información debido a que no gestiona los riesgos de tecnologías de información, por lo que diseñar un modelo adaptado a su realidad para contrarrestar los riesgos a los que los activos de sus procesos críticos están expuestos y que permita la continuidad del negocio.

Este proyecto propone un modelo para la gestión de riesgo de tecnologías de información (TI) acorde o adaptado a la realidad de la empresa CHANCAFE NORTE SAC. Incluye las fases, actividades, procedimientos y la forma de cómo desarrollarlo o calcularlo; para determinar el riesgo intrínseco todo ello para proponer mecanismos de control o salvaguardas para finalmente determinar el nivel de riesgo residual.

En el capítulo I, se detalla el planteamiento del proyecto de investigación; contempla la descripción del problema que atraviesa la empresa CHANCAFE NORTE SAC por la no gestión de los riesgos de TI. También plantea los objetivos específicos y el objetivo general que es desarrollar un modelo de gestión de riesgos de TI como soporte de la seguridad de TI de los procesos de evaluación, financiamiento y cobranza en la empresa CHANCAFE NORTE S.A.C.

En el capítulo II, contiene la base teórica, definiciones de términos técnicos, marcos de referencia, estándares internacionales, entre otros; todos relacionados a la seguridad de TI, con la finalidad de sustentar el modelo de gestión de riesgos propuesto.

En el capítulo III, se describen los métodos de recolección de datos utilizados en esta investigación, así como también la descripción paso a paso del modelo propuesto acorde con el objetivo general.

En capítulo IV, se muestran los resultados obtenidos por cada etapa que fue detallada en el capítulo anterior, en base a su desarrollo.

Se analizó los procesos críticos en el cual, por medio de un Análisis de Impacto de Negocio, se obtienen la lista de los activos críticos, posteriormente se clasificaron y priorizaron en relación a su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Se identificaron las amenazas por activo y vulnerabilidades para luego valorar el impacto y probabilidad de ocurrencia de cada una de ellas; posterior a ello se calculó el nivel de riesgo intrínseco en concordancia al apetito y tolerancia al riesgo definido por la empresa.

Acorde al nivel de riesgo se identificaron los controles o salvaguardas pertinentes, se evaluó según los criterios definidos en el capítulo anterior para obtener la efectividad de los controles.

Se determinó el nivel de riesgo residual al que están subyugado los activos tomando el valor de los activos y la valorización de las amenazas y el grado de efectividad de las salvaguardas desplegadas

En capítulo V se realizó la discusión de resultados obtenidos en esta investigación.

I. EL PROBLEMA DE LA INVESTIGACIÓN

1.1. Descripción del Problema

Las empresas en general y con el avance de nuevas tecnologías, optan por implementar proyectos basados en éstas para dar soporte a sus procesos, para generar valor y ser más competitivas.

La tecnología a pesar de ser facilitadora presenta a la vez riesgo potencialmente de alto impacto como lo es el riesgo cibernético en forma de robo de cuentas, datos, destrucción de archivos, deshabilitación o degradación de sistemas que se han posicionado en lo más alto en el pensamiento. Aunque, existen más riesgos de Tecnologías de Información (TI) el cual debe generar preocupación en la primera línea en la organización. (Deloitte, 2016)

Las organizaciones son cada vez más conscientes del impacto que las amenazas de TI pueden tener sobre ellas. Las empresas de cada sector económico a menudo informan que debido a errores sufren pérdidas, ataques a los servicios referente a TI, lo que afecta gravemente su imagen, así como su estabilidad económica y sus actividades. Por un lado, para desarrollar un análisis de riesgos existen estándares y normas; y metodologías por el otro lado; ambos no garantizan el éxito si no se aplican de manera adecuada. (Gomez, Pérez, Donoso y Herrera, 2010)

Actualmente existen muchas metodologías y marcos teóricos como referencia en la gestión de riesgos, como lo es: MAGERIT, ISO/IEC 31000, ISO/IEC 27005 así como otros marcos que abordan propuestas relacionadas como: COSO II, ITIL, COBIT, ISO/IEC 27001 y 27002, etc., las mismas que se han impuesto como referencias de facto y que dominan en nuestro medio. Sin embargo, éstas son aplicables a realidades distintas a la nuestra, lo cual genera la necesidad de desarrollar propuestas que se ajusten a los tipos de empresas que existen en nuestro medio.

CHANCAFE NORTE SAC se dedica como empresa a la venta de electrodomésticos, equipos de cómputo, motos y muebles importados o nacionales, su sucursal administrativa se ubica en la ciudad de Chiclayo y cuenta con 24 tiendas a nivel nacional en el norte y oriente del Perú.

Su actividad principal radica en la venta al contado y crédito directo. Los procesos administrativos vienen desarrollándose desde el 2009 en su principal sucursal en la ciudad de Chiclayo. Los procesos de evaluación, financiamiento y cobranza que involucra la venta al crédito son los más críticos no solo por la rentabilidad que genera sino porque a partir de la información que generan dichos procesos, se toman decisiones.

A diario la organización se encuentra expuesta por riesgos accidentales, internos y externos que vulneran la integridad de la información perjudicando los procesos del negocio y a la imagen institucional. Es ahí donde la confianza se convierte en un valor crítico para la prestación de servicios. Se evidencia lo siguiente:

- La organización cuenta con el Área de Tecnologías de Información desempeñando funciones como administración de bases de datos, desarrollo de software, soporte técnico de red, entre otras propias del área. No existe orgánicamente la Unidad de Riesgos; por ende, no cuenta con un proceso de

evaluación y tratamiento que analice los activos de TI críticos y la información que debe ser protegida; y que generan valor para el negocio.

- La empresa evidencia la poca inversión en seguridad de la información y no cuenta con un plan de continuidad de negocio, mostrándose el temor latente por el impacto negativo de cada incidencia ocurrida.
- Los activos de TI no se han definido ni priorizado de acuerdo a la criticidad que éstos tienen con los procesos. No se registran los problemas e incidentes ocurridos referentes a la seguridad de la información, siendo sólo identificados por la recurrencia de los mismos y por ende no todos tomados en cuenta cuando se trata de buscar mejoras en el área.
- La información no se encuentra clasificada ni priorizada el cual no determina los niveles de acceso a los usuarios formalmente y solo se asignan a solicitud de gerencia, pero estos no se registran ni se controlan, teniendo estos a disposición toda la información de la empresa incumpliendo los principios de seguridad de TI.
- La rotación del personal en la empresa afecta al desarrollo del proceso debido al tiempo en el proceso de adaptación de cada personal, además de tener el riesgo latente de que cada trabajador que ha renunciado o despedido el empleador, tome acciones perjudiciales contra la organización utilizando la información de la empresa proporcionada durante su permanencia laboral.

A causa de dichos problemas en la empresa se suscitan interrupciones en sus procesos críticos, pérdida de información y daños económicos frecuentemente; además de tener el temor latente de pérdidas a mayor escala.

Entender los marcos de referencia para el análisis y gestión de riesgos no garantiza su culminación exitosa. Por lo tanto, se debe diseñar y proponer un modelo de gestión de riesgos que de manera efectiva y eficiente aplique dichos marcos en el análisis de riesgos de TI.

De acuerdo a lo descrito es necesario desarrollar un modelo para la gestión de riesgos de TI para el soporte de la seguridad de la información en base a los procesos de evaluación, financiamiento y cobranza en la empresa CHANCAFE NORTE S.A.C.

1.2. Formulación del problema

En consecuencia, el problema central de la investigación es:

¿De qué manera el modelo propuesto para la gestión de riesgos de TI basada en la metodología MAGERIT ayuda a dar soporte a la seguridad de la información de los procesos críticos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE SAC?

1.3. Objetivos de la investigación

1.3.1 Objetivo general

Desarrollar un modelo de gestión de riesgos de TI como soporte de la seguridad de la información de los procesos de evaluación, financiamiento y cobranza en la empresa CHANCAFE NORTE S.A.C.

1.3.2 Objetivos específicos

Se consideran los siguientes:

1. Realizar un análisis de los procesos de evaluación, financiamiento y cobranza para identificar los activos de TI críticos y la información que debe ser protegida y que generan valor para el negocio. A través de un análisis de impacto de negocio (BIA).
2. Clasificar y priorizar los activos de acuerdo con su criticidad en la dependencia con la generación de valor para el negocio.
3. Identificar y valorar los escenarios de riesgo para cada activo de TI a través de un análisis de amenazas, impactos y probabilidad de ocurrencia.
4. Determinar los niveles de exposición al riesgo de TI de acuerdo con el apetito y la tolerancia al riesgo determinado por la institución para cada proceso.
5. Desarrollar una estrategia de tratamiento de los riesgos a través de controles, salvaguardas o mecanismos de seguridad.

1.4. Justificación de la investigación

En el ámbito tecnológico, por lo que en base a la gestión de riesgos de TI/SI de MAGERIT, se ha logrado proponer un modelo aplicable a la gestión de riesgos de TI que involucra la evaluación y tratamiento de los mismos, ceñido a la particularidad de la empresa y sobre todo adaptable a la misma, con el propósito de garantizar continuidad de los procesos del negocio y disminuir los daños en la empresa CHANCAFE NORTE SAC.

En el ámbito social, por lo que la propuesta del modelo describe, por medio de un conjunto de procedimientos y actividades, la administración de los incidentes de la seguridad para reducir los daños en los procesos críticos, las caídas de los activos tecnológicos que los soportan, y que genera degrada la imagen de la organización.

En el ámbito económico, esta investigación no solo se enfoca en los avances sobre el uso de metodologías para disipar las consecuencias de los muchos problemas o necesidades que puedan encontrarse en la gestión de seguridad de TI, la gestión en la continuidad de los procesos del negocio y la de los riesgos operativos de TI, sino que además, este brinda la información para que la directiva pueda usarlo en toma de decisiones acertadas para implementar controles como mecanismo de seguridad de sus activos tecnológicos, de esta forma poder reducir gastos innecesarios en controles que no sean efectivos o en mecanismos de seguridad que luego no puedan monitorear ;por medio de ello se puede acrecentar los beneficios de la inversión en tecnología.

En el ámbito científico, este proyecto ha realizado una propuesta de metodología como aporte a lo científico para demostrar que, por medio de la propuesta de un modelo basado en metodologías y estándares internacionales, puede mejorar eficazmente la gestión de los riesgos referente a TI/SI de una empresa.

El proyecto también servirá de referencia y guía para la realización de posteriores investigaciones que tengan como finalidad la automatización de la Gestión de Riesgos referente a la Seguridad de la Información.

II. MARCO TEÓRICO

2.1 Bases Teóricas

2.1.1 Riesgo de TI

La RAE[1] se refiere al riesgo como la contingencia o la proximidad de un perjuicio o daño.

La ISO 31000 (2009) ,el riesgo es la consecuencia de las dudas sobre el cumplimiento de nuestros objetivos. Necesitamos comprender que la consecuencia es algo que se desvía de las expectativas, tanto positiva como negativamente. El riesgo a menudo se expresa como una combinación del impacto de un evento, así como la probabilidad de ocurrencia. Por la incertidumbre se refiere a la falta de información respecto al entendimiento de un evento, sus efectos o probabilidad.

La ISO/IEC 27005:2008 que se utiliza como guía para gestionar los riesgos de TI, se refiere que dicho riesgo es el potencial que tiene una o las amenazas para explotar cada vulnerabilidad de uno o grupos de activos causando perjuicio. (Alvarez Sosa, 2013).

MAGERIT se refiere al riesgo como la estimación de la exposición que un activo o un grupo de ellos tiene referente a la materialización de una amenaza que causa daños a la entidad u organización.

2.1.2 Análisis y gestión de riesgo de TI

El análisis y gestión de riesgos tecnológicos incluye determinar el nivel de seguridad requerida por la organización para la información, proporcionando a la alta dirección elementos claros para aprobar planes, recursos e incluso políticas con el fin de lograr un nivel de riesgo tolerable dentro de la organización (Vásquez, 2013).

MAGERIT lo define como un proceso que estima el impacto de los riesgos a los que una organización está expuesta. (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

El análisis posibilita determinar cómo se ve, el valor que tiene y la forma en que se protege el sistema. De acuerdo con el propósito y las políticas de cada entidad, la actividad de gestión de riesgos hace posible el desarrollo, la ejecución y el mantenimiento de un programa de seguridad para lograr sus objetivos y riesgos aprobado por la directiva. Proceso de Gestión de Riesgos es como se conocen a todas estas actividades. (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012).

El análisis está incluido en la planificación de las actividades de toma de decisiones sobre el tratamiento. Las decisiones se formalizan durante la fase de implementación, donde se pueden desplegar convenientemente los elementos que monitorean las medidas que fueron tomadas para que se pueda evaluar su efectividad y las acciones tomadas se lleven a cabo en un período regular,

[1] Real Academia Española de la lengua.

excelente o de mejora continua (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012).

En MAGERIT (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012) el método de análisis de riesgos considera estas definiciones:

- **Activos:** es la funcionalidad o el componente de un sistema de información que es vulnerable a ataques intencionales o no intencionales con efectos para la entidad. Incluye: equipos (hardware), aplicaciones (software), información, servicios, datos, recursos físicos, comunicaciones, recursos humanos y también administrativos.
- **Amenazas:** motivo potencial de evento que puede generar perjuicio a una organización o a un sistema de información.
- **Vulnerabilidades:** en detalle se les denomina así a las debilidades de los activos o de sus salvaguardas que favorece la materialización de una o más amenazas.
- **Impacto:** efecto sobre un activo cuando se concreta una amenaza.
- **Probabilidad:** la cuantificación y/o cualificación de las veces que la amenaza puede concretarse.

2.1.3 ISO/IEC 31000

La ISO/IEC 31000; tiene como objetivo disminuir, gestionar y controlar todo riesgo (todo tipo) que dificulte la consecución de los objetivos y que además se pueda usar en cualquier tipo de organización, porque proporciona guía exhaustivos y principios para ayudar a las organizaciones o entidades en la gestión de sus riesgos.

La ISO/IEC 31000:2009, propone los principios a ser cumplidos para gestionar el riesgo eficazmente. Sugiere además que en las organizaciones o empresas realicen, pongan en marcha y continúen mejorando un marco o una estructura como soporte con el propósito de incorporar el proceso de gestión de riesgos en la corporación y demás ámbitos. (Castro, 2010).

En la versión ISO/IEC 31000:2018 se enfoca, en la atención de gestión del riesgo, y que lo toma como medio para disminuir, de manera prevista, las incertidumbres que posiblemente pudieran suscitarse. (Bureau Veritas España, 2018).

Una exitosa gestión del riesgo, según la UNE ISO 31000[2] (2018) está conformado:

[2] Realizada por el comité técnico CTN 307 *Gestión de riesgos*, su secretaría desempeña UNE; Ésta es idéntica a la norma internacional ISO 31000:2018

1. **Principios de la gestión del riesgo.**
   Los principios establecidos se muestran en la siguiente figura:

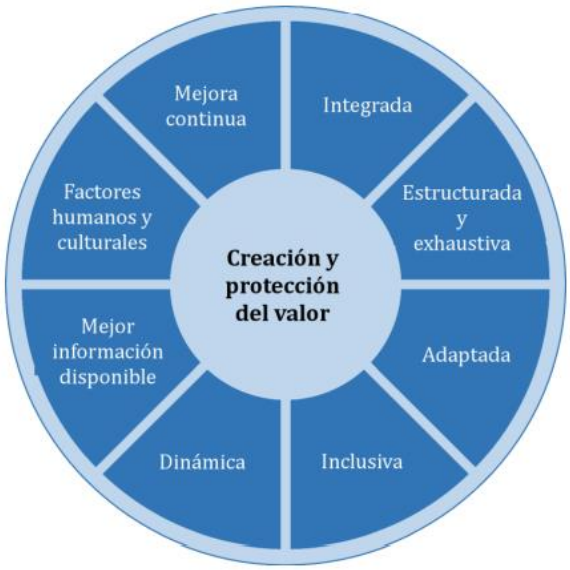


Gráfico N° 1: La gestión del riesgo en base a sus principios.

Fuente: (ISO/IEC 31000:2018)

i. **Integrada:** la gestión de los riesgos es el punto más importante de todas las actividades de la organización.
ii. **Estructurado:** Enfocado en la gestión referente al riesgo para contribuir a que los resultados sean comparables y claros.
iii. **Adaptada:** la gestión del riesgo y sus procesos se adaptan y corresponden al contexto ya sea interno o de manera externa de la entidad en relación a sus objetivos y propósitos.
iv. **Inclusiva:** La intervención oportuna de todas las partes que tienen interés.
v. **Dinámica:** Los riesgos pueden originarse, modificarse o extinguirse conforme lo hace el entorno dentro y fuera de la entidad.
vi. **Información disponible:** La información de ingreso a la gestión del riesgo es histórica y actual; así como futuras.
vii. **Factores humanos y culturales:** influyen fuertemente en cada fase de la gestión del riesgo.
viii. **Mejora continua:** gracias al aprendizaje y la experiencia.

2. **El marco de trabajo.**
   Se visualiza en el siguiente gráfico:

Gráfico N° 2: Marco de trabajo para la gestión del riesgo

Fuente: (ISO/IEC 31000:2018)

a. **Liderazgo y compromiso:** La directiva, cuando sea necesario, debería demostrar el liderazgo y compromiso donde sobre todo se adapten e implementen todos los elementos del marco de referencia y aseguren que los recursos sean asignados.
b. **Integración:** va a depender de la compresión de las estructuras y el entorno de la entidad, donde el riesgo se gestiona en todas las partes de dicha estructura y todos los miembros tiene la responsabilidad de gestionarlo.
c. **Diseño:** Al ser diseñado un marco referente a la gestión de riesgos, deben como organización analizar y comprender su entorno externo e interno.
d. **Implementación:** La organización lo hace mediante un plan apropiado con cronogramas y recursos; determinando dónde (el lugar), cuándo (el tiempo), cómo (la forma) y quién toma las decisiones; el cambio de los procesos aplicables para la misma; y la garantía de que las medidas tomadas para la gestión del riesgo por la organización son claramente comprendidas.
e. **Valoración:** Medir cada cierto tiempo el marco referencial de la gestión del riesgo conforme a su objetivo; y determinar si es el adecuado.
f. **Mejora:** La organización debe hacer seguimiento continuo e ir adaptando el marco referencial de gestión del riesgo conforme a los cambios internos y externos.

3. **El proceso de gestión del riesgo.**
   El proceso se ilustra de la siguiente manera:

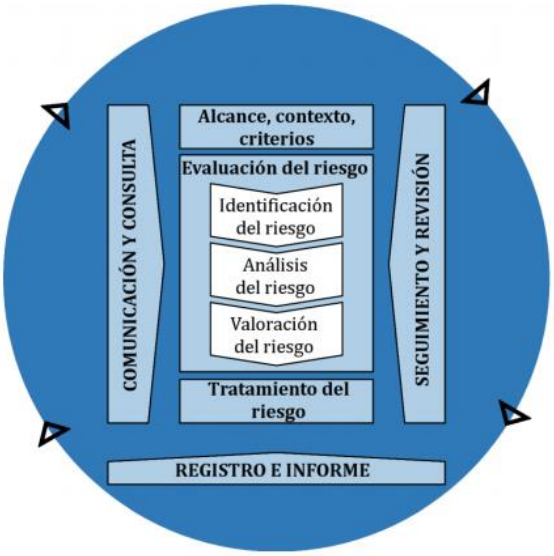


Gráfico N° 3: Gestión del riesgo en base a su proceso.

Fuente: (ISO/IEC 31000:2018)

a. **Comunicación y consulta:** con la finalidad de ayudar a comprender el riesgo, cómo se toman decisiones y la razón por la que es necesario tomar acciones.
b. **Alcance, contexto y criterios:** permite un tratamiento del riesgo apropiado para el mismo, por medio de la adaptación del proceso.
c. **Evaluación:**

   i. **Identificación del riesgo:** aquí se puede identificar y detallar los riesgos que ayudan o impiden a la organización cumplir con sus objetivos.
   ii. **Análisis de riesgo:** Con niveles a detalle de forma compleja. Se realiza dependiendo del motivo, la disposición con que cuenta y la confidencialidad de la información además de los medios a disposición.
   iii. Valoración del riesgo: involucra que debe hacerse una comparación del resultado de los análisis del riesgo según los criterios preestablecidos del mismo para determinar cuándo se necesita tomar nuevas acciones.

d. **Tratamiento del riesgo:** debe estar integrado en procesos de la entidad, en consulta con las partes interesadas con el propósito de realizar la elección e implementación de opciones con la finalidad de que el riesgo pueda ser abordado.
e. **Seguimiento y revisión:** Se aseguran y mejoran el desempeño del diseño, la puesta en marcha y los resultados.
f. **Registro e informe:** Se documentan e informan los resultados del proceso por medios apropiados.

2.1.4 ISO/IEC 27001 – Sistema de Gestión de la Seguridad de la Información

Esta ISO incluye pautas para el desarrollo y la operatividad de un Sistema de Gestión de Seguridad de la Información (SGSI), despliega una lista de mecanismos de control para gestionar la mitigación de los riesgos sobre los activos. Referente a la efectividad de la implementación del SGSI se puede confirmar por medio de una auditoría. (Aguirre Mollehuanca , 2014)

Esta ISO brinda pautas para la implementación, desarrollo, monitoreo, revisión, mantenimiento y control para mejora de un Sistema de Gestión de Seguridad de Información en la organización. (ISO/IEC 27001:2005, 2005)

En su versión del 2013 especifica los requisitos para la colocación, implementación, mantenimiento y control continuo de mejora de un SGSI. Estos requisitos describen el desenvolvimiento esperado cuando el SGSI está en pleno funcionamiento. No es la naturaleza de este estándar ser guía o directriz para estructurar o desarrollar un SGSI.

2.1.5 ISO/IEC 27002 - Código de prácticas para los controles de seguridad de la información

Es guía para las normas de la organización referente a la seguridad de TI; además de buenas prácticas de gestión de seguridad de la información. Esto incluye selección, puesta en marcha o implementación y finalmente la gestión de salvaguardas o controles, considerando los riesgos de TI. (ISO/IEC 27001:2013, 2013).

En la versión del 2013 ha sido propuesta para ser utilizada en entidades u organizaciones que buscan: en primer lugar, seleccionar o elegir mecanismos de control en el proceso de implementación de un SGSI con base en la ISO/IEC 27001. Luego, poner en marcha o implementar los mecanismos de seguridad aceptados; finalmente, desarrollar guías referentes a la gestión de seguridad de la información en la organización. La ISO proporciona mecanismos que buscan minimizar el impacto de ocurrencia de los múltiples riesgos a los la entidad está expuesta. (ISO/IEC 27002:2013, 2013) .

2.1.6 ISO/IEC 27005

Es parte de la familia ISO 27000; complementa a las normas 27001 y 27002 ambas ISO/IEC. Esta norma responde al por qué de realizar un análisis de riesgos , esta norma no proporciona una guía para ello. (Crespo Rin, 2013)

La conforman 12 cláusulas y 6 anexos, los anexos sirven como soporte al desarrollo de cada cláusula. A partir de la cláusula 7 abarca la gestión de riesgos

N^{o} 7. Estable el contexto, define los objetivos, define su alcance y las políticas; y enfoque de la organización en todo el proceso.

Nº 8. Valoración del riesgo, identifica, estima, evalúa y analiza los riesgos.

Nº 9. Tratamiento del riesgo, propone el medio para el tratamiento de cada riesgo valorado.

Nº 10. Aceptación del riesgo, decide qué riesgos aceptar, y lo justifica. El riesgo residual se debe tratar.

Nº 11. Comunicación del riesgo, intercambiar información de los riesgos entre los interesados, se realizará a lo largo del proceso.

Nº 12. Monitoreo y Revisión, la actualización en el análisis de riesgos incluye cada cambio de manera interna o externa que vulneran a la estimación de cada riesgo. Se monitorea y evalúa constantemente.

Proceso para la gestión de riesgos en ISO 27005:

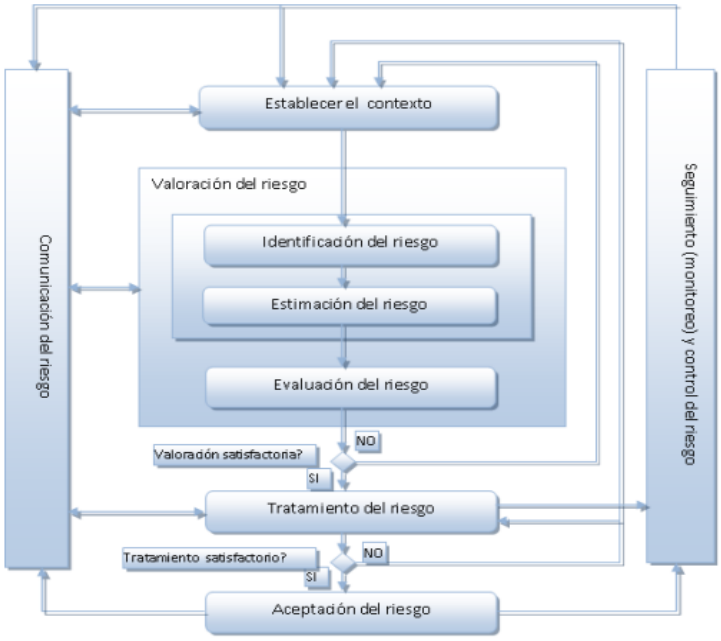


Gráfico N° 4: La gestión de riesgos en base a la ISO/IEC 27005

Fuente: (Crespo Rin, 2013)

El 10 de Julio de 2018, ISO publicó la nueva versión de la ISO/IEC 27005 el cual cobra particular importancia por ser una de las principales normas de apoyo a la de requisitos ISO/IEC 27001:2013 y que no había sido actualizada desde el 2011.Esta tercera edición se centra principalmente en eliminar las referencias que ya no son de utilidad y las modificaciones necesarias para que la redacción sea compatible con los requerimientos y fines de la ISO/IEC 27001:2013.

2.1.7 MAGERIT

Metodología de Análisis y Gestión de Riesgos de Tecnología de la información (MAGERIT) es un método , que tiene por misión identificar los riesgos a los que están expuestos los sistemas de información con la finalidad de proponer medidas apropiadas como mecanismos de seguridad o salvaguardas que deberían adoptarse para controlarlos (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

El CSAE[3] ha diseñado MAGERIT en consecuencia a la percepción sobre que la sociedad en conjunto cada vez depende más y más de los sistemas de información con la finalidad de alcanzar sus objetivos. Las tecnologías de la información y las comunicaciones (TIC) otorgan ventajas, aunque éstos conllevan algunos riesgos que para poder mantener a los usuarios en un nivel aceptable de confianza a los servicios; deben ser controlados. (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

De acuerdo a la ISO 31000, MAGERIT cumple con el Proceso de Gestión de Riesgos en el "Marco de Gestión de Riesgos". Esto quiere decir que MAGERIT desarrolla un Proceso de Gestión de Riesgos en un marco con la finalidad de que la directiva que toma las decisiones lo haga tomando en cuenta los riesgos que involucran el uso de las tecnologías de la información. (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

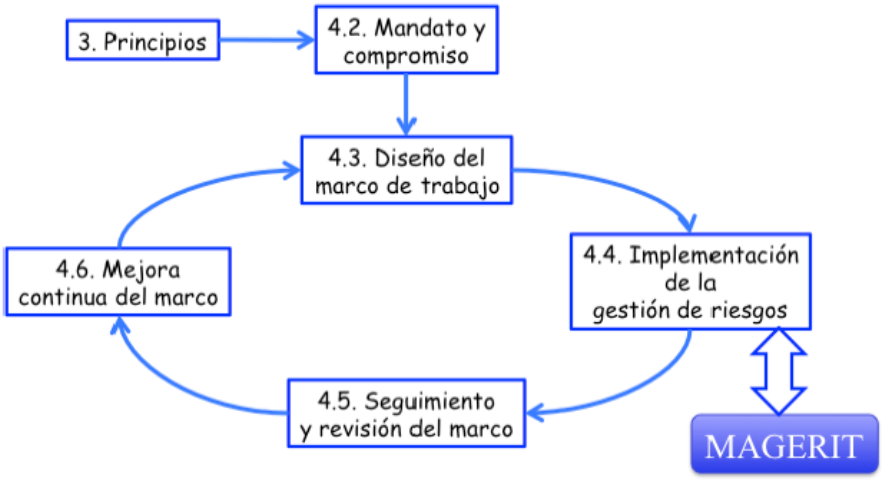


Gráfico N° 5: Gestión de riesgos según ISO 31000

Fuente:(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

Los objetivos de Magerit:

- Dar a conocer los riesgos y generar necesidad de gestionarlos.
- Ofrecer un método para el análisis de riesgos referente al riesgo de TI.
- Facilitar la planificación del control de los riesgos.
- Llevar a la organización a prepararse para procesos de certificación en riesgos.

Dimensiones según Magerit de la seguridad de la información:

- Disponibilidad de los servicios de ser usados cuando se requieran.
- Integridad o mantenimiento de la exactitud de cada dato.
- Confidencialidad ya que solo debe ser accesible a las personas autorizadas.

Además, añade otras dimensiones derivadas:

[3] CSAE: Consejo Superior de Administración Electrónica.

- Autenticidad: Propiedad en que una entidad es quien dice ser y/o que garantiza la fuente de donde procede cada dato.
- Trazabilidad: Consiste en que se podrá determinar quién hizo qué y cuándo lo hizo.

Análisis y tratamientos de los riesgos

Las actividades trabajan en conjunto en el proceso Gestión de Riesgos.

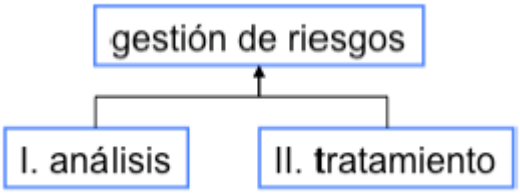


Gráfico N° 6: Actividades de la Gestión de Riesgos

Fuente: *(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)*

I. **análisis**, estimación del nivel de riesgo a la que está expuesto una organización o entidad. La actividad determina con lo que cuenta la organización para estimar lo que podría pasar.
Considera los elementos:
   a. **activos**, se refiere a los componentes que están estrechamente vinculados con el sistema de información y que son la piedra angular de los objetivos de la Organización.
   b. **Amenazas**, que es lo que le puede ocurrir a los activos y que causa daño a la Organización.
   c. **salvaguardas**, que no son más que los mecanismos de protección para evitar que se materialicen las amenazas.

A partir de estos se puede determinar:
   a. **el impacto**: lo que podría pasar
   b. **el riesgo**: lo que probablemente va a pasar

II. **tratamiento,** para preparar la defensa a conciencia y de manera limitada, con el propósito de evitar daños y a la vez estar entrenados para manejar escenarios fortuitos, permanecer exitosamente a los incidentes y continuar trabajando de manera óptima; haciendo que el riesgo sea aceptable para la organización.

A. Método de análisis de riesgos

Magerit (2012) indica los siguientes tareas:

1. determinar los activos organizacionales apropiados, sus interrelaciones y valores, es decir, qué daños (costos) resultará en su deterioro.
2. identificar las amenazas a estos activos.
3. determinar qué controles o salvaguardas se están utilizando y su eficacia.

4. estimar el impacto, entendido como la degradación a la propiedad por la realización de cualquier amenaza.
5. estimar o valorar el riesgo, que se define por el impacto y por la probabilidad de ocurrencia de la amenaza

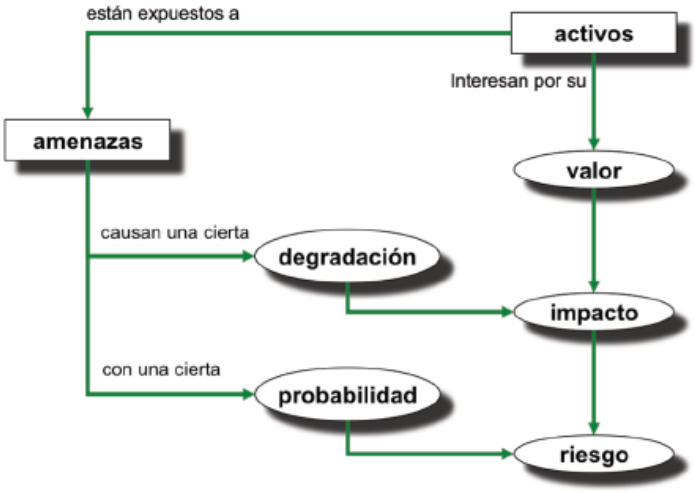


Gráfico N° 7: Elementos del análisis de riesgos potenciales

Fuente: *(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)*

El análisis de los riesgos comprende las siguientes tareas:

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Gráfico N° 8: Tareas del Método de Análisis de Riesgos.

Fuente*:* (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

MAR. 1: Activos

Su clasificación se da ya se por su tipo o su naturaleza en razón de su función. **(Ver anexo N° 03)**

Las dimensiones por las que son valoradas son los atributos que hacen valiosos a los activos o un activo.

Para valorar los activos es muy importante que:

- la escala sea común para todas las dimensiones, de esta forma permitirá comparar riesgos,
- la escala sea logarítmica y que se centre en las diferencias relativas de valor,
- el criterio usado sea homogéneo para permitir comparar análisis realizados de manera independiente.

MAR 2 Amenazas

Cuando se identifica a una amenaza, el siguiente paso es valorar su influencia en sobre el activo:

Degradación: cuanto se dañaría el valor del activo.

Probabilidad: la probabilidad de que se materialice.

MAR 3 Salvaguardas

Se refieren a los mecanismos referente a la tecnología que reducen el riesgo.

MAR 4 Estimación del estado del riesgo

Impacto residual

Como solo ha cambiado en magnitud de la degradación, se recalcula este nuevo nivel.

Riesgo residual

Se recalcula el riesgo utilizando el impacto, así como la probabilidad; ambas residuales.

B. Proceso de gestión de riesgos

Resaltan referente al presente proceso según Magerit Versión 3.0 (2012):

- **Evaluación:** estimación de los valores residuales de impacto y riesgo.
- **Aceptación del riesgo:** definir el nivel de impacto y riesgo tolerable.
- **Tratamiento:** el órgano directivo puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información.

2.1.8 El Apetito y Tolerancia al Riesgo

Se cuenta con las siguientes definiciones:

a. El apetito: el riesgo que la empresa está dispuesta a buscar o que acepta en relación con el logro de objetivos.

b. Tolerancia: el riesgo que la organización acepta pero que lo considera como el límite o máximo para lograr sus objetivos.

c. Capacidad: el riesgo el cual la organización es capaz de soportar referente al cumplimiento de sus objetivos.

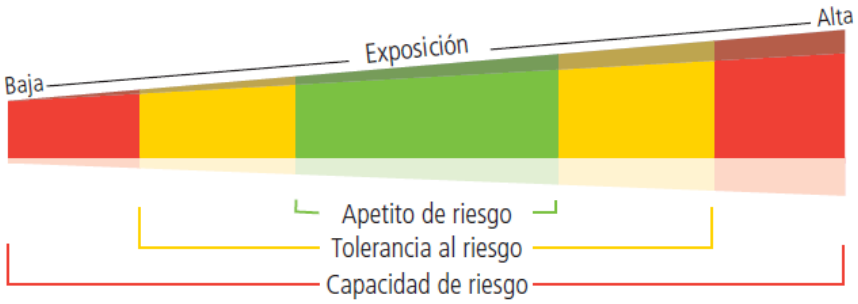


Gráfico N° 9: Apetito y la tolerancia al riesgo.

Fuente: (Instituto de Auditores Internos de España, 2012)

III. MARCO METODOLÓGICO

3.1 Tipo de investigación

El presente proyecto es de tipo descriptivo propositivo no experimental. El proyecto describe los procedimientos, actividades, tareas y formas de cálculo que están contemplados en el modelo de gestión de riesgos; la presente investigación no pretende modificar la realidad actual de la empresa, sino que solo lo presenta a nivel propositivo. No será experimental ya que no se implementará el modelo debido a que la empresa evaluará a un largo plazo la implementación del modelo propuesto.

3.2 Métodos y técnicas de recolección de datos

Se aplicará las siguientes técnicas de recopilación de la información y su correspondiente instrumento:

- **Documentación**, de existir se tomarán a revisión los documentos estratégicos, legales y administrativos de CHANCAFE NORTE SAC – Chiclayo relacionada a la materia del caso de estudio y se extraerá por medio de fichas la información relevante de cada uno de ellos.

- **Entrevistas**, servirán para recopilar información en relación a los procesos de estudio y su relación con los activos críticos de TI. Además, para recopilar información sobre los procesos críticos, el diagnóstico de las salvaguardas que ya existen. Según sea el caso, se entrevistará a:

    - Jefatura de TI
    - Asistente de TI

- **Encuestas**, usando la técnica Delphi (juicio de expertos), con el propósito de que profesionales expertos en el área puedan evaluar la efectividad del diseño del modelo propuesto. Los profesionales con experiencia que fueron seleccionados tienen la autoridad y capacidad de acuerdo a su experiencia laboral y preparación académica para evaluar la seguridad de TI.

3.3 Método de investigación

Para alcanzar el objetivo, se ha identificado y evaluado los elementos, que plantea MAGERIT (actividades y tareas) y normas internaciones como la familia ISO referente a la seguridad de TI y la gestión de riesgos; tal como: activos de TI, amenazas, vulnerabilidades, impacto y probabilidad de ocurrencia; para de esta forma determinar el nivel de riesgo intrínseco y el nivel de riesgo residual.

El modelo propuesto está formado por 4 etapas tomado de la estructura de MAGERIT:

a) Caracterización de los activos: donde a través del análisis de los procesos se determinan los activos críticos de esta forma ser valorados de acuerdo a su criticidad.
b) Caracterización de las amenazas: en esta fase se identifican las amenazas y vulnerabilidades sobre lo que los activos están expuestos; así mismo como el impacto y probabilidad con la finalidad de obtener el nivel de riesgo intrínseco.

c) Caracterización de las salvaguardas: aquí se definen los mecanismos como salvaguardas y controles y se valora o mide de acuerdo a los criterios de efectividad.
d) Estimación del estado de riesgo residual: determina el riesgo residual al que están sometidos los activos teniendo en cuenta el valor de los activos y amenazas; así como también el grado de efectividad de las salvaguardas desplegadas.

El modelo general de gestión de riesgos se resume en el siguiente gráfico:

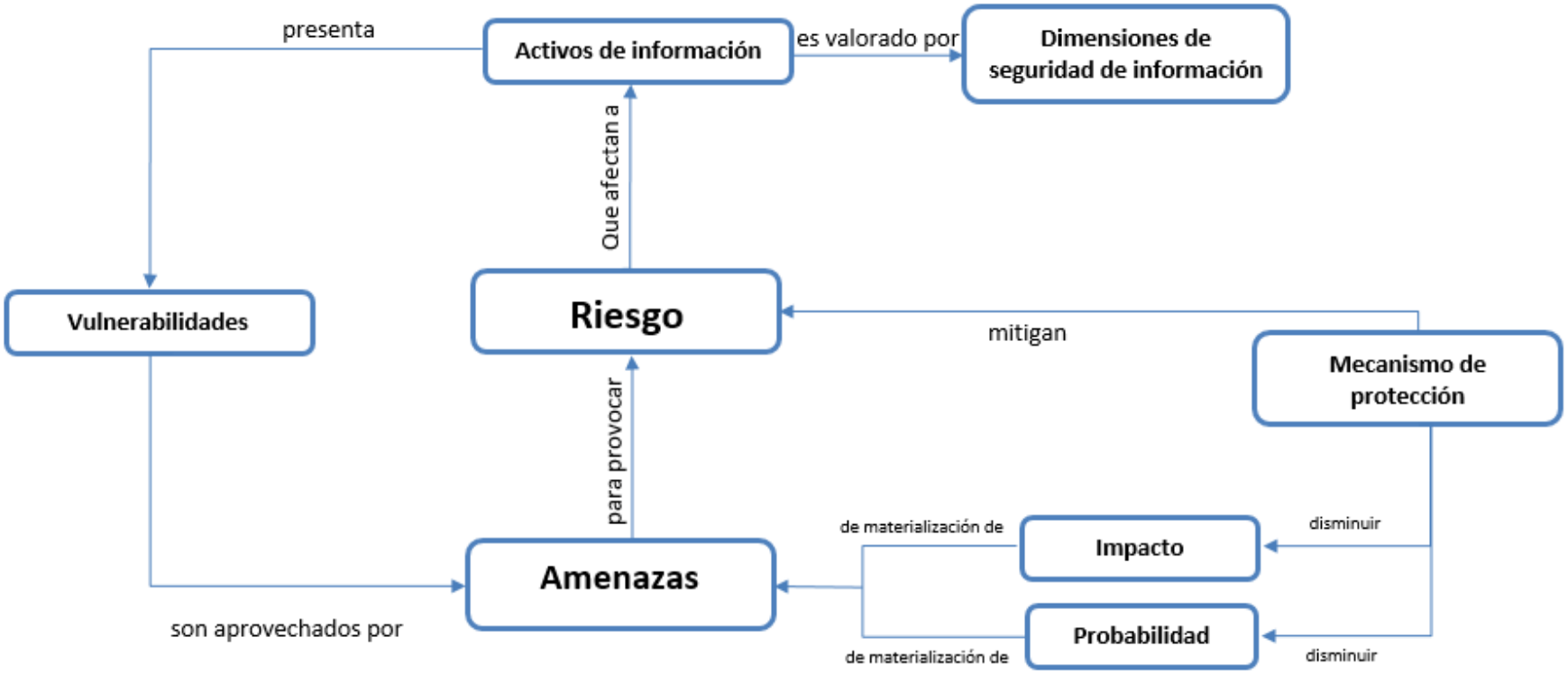


Gráfico N° 10: Modelo de gestión de riesgos propuesto.

Fuente: Elaboración propia

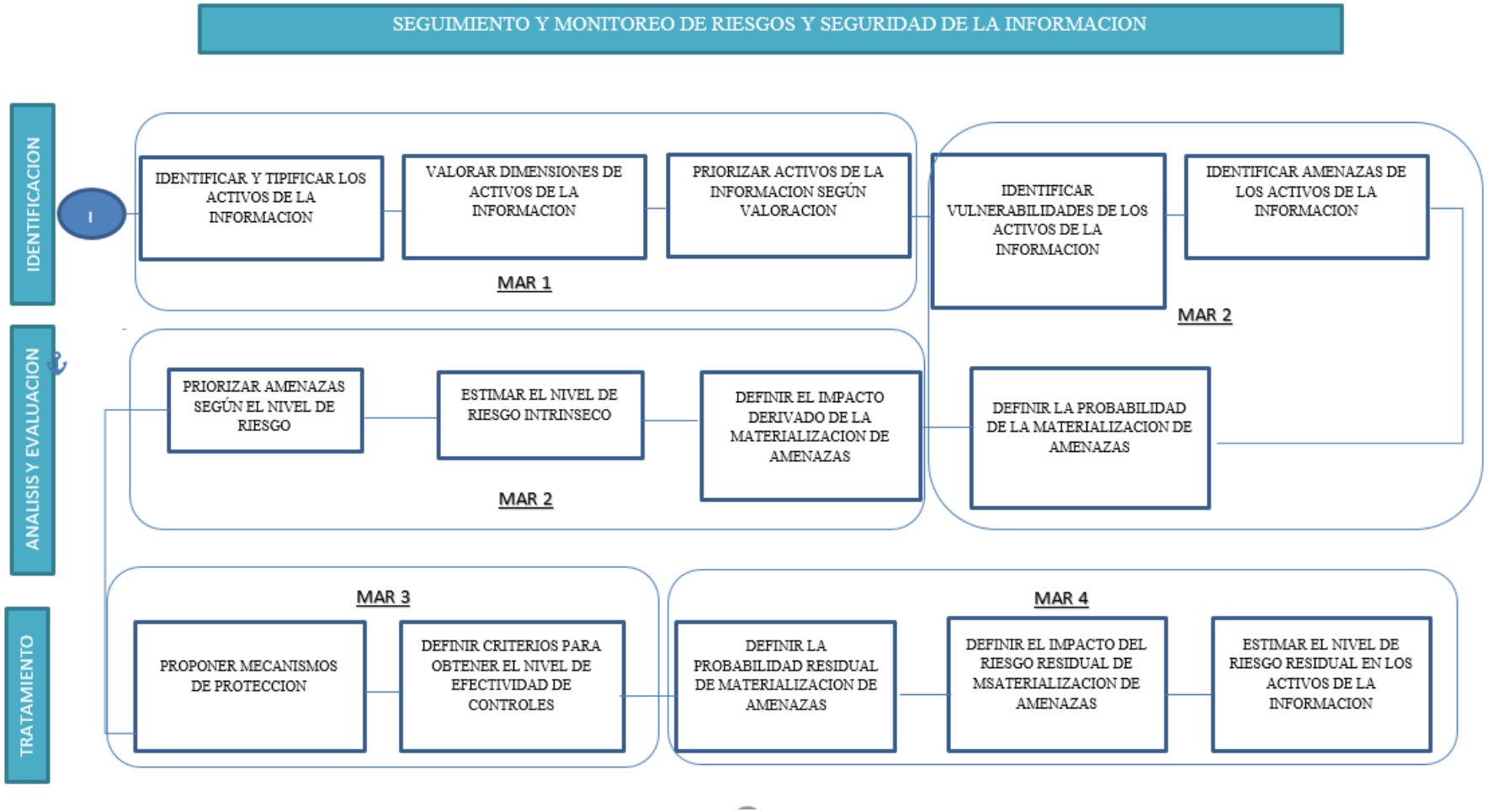


Gráfico N° 11: Metodología propuesta para la gestión de riesgos.

Fuente: Elaboración propia

MAR. 1 -Caracterización de los activos

Aquí se identificarán los activos por cada proceso crítico, clasificándolos según el tipo de activo, identificando la relación entre activos, valorando la importancia por cada dimensión de seguridad; para luego identificar los riesgos referentes a la seguridad de TI. La estructura de cada tarea se detalla en la siguiente ficha técnica:

Tabla N° 1: Ficha para la actividad de análisis de procesos para la identificación y la definición de la criticidad de los activos de TI.

<table>
<tr><td colspan="3">MAR- Método de Análisis de Riesgos
MAR. 1 -Caracterización de los activos</td></tr>
<tr><td colspan="3">MAR. 11 -Análisis de los procesos críticos de la empresa para identificar los activos críticos.</td></tr>
<tr><td colspan="3">Objetivo:</td></tr>
<tr><td colspan="3">Identificar los activos que están involucrados en los procesos críticos de la empresa.</td></tr>
<tr><td>Entradas</td><td>Salidas</td><td>Técnicas</td></tr>
<tr><td>- Identificación de los procesos más críticos del negocio

- Descripción de funciones de los puestos de trabajo</td><td>- Lista de los activos de TI a evaluar

- Clasificación de cada activo.</td><td>-Realizar un análisis (BIA) de impacto al negocio para obtener los activos de TI críticos de acuerdo a cada proceso.

-Reuniones y entrevistas con el personal de TI.

- Valoración por método Delphi
- Utilizar el Anexo N° 03</td></tr>
<tr><td colspan="3">MAR. 12 –Clasificar y priorizar los activos de acuerdo a su criticidad.</td></tr>
<tr><td colspan="3">Objetivo:</td></tr>
<tr><td colspan="3">Valorización de los activos de TI en base a cada dimensión de la seguridad.</td></tr>
<tr><td>Entradas</td><td>Salidas</td><td>Técnicas</td></tr>
<tr><td>- Lista de los activos de TI.</td><td>-Informe de la valorización de los activos de TI</td><td>-Reuniones y entrevistas con el personal de TI.

-Valoración por método Delphi

- Utilizar el Anexo N° 04</td></tr>
</table>

Fuente: Elaboración propia

MAR. 11 - Análisis de los procesos críticos de la empresa para identificar los activos críticos.

En esta tarea se identificarán los roles por cada proceso y subproceso crítico de la empresa y los activos de TI que dan soporte a cada uno. Para ello se utilizará un análisis de impacto del negocio (BIA) con el fin de obtener los activos críticos de acuerdo a cada proceso y subproceso.

Tabla N° 2: Formato para el Análisis de Impacto del Negocio por Proceso.

<table>
<tr><th colspan="3">NOMBRE DEL PROCESO</th></tr>
<tr><td>NOMBRE DEL SISTEMA:</td><td rowspan="3">RESPONSABLE DEL BIA</td><td>Responsable 1</td></tr>
<tr><td rowspan="2">Especificar el nombre del sistema principal</td><td>Responsable 2</td></tr>
<tr><td>Responsable 3</td></tr>
<tr><th>INDENTIFICAR CONCEPTOS CLAVE</th><th colspan="2">ROL</th></tr>
<tr><td colspan="3">Interno(identificar los usuarios , puestos de trabajo o áreas dentro de la empresa que tienen dependencia o dan soporte del sistema; especificar la relación con el sistema)</td></tr>
<tr><td rowspan="3">Posición interna 1</td><td colspan="2">Rol en el proceso-1</td></tr>
<tr><td colspan="2">Rol en el proceso-2</td></tr>
<tr><td colspan="2">Rol en el proceso-3</td></tr>
<tr><td rowspan="3">Posición interna 2</td><td colspan="2">Rol en el proceso-1</td></tr>
<tr><td colspan="2">Rol en el proceso-2</td></tr>
<tr><td colspan="2">Rol en el proceso-3</td></tr>
<tr><td rowspan="3">Posición interna 3</td><td colspan="2">Rol en el proceso-1</td></tr>
<tr><td colspan="2">Rol en el proceso-2</td></tr>
<tr><td colspan="2">Rol en el proceso-3</td></tr>
<tr><td colspan="3">Externo (identificar los usuarios , puestos de trabajo o áreas fuera de la empresa que dan soporte al sistema; especificar la relación con el sistema)</td></tr>
<tr><td>Posición externa 1</td><td colspan="2">Rol en el proceso-1</td></tr>
<tr><th colspan="3">IDENTIFICAR RECURSOS DE SISTEMA (hardware , software y otros recursos)</th></tr>
<tr><th>HARDWARE</th><th>TIPO</th><th>CANTIDAD</th></tr>
<tr><td>Hardware 1 (Ejemplo: servidores, estaciones de trabajo, etc.)</td><td>Tipo 1</td><td></td></tr>
<tr><th>SOFTWARE</th><th>TIPO</th><th>CANTIDAD</th></tr>
<tr><td>Software 1 (Ejemplo: aplicativos, sistemas operativos, etc.)</td><td>Tipo 1</td><td></td></tr>
<tr><th colspan="3">OTROS RECURSOS</th></tr>
<tr><td colspan="3">Identificar otros recursos relacionados en el proceso.</td></tr>
</table>

IDENTIFICAR ROLES CRITICOS	
Posición interna 1	*Rol crítico en el proceso 1*
	Rol crítico en el proceso 2
Posición interna 2	*Rol crítico en el proceso 1*
	Rol crítico en el proceso 2
Posición interna 3	*Rol crítico en el proceso 1*
	Rol crítico en el proceso 2
ENLAZAR ROLES CRITICOS A RECURSOS CRITICOS	
ROLES CRITICOS	**RECURSOS CRITICOS**
Posición interna 1	
Rol crítico en el proceso 1	*Recursos críticos que dan soporte a los roles críticos.*
Rol crítico en el proceso 2	
Posición interna 2	
Rol crítico en el proceso 1	*Recursos críticos que dan soporte a los roles críticos.*
Rol crítico en el proceso 2	
Posición interna 3	
Rol crítico en el proceso 1	*Recursos críticos que dan soporte a los roles críticos.*
Rol crítico en el proceso 2	

IDENTIFICAR IMPACTOS Y TIEMPOS ACEPTABLES DE LA CAIDA
(identifica el periodo máximo de interrupción y el tiempo objetivo de recuperación)

RECURSO	IMPACTO TRAS CAIDA	TMI (Tiempo Máximo de Interrupción)	TOR (Tiempo Objetivo de Recuperación)
Posición interna 1			
Recurso crítico 1	Describir la imposibilidad tras el impacto de la caída.		
Recurso crítico 2	Describir la imposibilidad tras el impacto de la caída.		

Recurso crítico 3	Describir la imposibilidad tras el impacto de la caída.		
Posición interna 2			
Recurso crítico 1	Describir la imposibilidad tras el impacto de la caída.		
Recurso crítico 2	Describir la imposibilidad tras el impacto de la caída.		
Recurso crítico 3	Describir la imposibilidad tras el impacto de la caída.		
Posición interna 3			
Recurso crítico 1	Describir la imposibilidad tras el impacto de la caída.		
Recurso crítico 2	Describir la imposibilidad tras el impacto de la caída.		
Recurso crítico 3	Describir la imposibilidad tras el impacto de la caída.		

INDENTIFICAR LA PRIORIDAD EN EL RECUPERO DE LOS RECURSOS CRÍTICOS (basado en el impacto tras la caída y el tiempo objetivo de recuperación, usar valoración cualitativas: alto, medio, bajo)	
RECURSOS	**PRIORIDAD DE RECUPERO**
Recurso crítico 1	
Recurso crítico 2	
Recurso crítico 3	

Fuente: Elaboración propia

Posteriormente se identificarán a los activos que cumplen la función de ser el soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE SAC. La clasificación que se usará será la propuesta por MAGERIT **(Ver anexo Nº 3).**

El inventario de activos de TI que se considerarán serán los identificados en el proceso en MAR. 11 (Análisis de los procesos críticos de la empresa para identificar los activos críticos) y los que dependan de ellos.

Se utilizará el siguiente formato para clasificar los activos de TI y usando como referencia el catálogo de activos de MAGERIT:

Tabla N° 3: Formato para consignar los activos de TI según su tipo.

N°	Tipo de activo de TI	Activo de TI	Activo (CODIGO)
1			
2			
3			

Fuente: Elaboración propia

MAR. 12 –Clasificar y priorizar los activos de acuerdo a su criticidad.

Al tener el inventario (**Tabla N° 3**) de los activos de TI se procederá a identificar y determinar el valor que representa a la organización según su seguridad. Estos se medirán bajo el criterio de las dimensiones de la seguridad definidos en el **Anexo N° 4**.

Dicha valoración se hará bajo la estimación de las pérdidas que se ocasionarían en la empresa comercial en caso de que el activo falle o caiga, a causa de que una amenaza se materialice; según el **Anexo N° 4** en relación a las dimensiones de la seguridad de la información:

Tabla N° 4: Escala y descripción de los criterios para la valoración de la criticidad de los activos de TI.

	Valor	Criterio
Disponibilidad	**1**	Sin relevancia
	2	Disponible al menos el 25% del tiempo
	3	Disponible al menos el 50% del tiempo
	4	Disponible al menos el 75% del tiempo
	5	Disponible al menos el 95% del tiempo
Integridad	**Valor**	**Criterio**
	1	Sin relevancia
	2	No tiene relevancia los errores que tenga o la información que falte
	3	Debe de estar sin errores y completo al menos en un 50%
	4	Debe de estar sin errores y completo al menos en un 75%
	5	Debe de estar sin errores y completo al menos en un 95%
Confidencialidad	**Valor**	**Criterio**
	1	Sin relevancia
	2	Perjuicios muy bajos, que no trasciende del área afectada
	3	Perjuicios bajos, que no repercute fuera del área afectada
	4	Los perjuicios serían importantes, el incidente impactaría en otras áreas
	5	Los perjuicios serían catastróficos, se compromete la imagen de la empresa.
Autenticidad	**Valor**	**Criterio**
	1	Sin relevancia
	2	No es importante conocer la fuente.
	3	Debe conocer la fuente al menos en un 50%
	4	Debe conocer la fuente al menos en un 75%
	5	Debe conocer la fuente al menos en un 95%
Trazabilidad	**Valor**	**Criterio**
	1	Sin relevancia
	2	Merma en la seguridad o dificultad para la investigación de un incidente
	3	Grave incidente de seguridad o dificultad para la investigación de incidentes graves
	4	Serio incidente de seguridad o dificultad para la investigación de incidentes serios
	5	Excepcional incidente serio de seguridad o dificultad para la investigación de incidentes excepcionalmente serios

Fuente: Elaboración propia

Tabla N° 5: Formato para la valoración de la criticidad de los activos de TI.

Activo	Criterios de seguridad					Total	Nivel de criticidad
	Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
1							
2							
3							

Fuente: Elaboración propia

Se obtendrán el nivel de criticidad por cada activo de TI según el promedio del valor calificado para cada criterio; su clasificación se realizará de la siguiente forma:

Tabla N° 6: Formato para la calificación del nivel de criticidad de los activos de TI

Rango	Nivel de criticidad	Descripción
1 – 5	1	Muy bajo
5 – 10	2	Bajo
11 – 15	3	Medio
16 – 20	4	Alto
21 – 25	5	Muy Alto

Fuente: Elaboración propia

MAR. 2 -Caracterización de las amenazas

En esta etapa se identificarán las amenazas y vulnerabilidades por cada activo; para luego valorizar el impacto y probabilidad de ocurrencia de las amenazas con el fin de determinar el nivel de riesgo intrínseco.

Tabla N° 7: Ficha para la actividad de reconocimiento de las amenazas, identificación de las vulnerabilidades, valoración del impacto y probabilidad de las amenazas; y estimación del nivel de riesgo.

MAR- Método de Análisis de Riesgos **MAR. 2 -Caracterización de las amenazas**		
MAR. 21 -Identificación de las amenazas		
Objetivo: Identificar las amenazas para cada activo de TI		
Entradas	**Salidas**	**Técnicas**
- Informe de la valorización de los activos de TI	- Informe de amenazas para cada activo de TI	- Reuniones y entrevistas con el personal de TI. - Utilizar el anexo N° 05 - Valoración Delphi
MAR. 22 -Identificación de vulnerabilidades por activo		
Objetivo: Identificar las vulnerabilidades para cada activo de TI		
Entradas	**Salidas**	**Técnicas**
- Informe de la valorización de los activos de TI	-Informe de vulnerabilidades por cada activo de TI	- Reuniones y entrevistas con el personal de TI.

		- Utilizar el anexo N° 02
MAR. 23 -Valorización del impacto y la probabilidad de ocurrencia de las amenazas.		
Objetivo: - Estimar el impacto que causaría la amenaza en cada dimensión del activo si llegara a materializarse - Estimar la probabilidad de ocurrencia de cada amenaza sobre cada activo.		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Listado de amenazas identificadas por activo de TI - Informes de vulnerabilidades	- Informe de amenazas , caracterizadas por el impacto y la probabilidad de ocurrencia	- Reuniones y entrevistas con el personal de TI. - Valoración Delphi
MAR. 24 -Valorización del Riesgo Intrínseco		
Objetivo: - Estimar el nivel de exposición al riesgo de TI según el apetito y tolerancia referente al riesgo para cada proceso.		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
-Informe de amenazas , caracterizadas por el impacto y la probabilidad de ocurrencia	- Informe del nivel de riesgo intrínseco.	- Reuniones y entrevistas con el personal de TI. - Valoración Delphi

Fuente: Elaboración propia

MAR. 21 – Identificación de las amenazas

Para desplegar la relación de amenazas por activo se tomará en consideración:

- La tipificación de los activos.
- La valorización de criticidad por cada activo según las dimensiones de la seguridad de TI
- Se utilizará el catálogo de amenazas por activo según MAGERIT (**Anexo N° 5**).

Tabla N° 8: Formato para el reconocimiento de amenazas por activo.

N°	Activo (CODIGO)	Amenaza	CODICO

1			
2			
3			

Fuente: Elaboración propia

MAR. 22 – Identificación de vulnerabilidades por activo

El resultado permite identificar las carencias internas que puedan ser usadas por las amenazas con el fin de materializarse y causar perjuicio a los activos de TI.

Para esta actividad se deben analizar las vulnerabilidades de tipo de seguridad: lógica, recursos humanos, física, ambiental, operacional, comunicaciones, mantenimiento, desarrollo y de adquisición.
La lista de vulnerabilidades se obtendrá con el trabajo en conjunto con el personal de la empresa.

Tabla N° 9: Formato para la identificación de las vulnerabilidades por cada Amenaza de los activos.

N°	Activo (CODIGO)	Amenaza (CODIGO)	Vulnerabilidad	CODIGO
1	Activo 1	Amenaza 1	Vulnerabilidad 1	
			Vulnerabilidad 2	
		Amenaza 2	Vulnerabilidad 1	
			Vulnerabilidad 2	
2	Activo 2	Amenaza 1	Vulnerabilidad 1	
			Vulnerabilidad 2	
		Amenaza 2	Vulnerabilidad 1	
			Vulnerabilidad 2	
			Vulnerabilidad 3	

Fuente: Elaboración propia

MAR. 23 - Valorización del impacto y la probabilidad de ocurrencia de las amenazas.

La valorización sirve para estimar la materialización de cada amenaza que se ha identificado por cada activo de TI. Esta tarea se calificará en base a la valorización del impacto y la probabilidad de que la amenaza ocurra.

Tabla N° 10: Valores y criterios de referencia para la valoración de los niveles de impacto de una amenaza.

[si] Segu	Valor	Criterio

	5	Causa un incidente excepcionalmente serio de seguridad o dificulta la investigación de incidentes excepcionalmente serios
	4	Causa un serio incidente de seguridad o dificulta la investigación de incidentes serios
	3	Causa un grave incidente de seguridad o dificulta la investigación de incidentes graves
	2	Causa una merma en la seguridad o dificulta la investigación de un incidente
	1	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o	**Valor**	**Criterio**
	5	causa de pérdidas económicas excepcionalmente elevadas
	4	causa de graves pérdidas económicas
	3	causa de pérdidas económicas o merma de ingresos
	2	de bajo valor económico
	1	supondría mínimas pérdidas económicas

[olm] Operaciones	**Valor**	**Criterio**
	5	Causa daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
	4	Causa daño serio a la eficacia o seguridad de la misión operativa o logística
	3	Perjudica la eficacia o seguridad de la misión operativa o logística
	2	Merma la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
	1	Merma la eficacia o seguridad de la misión operativa o logística de manera local

Fuente: Elaboración propia

- **Estimación del impacto de una amenaza**

Se usará el siguiente formato para la estimación del impacto de una amenaza:

Tabla N° 11: Formato para la calificación de la estimación del impacto de una amenaza

Activo	**Amenazas**	**Criterios de valoración**			**Total**	**Nivel de impacto**
		[si] Seguridad	**[cei] Intereses comerciales o económicos**	**[olm] Operaciones**		
1						
2						
3						

Fuente: Elaboración propia

Los niveles para valorizar el impacto de una amenaza se obtendrán del promedio de la calificación otorgadas a cada criterio de valorización y se clasificarán de la siguiente forma:

Tabla N° 12: Valoración de los niveles de impacto de una amenaza.

Rango	Nivel de Impacto	Descripción
1-3	1	Muy bajo
4-6	2	Bajo
7-9	3	Medio
10-12	4	Alto
13-15	5	Muy alto

Fuente: Elaboración propia

- **Estimación de La probabilidad de ocurrencia de una amenaza**

Se usará el siguiente formato para la calificación de la probabilidad de ocurrencia de cada una de las amenazas identificadas por activo TI:

Tabla N° 13: Formato para la calificación de la probabilidad de ocurrencia de una amenaza.

Nivel	Probabilidad	Descripción
1	Muy poco frecuente	Sin registro en los últimos 5 años
2	Poco frecuente	Probablemente se presenta una vez cada 5 años
3	Normal	Probablemente se presenta una vez al año
4	Frecuente	Probablemente se presenta una vez cada mes
5	Muy frecuente	Probablemente se presenta varias veces en el mes

Fuente: Elaboración propia

MAR. 24 - Valorización del Riesgo Intrínseco

- **Determinación del apetito y tolerancia del riesgo**

Tanto el apetito como la tolerancia al riesgo, está inmerso en el Riesgo Operacional, por lo que un incidente puede hacer que el resultado de un proceso sea diferente al esperado; estos fallos pueden ser ocasionados por fallas de los usuarios, en los sistemas o en los eventos internos o externos. Se considera al riesgo tecnológico dentro del riesgo operacional; es por ello que, para determinar el apetito del riesgo y la tolerancia, solo se involucrarán los riesgos que involucran al Riesgo Operacional con dependencia Tecnológica. Los riesgos operacionales se basan en la deficiencia de sus controles lo que conlleva al incumplimiento del objetivo del negocio.

Se utilizará la siguiente escala de valoración para los niveles de riesgo de TI en base a los siguientes escenarios de riesgo de TI:

Tabla N° 14: Escala de valoración para clasificar los niveles de riesgo de TI

ESCALA	DESCRIPCIÓN
MUY BAJO	La deficiencia del control no impide el cumplimiento de un objetivo
BAJO	La deficiencia del control genera perjuicios menores
MEDIO	La deficiencia del control genera pérdidas representativas
ALTO	La deficiencia del control representa una pérdida significativa, del tipo económico u operativo
MUY ALTO	La deficiencia del control representa una pérdida sustancial material, económica y/o sanción regulatoria

Tabla N° 15: Valorización para clasificar los niveles de riesgo de TI según los escenarios de riesgos.

ESCENARIO DE RIESGO	ESCALA	DESCRIPCIÓN
Obligaciones legales	**MUY BAJO**	Sin relevancia
	BAJO	Causa el incumplimiento leve de una regulación
	MEDIO	Causa el incumplimiento de una regulación
	ALTO	Causa el incumplimiento grave de una regulación
	MUY ALTO	Causa el incumplimiento excepcionalmente grave de una regulación
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Seguridad	**MUY BAJO**	Sin relevancia
	BAJO	Causa una merma en la seguridad
	MEDIO	Causa un grave incidente de seguridad
	ALTO	Causa un serio incidente de seguridad
	MUY ALTO	Causa un incidente excepcionalmente serio de seguridad
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Intereses comerciales y económicos	**MUY BAJO**	Sin relevancia
	BAJO	de bajo interés para la competencia o bajo valor comercial
	MEDIO	de cierto interés para la competencia o cierto valor comercial
	ALTO	de alto interés para la competencia o alto valor comercial
	MUY ALTO	de enorme interés para la competencia o elevado valor comercial
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Interrupción del servicio	**MUY BAJO**	Sin relevancia
	BAJO	Causa interrupción de los servicios propios de Chancafe Norte SAC
	MEDIO	Causa interrupción de los servicios propios de Chancafe Norte SAC con impacto en otras entidades o en los clientes
	ALTO	Causa interrupción seria de los servicios propios de Chancafe Norte SAC con un impacto significativo en otras entidades
	MUY ALTO	Causa interrupción excepcionalmente seria de los servicios propios de Chancafe Norte SAC con un serio impacto en otras entidades
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**

Operaciones	**MUY BAJO**	Sin relevancia
	BAJO	Disminuye la eficacia o seguridad de la misión operativa de manera local
	MEDIO	Disminuye la eficacia o seguridad de la misión operativa, repercute fuera del área local.
	ALTO	Causa daño serio a la eficacia o seguridad de la misión operativa
	MUY ALTO	Causa daño excepcionalmente serio a la eficacia o seguridad de la misión operativa
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Administración y gestión	**MUY BAJO**	Sin relevancia
	BAJO	Impide la operación efectiva de una parte de Chancafe Norte SAC
	MEDIO	Impide la operación efectiva de más de una parte de Chancafe Norte SAC
	ALTO	Impide la operación efectiva de Chancafe Norte SAC
	MUY ALTO	Impide seriamente la operación efectiva de Chancafe Norte SAC, pudiendo llegar a su cierre
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Pérdida de reputación	**MUY BAJO**	Sin relevancia
	BAJO	Afecta negativamente a las relaciones internas de Chancafe Norte SAC
	MEDIO	Causa cierta publicidad negativa para afectar negativamente a las relaciones con otras organizaciones
	ALTO	Causa publicidad negativa generalizada para afectar gravemente a las relaciones con otras organizaciones
	MUY ALTO	Causa publicidad negativa generalizada para afectar de forma excepcionalmente grave a las relaciones con otras organizaciones
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Persecución de delitos	**MUY BAJO**	Sin relevancia
	BAJO	Puede dificultar la investigación de delitos
	MEDIO	Dificulta la investigación de delitos
	ALTO	Impide la investigación de delitos graves
	MUY ALTO	Impide la investigación de delitos excepcionalmente graves
ESCENARIO DE RIESGO	**ESCALA**	**DESCRIPCIÓN**
Tiempo de recuperación del servicio	**MUY BAJO**	5 días < TOR
	BAJO	1 día < TOR < 5 días
	MEDIO	4 horas < TOR < 1 día
	ALTO	1 hora < TOR < 4 horas
	MUY ALTO	TOR < 1 hora

Fuente: Elaboración propia

Para determinar el apetito y la tolerancia en cada uno de los escenarios de riesgos de TI definidos que podrían afectar el no cumplimiento de los objetivos estratégicos u operacionales, se utilizará la siguiente estructura:

Tabla N° 16: Formato para determinar el apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional.

CHANCAFE NORTE SAC		
OBJETIVO OPERACIONAL:		
Apetito de riesgo de TI		
Tolerancia de riesgo de TI		
Escenario de riesgo de TI	**Impacto**	**Probabilidad**
Infraestructura física		
Personal de TI		
Gestión de proyectos		
Gestión de la seguridad		
Entrega y soporte de servicios de TI		
Cumplimiento corporativo		
Cumplimiento legal		
Otros escenarios		

- **Cálculo de los niveles de riesgos Intrínsecos (NRI)**

Para calcular el nivel de Riesgo Intrínseco de cada amenaza, que a su vez fue identificada por activo, el NRI estará en función de la valoración del impacto y la probabilidad de ocurrencia de cada una de las amenazas. Se utilizará la siguiente relación:

Nivel de Riesgo Intrínseco = Probabilidad de ocurrencia x Impacto

NRI= P x I

Considerando los niveles de riesgo definidos anteriormente, el NRI se ubicará en la siguiente tabla de mapa de calor:

Tabla N° 17: Mapa de calor para la valoración del impacto y probabilidad de las amenazas.

Impacto en los procesos	**Probabilidad de ocurrencia**				
	Muy poco frecuente	**Poco frecuente**	**Normal**	**Frecuente**	**Muy frecuente**
Muy alto	**B**	**M**	**A**	**MA**	**MA**
Alto	**B**	**B**	**M**	**A**	**MA**
Medio	**MB**	**B**	**M**	**M**	**A**
Bajo	**MB**	**B**	**B**	**B**	**M**
Muy bajo	**MB**	**MB**	**MB**	**B**	**B**

B=Bajo, MB= Muy Bajo, M=Medio, A=Alto, MA=Muy Alto

Fuente: Elaboración propia

MAR. 3 – Caracterización de las salvaguardas

Esta etapa comprende la definición e implementación de los mecanismos de seguridad como controles o salvaguardas que serán necesarias en el tratamiento de las amenazas.

Tabla N° 18: Ficha para la actividad de identificación y valorización de los controles o salvaguardas.

<table>
<tr><td colspan="3">MAR- Método de Análisis de Riesgos</td></tr>
<tr><td colspan="3">MAR. 3 -Caracterización de las salvaguardas</td></tr>
<tr><td colspan="3">MAR. 31 -Identificación de los controles o salvaguardas pertinentes</td></tr>
<tr><td colspan="3">Objetivo:</td></tr>
<tr><td colspan="3">- Identificar las salvaguardas necesarias para proteger el sistema.</td></tr>
<tr><td>Entradas</td><td>Salidas</td><td>Técnicas</td></tr>
<tr><td>- Informe del nivel de riesgo intrínseco</td><td>- Lista de salvaguardas desplegadas.</td><td>- Reuniones y entrevistas con el personal de TI.
- Usar el Anexo N° 6</td></tr>
<tr><td colspan="3">MAR. 32 -Valoración de las salvaguardas</td></tr>
<tr><td colspan="3">Objetivo:</td></tr>
<tr><td colspan="3">- Determinar el nivel de efectividad de las salvaguardas pertinentes</td></tr>
<tr><td>Entradas</td><td>Salidas</td><td>Técnicas</td></tr>
<tr><td>- Relación de salvaguardas desplegadas.</td><td>- Informe de salvaguardas desplegadas, caracterizadas por su nivel de efectividad.</td><td>- Reuniones y entrevistas con el personal de TI.
- Valoración Delphi</td></tr>
</table>

Fuente: Elaboración propia

MAR. 31 -Identificación de los controles o salvaguardas pertinentes

- **Plan de tratamiento de los riesgos intrínsecos**

  En esta actividad se determina la aceptación del riesgo; por un lado, si el riesgo es aceptado o por otro si es necesario algún tratamiento; esto es determinado por el apetito del riesgo definido con anterioridad.

  Según el nivel de Riesgo Intrínseco se determinará si es que el riesgo es aceptable o no para la empresa. Los niveles NRI con valoración “Muy Alta” o “Alta” son

los que se trataran por medio de salvaguardas o controles y para las valoraciones "Medio", "Baja" o "Muy Baja" se aceptará la convivencia con el riesgo.

Tabla N° 19: Criterios de aceptación para el Apetito al riesgo de TI según el nivel de exposición al riesgo .

Nivel de Riesgo Intrínseco	Criterio de aceptación
Muy alto	Riesgo No aceptado por Chancafe Norte SAC
Alto	Riesgo No aceptado por Chancafe Norte SAC
Medio	Riesgo aceptado por Chancafe Norte SAC
Bajo	Riesgo aceptado por Chancafe Norte SAC
Muy bajo	Riesgo aceptado por Chancafe Norte SAC

Fuente: Elaboración propia

Luego, se determinan las medidas de seguridad para los riesgos no aceptados por la empresa.

- **Implementación de las medidas de seguridad**

Los controles, se obtendrán del catálogo de salvaguardas de MAGERIT (**Anexo N° 6**), que se seleccionarán para el tratamiento de los riesgos.

- **Identificación de la estrategia de implementación de controles**

Una vez seleccionado el control o salvaguarda para cada riesgo intrínseco, se definirá la estrategia para su implementación según:

– Estrategia de aceptar el riesgo
– Estrategia de elegir el control
– Estrategia de mitigar el riesgo
– Estrategia de trasladar el riesgo a terceros
– Estrategia de prevenir el aumento del riesgo

MAR. 32 - Valoración de las salvaguardas

- **Definir criterios para obtener efectividad de las salvaguardas**

Tabla N° 20: Criterios para determinar el nivel de efectividad de las salvaguardas

MECANISMOS DE PORTECCION (SALVAGUARDAS)	**ESTADO DE MECANISMO DE PROTECCION (EMP)**	
	0	Implementado
	1	No implementado
	OPORTUNIDAD DE PROPUESTA DE MECANISMOS DE PROTECCION (OMP)	
	1	Preventivo
	2	Detectivo
	3	Correctivo
	GRADO DE IMPLEMENTACION (GI)	
	1	Manual
	2	Semiautomatizada
	3	Automatizado

- **Estado de mecanismo de protección (EMP)**: Se registrará según el estado del en el que se encuentra el mecanismo de protección.
- **Oportunidad de propuesta de mecanismos de protección (OMP)**: Se registrará la oportunidad de la propuesta para el activo analizado.
- **Grado de implementación (GI):** Se registrará el grado de implementación de los mecanismos para el activo analizado.
- **Nivel de efectividad**: el valor del nivel de efectividad del mecanismo de protección señalado para el activo analizado, se determinará de acuerdo al resultado de las combinaciones de EMP, OMP Y GI, tal y como se muestra a continuación:

Tabla N° 21: Equivalencia de la combinación de los criterios para determinar el nivel de efectividad de las salvaguardas.

NIVELES DE EFECTIVIDAD DE MEDIDAS DE PROTECCIÓN					
EMP	**OMP**	**GI**	**RESULTADO**	**DESCRIPCION**	**VALOR**
No implementado	Preventivo	Manual	No implementado/Preventivo/Manual	Deficiente	1
No implementado	Preventivo	Semiautomático	No implementado/Preventivo/Semiautomático	Deficiente	1
No implementado	Preventivo	Automatizado	No implementado/Preventivo/Automatizado	Deficiente	1
No implementado	Correctivo	Manual	No implementado/Correctivo/Manual	Deficiente	1
No implementado	Correctivo	Semiautomático	No implementado/Correctivo/Semiautomático	Deficiente	1
No implementado	Correctivo	Automatizado	No implementado/Correctivo/Automatizado	Deficiente	1
No implementado	Detectivo	Manual	No implementado/Detectivo/Manual	Deficiente	1
No implementado	Detectivo	Semiautomático	No implementado/Detectivo/Semiautomático	Deficiente	1
No implementado	Detectivo	Automatizado	No implementado/Detectivo/Automatizado	Deficiente	1
Implementado	Correctivo	Manual	Implementado/Correctivo/Manual	Regular	2

Implementado	Correctivo	Semiautomático	Implementado/Correctivo/Semiautomático	Regular	2
Implementado	Correctivo	Automatizado	Implementado/Correctivo/Automatizado	Regular	2
Implementado	Detectivo	Manual	Implementado/Detectivo/Manual	Más que regular	3
Implementado	Detectivo	Semiautomático	Implementado/Detectivo/Semiautomático	Más que regular	3
Implementado	Detectivo	Automatizado	Implementado/Detectivo/Automatizado	Bueno	4
Implementado	Preventivo	Manual	Implementado/Preventivo/Manual	Bueno	4
Implementado	Preventivo	Semiautomático	Implementado/Preventivo/Semiautomático	Optimo	5
Implementado	Preventivo	Automatizado	Implementado/Preventivo/Automatizado	Optimo	5

Fuente: Elaboración propia

Importante: De contar con más de un mecanismo de protección por riesgo de TI analizado, en la matriz de riesgos se consignará el promedio de los valores resultantes de la combinación de los criterios.

MAR. 4 – Estimación del estado de riesgo residual

En esta etapa se determina el riesgo residual (RR) al que están doblegados los activos teniendo en cuenta el grado de efectividad de las salvaguardas desplegadas.

Tabla N° 22: Ficha para la actividad de valorización del riesgo residual.

MAR- Método de Análisis de Riesgos **MAR. 4 -Estimación del estado del riesgo residual**		
MAR. 41 -Estimación del riesgo residual		
Objetivo:		
- Estimar el impacto residual que causaría la amenaza en cada dimensión del activo si llegara a materializarse. - Estimar la probabilidad de ocurrencia residual de cada amenaza sobre cada activo. - Determinar el riesgo residual al que esta doblegado el sistema		
Entradas o insumos necesarios	**Salidas**	**Técnicas**
- Informe de salvaguardas desplegadas, caracterizadas por su nivel de efectividad.	- Informe del riesgo residual.	- Reuniones y entrevistas con el personal de TI. - Valoración Delphi

Fuente: Elaboración propia

MAR. 41 – Estimación del riesgo residual.

- **Definir probabilidad residual de materialización de amenaza sobre un activo de información**

  Según el valor del nivel de efectividad de las salvaguardas, el valor de la probabilidad residual se obtiene mediante la diferencia del valor de la probabilidad de materialización de amenazas (PMA) menos el valor según la equivalencia del nivel de efectividad de la salvaguarda del activo analizado.

Tabla N° 23: Valoración de la probabilidad residual según la equivalencia del nivel de efectividad de las salvaguardas.

NIVEL DE EFECTIVIDAD DE LAS SALVAGUARDAS		PROBABILIDAD RESIDUAL
DESCRIPCION	**VALOR**	**PMA: Probabilidad de Materialización de las amenazas**
Deficiente	1	A la PMA se le resta 0
Regular	2	A la PMA se le resta 1
Más que regular	3	A la PMA se le resta 2
Bueno	4	A la PMA se le resta 3
Optimo	5	A la PMA se le resta 4

- **Definir impacto residual de materialización de amenaza sobre un activo de información.**

Según el valor del nivel de efectividad de las salvaguardas, el valor del impacto residual se obtiene mediante la diferencia del valor de impacto de materialización (IMI) menos el valor según la equivalencia del nivel de efectividad de la salvaguarda del activo analizado.

Tabla N° 24: Valoración del impacto residual según la equivalencia del nivel de efectividad de las salvaguardas

NIVEL DE EFECTIVIDAD DEL MECANISMO DE PROTECCION		IMPACTO RESIDUAL
DESCRIPCION	**VALOR**	**IMI Impacto intrínseco**
Deficiente	1	A IMI se le resta 0
Regular	2	A IMI se le resta 1
Más que regular	3	A IMI se le resta 2
Bueno	4	A lMI se le resta 3
Optimo	5	A IMI se le resta 4

- **Definir el nivel de riesgo residual (NRR)**

Para calcular el nivel de Riesgo Residual de cada amenaza, que a su vez fue identificada por activo, el NRR estará en función de la valoración del impacto residual y la probabilidad residual de ocurrencia de cada una de las amenazas. Se utilizará la siguiente relación:

Nivel de Riesgo Residual = Probabilidad residual x Impacto residual

NRR= PR x IR

Considerando los niveles de riesgo definidos anteriormente, el NRR se ubicará en la siguiente tabla de mapa de calor:

Tabla N° 25: Matriz de calor para la valoración del impacto residual y probabilidad residual de las amenazas.

Impacto Residual en los procesos	Probabilidad Residual de ocurrencia				
	Muy poco frecuente	Poco frecuente	Normal	Frecuente	Muy frecuente
Muy alto	B	M	A	MA	MA
Alto	B	B	M	A	MA
Medio	MB	B	M	M	A
Bajo	MB	B	B	B	M
Muy bajo	MB	MB	MB	B	B

B=Bajo, MB= Muy Bajo, M=Medio, A=Alto, MA=Muy Alto

Fuente: Elaboración propia

IV. RESULTADOS

4.1 Análisis de los procesos críticos de la empresa para identificar los activos críticos.
A través del análisis de impacto al negocio se identificaron 4 subprocesos, posteriormente se realizó el análisis de impacto al negocio por cada subproceso.

Tabla N° 26: Procesos críticos de la empresa.

Proceso crítico de negocio	subproceso
Evaluación	**Aprobación del crédito.**
Financiamiento	**Desembolso del crédito**
Cobranza	**Amortización del crédito**
	Recuperación del crédito

Tabla N° 27: Análisis del subproceso Aprobación del crédito.

APROBACION DEL CREDITO		
NOMBRES DE SISTEMAS:	RESPONSABLE DEL BIA	SUPERVISOR DE CREDITO
EQUIFAX		ASESOR DE CREDITO
NAVASOFT V5.0		ADMINISTRADOR DE TIENDA
INDENTIFICAR CONCEPTOS CLAVE	**ROL**	
Interno*(identificar los usuarios , puestos de trabajo o áreas dentro de la empresa que tienen dependencia o dan soporte del sistema; especificar la relación con el sistema)*		
ASESOR DE VENTA	Consultar la disponibilidad de stock y precio del producto de compra al crédito.	
	Preparar expedientes de crédito con la documentación adecuada, según la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Prepara el expediente de crédito con la información requerida de forma ordenada y legible.	
	Elevar y fundamentar las propuestas de crédito al supervisor de crédito.	
SUPERVISOR DEL CREDITO	Registrar y hacerse responsable de la veracidad de la información registrada en el expediente de crédito del cliente, verificar la información.	
	Verificar que los créditos presentados por los asesores de venta estén sujetas a la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Organizar y controlar los procesos de información , tramitación, evaluación y aprobación de los créditos según normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Registrar, completar y actualizar la información del crédito en el sistema por cada operación de crédito.	

	Aprobar las solicitudes de crédito evaluadas favorablemente dentro de la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Autorizar y supervisar el desembolso de los créditos aprobados presentados por los asesores de venta.	
ADMINISTRADOR DE TIENDA	Supervisar el proceso de otorgamiento de créditos, normándolo y administrándolo.	
	Disponer y supervisar el desembolso de los créditos aprobados	
Externo *(identificar los usuarios , puestos de trabajo o áreas fuera de la empresa que dan soporte al sistema; especificar la relación con el sistema)*		
Central de riesgos SBS y Equifax	Consultar información del sistema financiero e historial crediticio.	
Portal RENIEC	Consultar información de datos personales.	
IDENTIFICAR RECURSOS DE SISTEMA (hardware , software y otros recursos)		
HARDWARE	**TIPO**	**CANTIDAD**
Servidores	Servidor de Comunicaciones	1
	Servidor de Base de Datos	1
Estaciones de trabajo		4
SOFTWARE	**TIPO**	**CANTIDAD**
Aplicativo	NAVASOFT V5.0 :	
	MODULO COTIZAR VENTAS CON FINANCIAMIENTO	
	CAJERO VENTAS	
	MICROSOFT OFFICE	
Sistema operativo	Windows 7 service pack 1	
OTROS RECURSOS		
Red LAN		
Internet (central de riesgos, RENIEC y correo electrónico)		
Fluido eléctrico		
Línea Telefónica		
Antivirus		
Impresora		
IDENTIFICAR ROLES CRITICOS		
ASESOR DE VENTA	Consultar la disponibilidad de stock y precio del producto de compra al crédito.	
	Preparar expedientes de crédito con la documentación adecuada, según la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Elevar y fundamentar las propuestas de crédito al supervisor de crédito.	
SUPERVISOR DEL CREDITO	Registrar y hacerse responsable de la veracidad de la información registrada en el expediente de crédito del cliente, verificar la información.	
	Verificar que los créditos presentados por los asesores de venta estén sujetas a la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	

	Registrar, completar y actualizar la información del crédito en el sistema por cada operación de crédito.
	Aprobar las solicitudes de crédito evaluadas favorablemente dentro de la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.
	Autorizar y supervisar el desembolso de los créditos aprobados presentados por los asesores de venta.
ADMINISTRADOR DE TIENDA	Supervisar el proceso de otorgamiento de créditos, normándolo y administrándolo.
ENLAZAR ROLES CRITICOS A RECURSOS CRITICOS	
ROLES CRITICOS	**RECURSOS CRITICOS**
ASESOR DE VENTA	
Consultar la disponibilidad de stock y precio del producto de compra al crédito.	Acceso a Navasoft: MODULO CAJERO VENTAS - COTIZACIONES
	Computadora
Preparar expedientes de crédito con la documentación adecuada, según la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	Fluido eléctrico
Elevar y fundamentar las propuestas de crédito al supervisor de crédito.	Red LAN
SUPERVISOR DEL CREDITO	
Registrar y hacerse responsable de la veracidad de la información registrada en el expediente de crédito del cliente, verificar la información.	Acceso a Navasoft: MODULO COTIZAR VENTA CON FINANCIAMIENTO
	Internet (central de riesgos, RENIEC y correo electrónico)
	Computadora
Verificar que los créditos presentados por los asesores de venta estén sujetas a la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC	Red LAN
Aprobar las solicitudes de crédito evaluadas favorablemente dentro de la normativa interna y requisitos establecidos por CHANCAFE NORTE SAC	Fluido eléctrico
Autorizar y supervisar el desembolso de los créditos aprobados presentados por los asesores de venta.	Impresora
ADMINISTRADOR DE TIENDA	
Supervisar el proceso de otorgamiento de créditos, normándolo y administrándolo.	Acceso a Navasoft: MODULO GESTION CUOTAS POR COBRAR
	Fluido eléctrico
	Laptop
	Red LAN

	Internet (central de riesgos, RENIEC y correo electrónico)		
	Microsoft office.		
IDENTIFICAR IMPACTOS Y TIEMPOS ACEPTABLES DE LA CAIDA (identifica el periodo máximo de interrupción y el tiempo objetivo de recuperación)			
RECURSO	**IMPACTO TRAS CAIDA**	**TMI**	**TOR**
ASESOR DE VENTA			
Acceso a Navasoft: MODULO CAJERO VENTAS - COTIZACIONES	Imposibilidad de: consultar la disponibilidad de stock y precio del producto de compra al crédito.	01:00	00:45
Computadora	Imposibilidad de: acceso a Navasoft-MODULO CAJERO VENTAS – COTIZACIONES	00:45	00:30
Fluido eléctrico	Imposibilidad de: acceder a los recursos de TI eléctricos que facilitan el desarrollo de sus funciones.	00:30	00:20
Red LAN	Imposibilidad de: acceder a los sistemas internos y externos, dificultando un desempeño normal.	01:00	00:45
SUPERVISOR DEL CREDITO			
Acceso a Navasoft: MODULO COTIZAR VENTA CON FINANCIAMIENTO	Imposibilidad de: registrar la información de monto del crédito, monto de cuota, número de cuotas y generar el número de solicitud.	01:00	00:45
Internet (central de riesgos, RENIEC y correo electrónico)	Imposibilidad de: acceder a los Aprobar las solicitudes de crédito evaluadas favorablemente por los asesores de ventas dentro de la autonomía establecida.	01:00	00:45
Computadora	Imposibilidad de: elaboración de informes, fichas de registro, y demás utilitarios.	01:00	00:45
Red LAN	Imposibilidad de: acceder a los sistemas internos externos, dificultando un desempeño normal.	01:00	00:45
Fluido eléctrico	Imposibilidad de: acceder a los recursos de TI eléctricos que facilitan el desarrollo de sus funciones.	01:00	00:45

Impresora	Imposibilidad de: imprimir informes, fichas de registro, y demás utilitarios.	02:00	01:00
ADMINISTRADOR DE TIENDA			
Acceso a Navasoft: MODULO GESTION CUOTAS POR COBRAR	Imposibilidad de: Revisar las propuestas de crédito registradas por los asesores de ventas.	00:30	00:20
Fluido eléctrico	Imposibilidad de: acceder a los recursos de TI eléctricos que facilitan el desarrollo de sus funciones.	00:30	00:25
Laptop	Imposibilidad de: acceder a las plataformas de sistemas internos y externos, a las fichas de registro y demás utilitarios y a la data histórica.	01:00	00:45
Red LAN	Imposibilidad de: acceder a los sistemas internos externos, dificultando un desempeño normal.	00:30	00:20
Internet (central de riesgos, RENIEC y correo electrónico)	Imposibilidad de: acceder a las centrales de riesgo, portales de información del solicitante del crédito y de autorización para otorgamientos de créditos.	00:30	00:20
Microsoft office.	Imposibilidad de: elaboración de informes, fichas de registro, y demás utilitarios.	02:00	01:00

INDENTIFICAR LA PRIORIDAD EN EL RECUPERO DE LOS RECURSOS CRÍTICOS (basado en el impacto tras la caída y el tiempo objetivo de recuperación, usar valoración cualitativas: alto, medio, bajo)

RECURSOS	PRIORIDAD DE RECUPERO
NAVASOFT V5.0	ALTO
Computadora	ALTO
Fluido eléctrico	ALTO
Internet	ALTO
Red LAN	ALTO
Impresora	MEDIO
Microsoft office.	MEDIO

Tabla N° 28: Análisis del subproceso Desembolso del Crédito.

DESEMBOLSO DEL CREDITO		
NOMBRES DE SISTEMAS:	RESPONSABLE DEL BIA	SUPERVISOR DE CREDITO
NAVASOFT V5.0		CAJERO
		AUXILIAR DE DESPACHO
INDENTIFICAR CONCEPTOS CLAVE	**ROL**	
Interno*(identificar los usuarios , puestos de trabajo o áreas dentro de la empresa que tienen dependencia o dan soporte del sistema; especificar la relación con el sistema)*		
CAJERO	Emitir el comprobante de compra del producto al crédito.	
	Hacer entrega al supervisor de crédito y tesorería diariamente los documentos físicos de las operaciones realizadas en el día para el archivo de los mismos.	
	Recepción en el sistema la información del producto, número de cuotas e inicial de los créditos; generada por el supervisor de créditos.	
SUPERVISOR DEL CREDITO	Autorizar el desembolso de créditos en productos de la tienda y emitir el cronograma de pagos.	
	Verificar la conformidad de los expedientes de crédito según normativa interna y requisitos establecidos por CHANCAFE NORTE SAC.	
	Generar y entregar al cliente el cronograma de pagos del crédito.	
	Archivar el expediente de crédito.	
AUXILIAR DE DESPACHO	Verificar la conformidad del comprobante de pago generado por el cajero.	
	Ubicar en el almacén el producto a entregar al cliente.	
	Generar la GUIA DE REMISION en el sistema seleccionando el modelo, serie y características del producto a despachar.	
	Hacer firmar al cliente la conformidad de la entrega del producto.	
Externo *(identificar los usuarios , puestos de trabajo o áreas fuera de la empresa que dan soporte al sistema; especificar la relación con el sistema)*		
Proveedor de facturación Electrónica	Emitir y enviar las facturas electrónicas a SUNAT	
IDENTIFICAR RECURSOS DE SISTEMA (hardware , software y otros recursos)		
HARDWARE	**TIPO**	**CANTIDAD**
Servidores	Servidor de Comunicaciones	1
	Servidor de Base de Datos	1
Estaciones de trabajo		28
SOFTWARE	**TIPO**	**CANTIDAD**
Aplicativo	NAVASOFT V5.0:	

	Módulo VENTAS - EMISION COMPROBANTE DE PAGO	
	Módulo FINANCIERA - CANJE	
	Módulo CAJERO VENTAS - DESPACHO	
	Módulo de Facturación Electrónica.	
Sistema operativo	Windows 7 service pack 1	
OTROS RECURSOS		
Red LAN		
Internet (correo electrónico)		
Fluido eléctrico		
Línea Telefónica		
Antivirus		
Impresora		
IDENTIFICAR ROLES CRITICOS		
CAJERO	Emitir el comprobante de compra del producto al crédito.	
	Recepción en el sistema la información del producto, número de cuotas e inicial de los créditos; generada por el supervisor de créditos.	
SUPERVISOR DEL CREDITO	Autorizar el desembolso de créditos en productos de la tienda y emitir el cronograma de pagos.	
	Generar y entregar al cliente el cronograma de pagos del crédito.	
AUXILIAR DESPACHO	Verificar la conformidad del comprobante de pago generado por el cajero.	
	Generar la GUIA DE REMISION en el sistema seleccionando el modelo, serie y características del producto a despachar.	
ENLAZAR ROLES CRITICOS A RECURSOS CRITICOS		
ROLES CRITICOS	**RECURSOS CRITICOS**	
CAJERO		
Emitir el comprobante de compra del producto al crédito.	Acceso a Navasoft: Módulo VENTAS - EMISION COMPROBANTE DE PAGO	
	Acceso a Navasoft: Módulo de Facturación Electrónica.	
	Acceso a Navasoft: Módulo FINANCIERA - CANJE	
	Computadora	
	Red LAN	
	Fluido eléctrico	
	Impresora	
Recepción en el sistema la información del producto, número de	Internet (Correo electrónico)	

cuotas e inicial de los créditos; generada por el supervisor de créditos.	
SUPERVISOR DEL CREDITO	
Autorizar el desembolso de créditos en productos de la tienda y emitir el cronograma de pagos.	Acceso a Navasoft: Módulo COMERCIAL CREDICON-SOLICITUD DE CREDITO
	Computadora
	Red LAN
	Internet (correo electrónico)
	Fluido eléctrico
Generar y entregar al cliente el cronograma de pagos del crédito.	Impresora
AUXILIAR DE DESPACHO	
Verificar la conformidad del comprobante de pago generado por el cajero.	Acceso a Navasoft: Módulo CAJERO VENTAS - DESPACHO
	Computadora
	Red LAN
	Internet (correo electrónico)
	Fluido eléctrico
Generar la GUIA DE REMISION en el sistema seleccionando el modelo, serie y características del producto a despachar.	Impresora

IDENTIFICAR IMPACTOS Y TIEMPOS ACEPTABLES DE LA CAIDA
(identifica el periodo máximo de interrupción y el tiempo objetivo de recuperación)

RECURSO	IMPACTO TRAS CAIDA	TMI	TOR
CAJERO			
Acceso a Navasoft: Módulo VENTAS - EMISION COMPROBANTE DE PAGO	Imposibilidad de: Emitir el comprobante de compra del producto al crédito y recepcionar en el sistema la información del producto, número de cuotas e inicial de los créditos; generada por el supervisor de créditos.	01:00	00:45
Acceso a Navasoft: Módulo FINANCIERA - CANJE			

Acceso a Navasoft: Módulo de Facturación Electrónica.			
Computadora	Imposibilidad de: acceso Navasoft Módulo VENTAS - EMISION COMPROBANTE DE PAGO y Módulo FINANCIERA - CANJE		
Red LAN	Imposibilidad de: accederá los sistemas internos y externos, dificultando un desempeño normal.		
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.	00:30	00:10
Impresora	Imposibilidad de: imprimir comprobante de pago.		
Internet (Correo electrónico)	Imposibilidad de: usar el correo electrónico.	01:00	00:45
SUPERVISOR DEL CREDITO			
Acceso a Navasoft: Módulo COMERCIAL CREDICON-SOLICITUD DE CREDITO	Imposibilidad de: Autorizar el desembolso de créditos en productos de la tienda y emitir el cronograma de pagos; además generar y entregar al cliente el cronograma de pagos del crédito.	01:00	00:45
Computadora	Imposibilidad de: acceso a Navasoft- Módulo COMERCIAL CREDICON-SOLICITUD DE CREDITO		
Red LAN	Imposibilidad de: acceder a los sistemas internos y externos, dificultando un desempeño normal.		
Internet (correo electrónico)	Imposibilidad de: usar el correo electrónico.		
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.	00:30	00:10
Impresora	Imposibilidad de: imprimir el cronograma de pagos del crédito.		
AUXILIAR DE DESPACHO			
Acceso a Navasoft: Módulo CAJERO VENTAS - DESPACHO	Imposibilidad de: Verificar la conformidad del comprobante de pago generado por el cajero y generar la GUIA DE REMISION en el sistema seleccionando el modelo, serie y características del producto a despachar.	01:00	00:45
Computadora	Imposibilidad de: acceso a Navasoft- Módulo CAJERO VENTAS – DESPACHO		
Red LAN	Imposibilidad de: acceder a los sistemas internos y externos, dificultando un desempeño normal.		
Internet (correo electrónico)	Imposibilidad de: usar el correo electrónico.		
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.	00:30	00:10
Impresora	Imposibilidad de: imprimir la guía de remisión.		

INDENTIFICAR LA PRIORIDAD EN EL RECUPERO DE LOS RECURSOS CRÍTICOS (basado en el impacto tras la caída y el tiempo objetivo de recuperación, usar valoración cualitativas: alto, medio, bajo)

RECURSOS	PRIORIDAD DE RECUPERO
NAVASOFT V5.0	ALTO
Computadora	ALTO
Fluido eléctrico	ALTO
Red LAN	ALTO
Impresora	ALTO
Internet	MEDIO

Tabla N° 29: Análisis del subproceso Amortización del Crédito.

AMORTIZACION DEL CREDITO		
NOMBRES DE SISTEMAS:	RESPONSABLE DEL BIA	CAJERO
NAVASOFT V5.0		
INDENTIFICAR CONCEPTOS CLAVE	**ROL**	
Interno*(identificar los usuarios , puestos de trabajo o áreas dentro de la empresa que tienen dependencia o dan soporte del sistema; especificar la relación con el sistema)*		
CAJERO	Declarar los sobrantes y faltantes de efectivo al cierre de su turno.	
	Mantener el compromiso de confidencialidad sobre los aportes realizados por los clientes y sobre la recaudación de CHANCAFE NORTE SAC	
	Verificar la autenticidad del dinero falso siguiendo las normas establecidas por CHANCAFE NORTE SAC.	
	Registrar los pagos en el sistema verificando la actualización automatizada de los saldos.	
	Emitir el voucher de pago de la cuota y/o total del crédito; y entregarle al cliente.	
	Hacer entrega diariamente al asistente de Tesorería los documentos físicos de las operaciones realizadas al cierre del turno.	
IDENTIFICAR RECURSOS DE SISTEMA (hardware , software y otros recursos)		
HARDWARE	**TIPO**	**CANTIDAD**
Servidores	Servidor de Comunicaciones	1
	Servidor de Base de Datos	1
Estaciones de trabajo		24
SOFTWARE	**TIPO**	**CANTIDAD**
Aplicativo	Navasoft : Módulo MODULO GESTION CUOTAS POR COBRAR	
	MICROSOFT OFFICE: EXCEL	
Sistema operativo	Windows 7 service pack 1	
OTROS RECURSOS		
Red LAN		
Internet (central de riesgos y correo electrónico)		

Fluido eléctrico	
Línea Telefónica	
Antivirus	
Impresora	
IDENTIFICAR ROLES CRITICOS	
CAJERO	Declarar los sobrantes y faltantes de efectivo al cierre de su turno.
	Emitir el voucher de pago de la cuota y/o total del crédito; y entregarle al cliente.
	Registrar los pagos en el sistema verificando la actualización automatizada de los saldos.
ENLAZAR ROLES CRITICOS A RECURSOS CRITICOS	
ROLES CRITICOS	**RECURSOS CRITICOS**
CAJERO	
Declarar los sobrantes y faltantes de efectivo al cierre de su turno.	Acceso a Navasoft: Módulo MODULO GESTION CUOTAS POR COBRAR
	Microsoft Excel
	Computadora
	Red LAN
Emitir el voucher de pago de la cuota y/o total del crédito; y entregarle al cliente.	Fluido eléctrico
Registrar los pagos en el sistema verificando la actualización automatizada de los saldos.	Impresora

IDENTIFICAR IMPACTOS Y TIEMPOS ACEPTABLES DE LA CAIDA
(identifica el periodo máximo de interrupción y el tiempo objetivo de recuperación)

RECURSO	IMPACTO TRAS CAIDA	TMI	TOR
CAJERO			
Acceso a Navasoft: Módulo MODULO GESTION CUOTAS POR COBRAR	Imposibilidad de: Emitir el voucher de pago de la cuota y/o total del crédito; y entregarle al cliente; registrar los pagos en el sistema verificando la actualización automatizada de los saldos.	00:30	00:20
Microsoft Excel	Imposibilidad de: declarar los sobrantes y faltantes de efectivo al cierre de su turno.	00:30	00:20
Red LAN	Imposibilidad de: acceder a los sistemas internos y externos, dificultando un desempeño normal.	00:30	00:20
Computadora	Imposibilidad de: acceso a Navasoft- Módulo MODULO GESTION CUOTAS POR COBRAR	00:30	00:20
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.	00:30	00:10
Impresora	Imposibilidad de: el voucher de pago de la cuota y/o total del crédito	00:45	00:30

INDENTIFICAR LA PRIORIDAD EN EL RECUPERO DE LOS RECURSOS CRÍTICOS (basado en el impacto tras la caída y el tiempo objetivo de recuperación, usar valoración cualitativas: alto, medio, bajo)	
RECURSOS	**PRIORIDAD DE RECUPERO**
NAVASOFT V5.0	ALTO
Computadora	ALTO
Fluido eléctrico	ALTO
Red LAN	ALTO
Microsoft Excel	ALTO
Impresora	MEDIO

Tabla N° 30: Análisis del subproceso Recuperación del crédito.

RECUPERACION DEL CREDITO		
NOMBRES DE SISTEMAS:	RESPONSABLE DEL BIA	JEFE DE COBRANZA
NAVASOFT V5.0		GESTOR DE COBRANZA
INDENTIFICAR CONCEPTOS CLAVE	**ROL**	
Interno*(identificar los usuarios , puestos de trabajo o áreas dentro de la empresa que tienen dependencia o dan soporte del sistema; especificar la relación con el sistema)*		
JEFE DE COBRANZAS	Programar, dirigir y controlar la gestión de recuperaciones de créditos en las carteras de cobranzas de cartera vencida y judicial, procurando que los índices de morosidad estés por debajo de lo permitido.	
	Ejecutar seguimiento diario a la cobranza realizada en cada agencia en coordinación con los gestores de cobranza, verificando el estado del crédito, fechas de pago.	
	Controlar la labor diaria del gestor de recuperaciones evaluando los informes y disponiendo las medidas más oportunas a fin de lograr eficiencia y productividad en la recuperación de las carteras.	
	Realizar la lista de productos a embargar de acuerdo a la política de recuperación de cartera morosa y entregarla a cada gestor de cobranza para el recojo de los productos de la misma.	
	Registrar el recupero de los productos embargados y el estado de los mismos.	
	Informar a la gerencia general sobre las irregularidades presentadas en la gestión de recuperación con el fin de que se tomen las medidas correctivas.	
GESTOR DE COBRANZA	Comunicar e informar a los deudores titulares y/o avales el vencimiento de sus cuotas y el monto de la mora acumulada.	

	Comunicar al deudor y/o avales por escrito el vencimiento de sus cuotas y solicitar el pago de la cuota vencida.	
	Embargar los productos de los créditos indicados por el JEFE DE COBRANZA e informar sobre el estado de los mismos.	
	Entregar las cartas de cobranza extrajudicial a los clientes que mantienen créditos vencidos y visitar a clientes que ameritan una gestión directa.	
IDENTIFICAR RECURSOS DE SISTEMA (hardware , software y otros recursos)		
HARDWARE	**TIPO**	**CANTIDAD**
Servidores	Servidor de Comunicaciones	1
	Servidor de Base de Datos	1
	Servidor de aplicaciones	
Estaciones de trabajo		28
SOFTWARE	**TIPO**	**CANTIDAD**
Aplicativo	Navasoft : MODULO DE GESTION CUOTAS POR COBRAR	
	MICROSOFT OFFICE: EXCEL	
	Aplicación web: MODULO COMPLEMENTARIO	
Sistema operativo	Windows 7 service pack 1	
OTROS RECURSOS		
Red LAN		
Internet (correo electrónico)		
Fluido eléctrico		
Línea Telefónica		
Antivirus		
Impresora		
IDENTIFICAR ROLES CRITICOS		
JEFE DE COBRANZA	Programar, dirigir y controlar la gestión de recuperaciones de créditos en las carteras de cobranzas de cartera vencida y judicial, procurando que los índices de morosidad estén por debajo de lo permitido.	
	Ejecutar seguimiento diario a la cobranza realizada en cada agencia en coordinación con los gestores de cobranza, verificando el estado del crédito, fechas de pago.	
	Controlar la labor diaria del gestor de recuperaciones evaluando los informes y disponiendo las medidas más oportunas a fin de lograr eficiencia y productividad en la recuperación de las carteras.	
	Realizar la lista de productos a embargar de acuerdo a la política de recuperación de cartera morosa y entregarla a cada gestor de cobranza para el recojo de los productos de la misma.	
	Registrar el recupero de los productos embargados y el estado de los mismos.	

GESTOR DE COBRANZA	Comunicar e informar a los deudores titulares y/o avales el vencimiento de sus cuotas y el monto de la mora acumulada.
	Comunicar al deudor y/o avales por escrito el vencimiento de sus cuotas y solicitar el pago de la cuota vencida.
	Embargar los productos de los créditos indicados por el JEFE DE COBRANZA e informar sobre el estado de los mismos.
ENLAZAR ROLES CRITICOS A RECURSOS CRITICOS	
ROLES CRITICOS	**RECURSOS CRITICOS**
JEFE DE COBRANZA	
Programar, dirigir y controlar la gestión de recuperaciones de créditos en las carteras de cobranzas de cartera vencida y judicial, procurando que los índices de morosidad estén por debajo de lo permitido.	Acceso a Navasoft: Módulo de GESTION CUOTAS POR COBRAR
	Aplicación web: MODULO COMPLEMENTARIO
Ejecutar seguimiento diario a la cobranza realizada en cada agencia en coordinación con los gestores de cobranza, verificando el estado del crédito, fechas de pago.	Microsoft Excel
Controlar la labor diaria del gestor de recuperaciones evaluando los informes y disponiendo las medidas más oportunas a fin de lograr eficiencia y productividad en la recuperación de las carteras.	Computadora
Registrar el recupero de los productos embargados y el estado de los mismos.	Fluido eléctrico
Realizar la lista de productos a embargar de acuerdo a la política de recuperación de cartera morosa y entregarla a cada gestor de cobranza para el recojo de los productos de la misma.	Internet (correo electrónico)
GESTOR DE COBRANZA	
Comunicar e informar a los deudores titulares y/o avales el vencimiento de sus cuotas y el monto de la mora acumulada.	Microsoft Excel
	Telefonía Móvil

	Computadora
	Fluido eléctrico
Comunicar al deudor y/o avales por escrito el vencimiento de sus cuotas y solicitar el pago de la cuota vencida.	Impresora
Embargar los productos de los créditos indicados por el JEFE DE COBRANZA e informar sobre el estado de los mismos.	Internet (correo electrónico)

IDENTIFICAR IMPACTOS Y TIEMPOS ACEPTABLES DE LA CAIDA
(identifica el periodo máximo de interrupción y el tiempo objetivo de recuperación)

RECURSO	IMPACTO TRAS CAIDA	TMI	TOR
JEFE DE COBRANZA			
Acceso a Navasoft: Módulo de GESTION CUOTAS POR COBRAR	Imposibilidad de: acceder al estado de crédito de los clientes y ejecutar la cobranza.	00:20	00:10
	Imposibilidad de: identificar a aquellos clientes que ameriten una gestión directa.		
Aplicación web: MODULO COMPLEMENTARIO	Imposibilidad de: Registrar los datos y estado de los productos embargados.	00:45	00:30
Microsoft Excel	Imposibilidad de: realizar la lista de clientes que ameritan gestión de cobranza y/o embargo.	00:20	00:10
Computadora	Imposibilidad de : acceso a Navasoft: Módulo de GESTION CUOTAS POR COBRAR	00:30	00:10
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.		
Internet (correo electrónico)	Imposibilidad de: usar el correo electrónico.	01:00	00:45
GESTOR DE COBRANZA			
Microsoft Excel	Imposibilidad de: visualizar la lista de	00:20	00:10

	clientes que ameritan gestión de cobranza y/o embargo.		
Telefonía Móvil	Imposibilidad de: comunicar e informar a los deudores titulares y/o avales el vencimiento de sus cuotas y el monto de la mora acumulada.	01:00	00:45
Computadora	Imposibilidad de registrar, a través de herramientas ofimáticas, las gestiones diarias realizadas.	00:20	00:10
Fluido eléctrico	Imposibilidad de: Acceder a los dispositivos eléctricos que facilitan las operaciones.		
Impresora	Imposibilidad de: imprimir reportes y notificaciones a los clientes deudores.	00:20	00:10
Internet (correo electrónico)	Imposibilidad de: usar el correo electrónico.	01:00	00:45

INDENTIFICAR LA PRIORIDAD EN EL RECUPERO DE LOS RECURSOS CRÍTICOS (basado en el impacto tras la caída y el tiempo objetivo de recuperación, usar valoración cualitativas: alto, medio, bajo)	
RECURSOS	**PRIORIDAD DE RECUPERO**
NAVASOFT V5.0	ALTO
MODULO COMPLEMENTARIO	ALTO
Computadora	ALTO
Fluido eléctrico	ALTO
Red LAN	ALTO
Microsoft Excel	ALTO
Impresora	ALTO
Internet (correo electrónico)	MEDIO

A partir de lo anterior se ha identificado los siguientes activos de TI que le dan soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE SAC.

Tabla N° 31: Inventario de activos de TI de los procesos de Evaluación, Financiamiento y Cobranza.

N°	ACTIVO
1	Servidor: comunicaciones (principal)
2	Servidor: base de datos principal y aplicaciones
3	Red para comunicaciones: gabinetes, switch central y de borde, firewall
4	Data center o sala de servidores
5	Bases de datos alternas
6	Backups de base de datos
7	Personal de área de TI : jefatura y asistentes.
8	Aplicaciones informáticas de créditos y cobranzas: NAVASOT y programa complementario.
9	Correo electrónico de la institución.
10	Equipos de cómputo para terminales de cajeros y vendedores
11	Código fuente de las aplicaciones
12	Desarrolladores de sistemas : encargados del desarrollo de los requerimientos
13	Equipos de cómputo de los desarrolladores de sistemas: hardware.
14	Backups de desarrollo y mantenimiento: código fuente
15	Herramientas de desarrollo
16	Registros de control de cambios de las aplicaciones: manuales de usuarios, pruebas , scripts.

Utilizando la clasificación propuesta de MAGERIT, se tiene el siguiente resultado:

Tabla N° 32: Clasificación de los activos de TI identificados.

N°	Tipo de activo	Activo	CODIGO
1	[COM] Redes de comunicaciones	Red de comunicaciones	**ACT1**
2	[D] Datos / Información	Código fuente de las aplicaciones	**ACT2**
3	[D] Datos / Información	Registros de control de cambios de las aplicaciones: manuales de usuarios, pruebas , scripts.	**ACT3**
4	[D] Datos / Información	Bases de Datos.	**ACT4**
5	[HW] Equipamiento informático (hardware)	Equipos de cómputo para terminales de cajeros y vendedores	**ACT5**
6	[HW] Equipamiento informático (hardware)	Equipos de cómputo de los desarrolladores de sistemas: hardware.	**ACT6**
7	[L] Instalaciones	Data center o sala de servidores	**ACT7**
8	[Media] Soportes de información	Backups de desarrollo y mantenimiento: código fuente.	**ACT8**
9	[Media] Soportes de información	Backups de base de datos	**ACT9**
10	[P] Personal	Personal de área de TI : jefatura y asistentes.	**ACT10**
11	[P] Personal	Desarrolladores de sistemas : encargados del desarrollo de los requerimientos	**ACT11**
12	[S] Servicios	Servidor: comunicaciones (principal)	**ACT12**

13	[S] Servicios	Servidor: base de datos y aplicaciones (principal)	**ACT13**
14	[S] Servicios	Correo electrónico de la institución.	**ACT14**
15	[SW] Software - Aplicaciones informáticas	Herramientas de desarrollo	**ACT15**
16	[SW] Software - Aplicaciones informáticas	Aplicaciones informáticas de créditos y cobranzas: NAVASOT y programa complementario.	**ACT16**

4.2 Clasificar y priorizar los activos de acuerdo a su criticidad.

Una vez inventariados los activos de TI se ha valorado y clasificado su nivel de importancia o criticidad, tomando como base la calificación dada a cada característica o dimensión de seguridad de la información, de acuerdo a las escalas de valoración propuestas, obteniéndose los siguientes resultados:

Tabla N° 33: Valoración del nivel de criticidad de los activos de TI identificados.

N°	Activo (CODIGO)	Criterios de seguridad					Total	Nivel de criticidad
		Confidencialidad	Integridad	Disponibilidad	Autenticidad	Trazabilidad		
1	**ACT1**	4	1	5	1	4	3	Medio
2	**ACT2**	4	5	5	5	4	4	Alto
3	**ACT3**	4	4	5	4	4	4	Alto
4	**ACT4**	5	5	5	5	5	5	Muy alto
5	**ACT5**	5	5	5	5	5	5	Muy alto
6	**ACT6**	4	5	5	5	4	4	Alto
7	**ACT7**	4	1	5	1	4	3	Medio
8	**ACT8**	4	5	5	5	4	4	Alto
9	**ACT9**	5	5	5	5	5	5	Muy alto
10	**ACT10**	4	1	5	1	4	3	Medio
11	**ACT11**	4	1	5	1	4	3	Medio
12	**ACT12**	4	5	5	5	4	4	Alto
13	**ACT13**	5	5	5	5	5	5	Muy alto
14	**ACT14**	4	4	5	4	4	4	Alto
15	**ACT15**	3	4	4	4	3	3	Medio
16	**ACT16**	4	4	5	4	4	4	Alto

4.3 Identificación de las amenazas de los activos de TI

Para cada activo de TI se han identificado las siguientes amenazas:

Tabla N° 34: Listado de amenazas por Activo de TI.

N°	Activo (CODIGO)	Amenaza	CODIGO
1	**ACT1**	Paralización del servicio (comunicaciones)	**AME1**
2	**ACT2**	Pérdida de la correlación o continuidad del código fuente de la versión actual en producción de sistemas.	**AME2**
		Multas, penalizaciones y pérdida de información a causa de los cambios en el códigos fuente en beneficio del trabajador	**AME3**
3	**ACT3**	No ser posible determinar el origen o la fuente de los cambios en el código fuente.	**AME4**

4	**ACT4**	Sanciones, penalizaciones y/o multas. Información sensible y relevante de la empresa que no se pueda recuperar a causa de accesos no adecuados a las bases de datos.	**AME5**
		Insuficiente espacio de almacenamiento.	**AME6**
5	**ACT5**	Información sensible que no se pueda recuperar a causa de fallas de equipos de cómputo que cumplen con la función de ser el soporte de los procesos del negocio.	**AME7**
6	**ACT6**	Prórrogas de tiempo en las actividades, pérdida de recursos o retrasos en las actividades a causa de infección de virus informáticos.	**AME8**
7	**ACT7**	Sabotaje a las instalaciones.	**AME9**
		Robo o sustracción de activos de TI del cuarto de servidores (costo de hardware / paralización de las Operaciones)	**AME10**
8	**ACT8**	No ser posible reestablecer las adecuaciones a los sistemas.	**AME11**
9	**ACT9**	Detenimiento de los procesos, debido a la pérdida de información importante por la falta de protección en los dispositivos donde se almacenan.	**AME12**
10	**ACT10**	Extender en tiempo las actividades, detenimiento de los procesos, pérdida de información importante debido a fuga de recurso humano.	**AME13**
		Alteración de la integridad, divulgación y destrucción de la información	**AME14**
11	**ACT11**	Los tiempos de desarrollo para los requerimientos incumplen el cronograma establecido para las actividades.	**AME15**
		Información importante que no se pueda recuperar debido a fuga por medio de correos electrónicos y/o sitios de internet.	**AME16**
		Recursos que no se puedan recuperar a causa de las implementaciones no alineadas a una metodología y estándares de desarrollo de Software.	**AME17**
12	**ACT12**	No se puede acceder a los servicios de red en consecuencia a la paralización de procesos y/o actividades del negocio.	**AME18**
13	**ACT13**	Pérdida de recursos, penalizaciones y multas a causa de la modificación de información importante.	**AME19**
14	**ACT14**	No cumplir con los tiempos asignados a las actividades a causa de las caídas en el servicio de correo electrónico	**AME20**
		No poder recuperar datos a causa de la administración no adecuada del servidor de correo electrónico por parte del proveedor.	**AME21**
15	**ACT15**	Desarrollo de requerimientos paralizados.	**AME22**
16	**ACT16**	Procesos paralizados debido a errores en el procesamiento de movimientos y/o transacciones a nivel de usuario/cliente.	**AME23**
		No brindar información exacta al personal involucrado en el negocio para el desarrollo de los procesos en consecuencia a errores en la integridad de los datos.	**AME24**

4.4 Listado de vulnerabilidades por Activo de TI – Amenaza

Las vulnerabilidades obtenidas de los datos recopilados en el levantamiento de la información de la empresa ya que son factores internos de la misma son:

Tabla N° 35: Listado de vulnerabilidades por Activo de TI.

N°	Activo (CODIGO)	Amenaza (CODIGO)	Vulnerabilidad	CODIGO
1	**ACT1**	**AME1**	Falla de sede central de comunicaciones	**VULN1**
			Falla en la red de comunicaciones de otras tiendas	**VULN2**
			Interrupción de los procesos debido a fallas eléctricas	**VULN3**
			No se dispone de firewall a nivel de hardware	**VULN4**
2	**ACT2**	**AME2**	No se hacen copias de seguridad	**VULN5**
			Accesos sin autorización a la computadora donde se realiza la consolidación de Software	**VULN6**
		AME3	Acceso totalizado al código fuente sin restricciones por parte de los desarrolladores.	**VULN7**
			Los controles de cambios entregados por el analista de desarrollo no se revisan a detalle.	**VULN8**
			Contraseñas no complejas o básicas en el respaldo de código fuente	**VULN9**
			Alteración del desarrollo de un proceso a causa de la manipulación del código fuente.	**VULN10**
3	**ACT3**	**AME4**	No poder identificar a los responsables de los cambios o modificaciones que se les asigna a los analistas de desarrollo.	**VULN11**
4	**ACT4**	**AME5**	Asignación de perfiles a los usuarios para acceder a la Base de datos sin un adecuado procedimiento.	**VULN12**
			Existencia de contraseñas que son fáciles de averiguar o no son adecuadas para usuarios locales y de red	**VULN13**
			Los privilegios de accesos a las aplicaciones que no son revisados periódicamente.	**VULN14**
			Ingreso o acceso a la base de datos por medio de otras aplicaciones	**VULN15**
			Virus y ataques informáticos	**VULN16**
			Copias de la Base de Datos sin autorización o permiso.	**VULN17**
			Modificación sin permiso o no autorizada de la base de datos.	**VULN18**
		AME6	Incremento de transacciones o movimientos.	**VULN19**
			No tener estipulado un procedimiento para el mantenimiento de base de datos.	**VULN20**
			Incremento de espacio por virus.	**VULN21**
5	**ACT5**	**AME7**	Personal no autorizado, ni instruido , ni capacitado para el mantenimiento de equipos de computo	**VULN22**
			Desconocimiento del periodo útil de los equipos.	**VULN23**
			Faltar o no cumplir el plan de mantenimiento de equipos.	**VULN24**
			Fallas en el sistema eléctrico.	**VULN25**
			Problemas de configuración de los equipos	**VULN26**
			Incorrecta manipulación de equipo por parte del usuario	**VULN27**
			Carencia de condiciones ambientales adecuadas	**VULN28**
			No se reconocen o identifican los equipos más importantes o críticos	**VULN29**

			El personal guarda información relevante en sus equipos pero no lo hace en el servidor.	**VULN30**
6	**ACT6**	**AME8**	Acceso totalizado a la Web	**VULN31**
7	**ACT7**	**AME9**	Ingreso no autorizado de personal a la sala de servidores.	**VULN32**
			No contar con un sistema de seguridad de los equipos que se encuentran en la sala de servidores.	**VULN33**
		AME10	No llevar un registro de acceso a las áreas restringidas	**VULN34**
			No tener un registro de acceso a la sala o cuarto de servidores	**VULN35**
			No tener un procedimiento para el control al personal encargado del mantenimiento en la empresa.	**VULN36**
			El personal de seguridad no lleva el control de los equipos del personal de mantenimiento que entran o salen.	**VULN37**
8	**ACT8**	**AME11**	No se trasladan a sitios alternos las copias de respaldo.	**VULN38**
9	**ACT9**	**AME12**	Falla en los discos duros del servidor	**VULN39**
			No contar con un lugar para la custodia de las copias de respaldo.	**VULN40**
			Errores al generar backups	**VULN41**
			Los backups no se registran o se controlan.	**VULN42**
10	**ACT10**	**AME13**	Segregación de funciones deficiente.	**VULN43**
			Sin plan de capacitación adecuado.	**VULN44**
			Situaciones que impiden o limitan al personal realizar sus actividades.	**VULN45**
		AME14	Exceso de privilegios en los accesos	**VULN46**
			Sin seguimiento de accesos	**VULN47**
			Sin acuerdos de confidencialidad	**VULN48**
			Actuar del personal de manera no normal en el desarrollo de sus responsabilidades.	**VULN49**
			No contar con un procedimiento en cuanto al mantenimiento de usuarios	**VULN50**
11	**ACT11**	**AME15**	Personal nuevo de desarrollo con nulo o poco conocimiento de los procesos del negocio.	**VULN51**
			Sobrecarga de requerimientos a desarrollar por poco personal.	**VULN52**
		AME16	No control de correos entrantes o salientes.	**VULN53**
			Acceso total a la Web	**VULN54**
		AME17	Inducción no adecuada.	**VULN55**
12	**ACT12**	**AME18**	Personal no especializado ni capacitado en el mantenimiento al servidor.	**VULN56**
			Error en los elementos físicos.	**VULN57**
			Error en el sistema operativo o parches.	**VULN58**
			Sin plan de mantenimiento de los servidores	**VULN59**
			Ataque de virus informáticos.	**VULN60**
13	**ACT13**	**AME19**	Acceso de manera totalizada a la base de datos y modificaciones por parte del Administrador	**VULN61**
			Diseño de base datos deficiente.	**VULN62**
			Acceso por canales no autorizados a la base de datos.	**VULN63**

14	**ACT14**	**AME20**	Problemas de conectividad con el servicio que brinda el proveedor.	**VULN64**
		AME21	Sin copias de respaldo (cuentas creadas, permisos y configuración)	**VULN65**
			Poca capacidad de almacenamiento.	**VULN66**
			Eliminación de cuentas debido a accesos no autorizados por parte del administrador.	**VULN67**
			Contraseñas no complejas.	**VULN68**
15	**ACT15**	**AME22**	Respaldo de copia de seguridad en lugares no seguros	**VULN69**
16	**ACT16**	**AME23**	Registro de información errónea por parte del usuario.	**VULN70**
			Error en la conectividad de red o en equipo de computo	**VULN71**
			Error en el sistema eléctrico.	**VULN72**
		AME24	Falta de soporte al sistema.	**VULN73**
			Sin control de las versiones del código fuente	**VULN74**

4.5 Determinación del apetito y la tolerancia al riesgo de TI

CHANCAFE NORTE SAC ha estipulado dos objetivos estratégicos u operacionales, el cual se tiene de conocimiento que la infraestructura tecnológica con la que cuenta da soporte a dichos objetivos:

1. Mejora en los procesos de la gestión créditos
   - Mejorar los procesos de gestión de aprobación, desembolso, amortización y recuperación del crédito.
2. Gestión del recurso humanos
   - Concientizar y fidelizar al recurso humano con la seguridad de la información.

Tabla N° 36: Estrategias de TI por cada objetivo estratégico u operacional de la empresa

Objetivo Estratégico u Operacional de la Empresa	**Estrategia relacionada con TI**
Mejorar los procesos de gestión de aprobación, desembolso, amortización y recuperación del crédito.	- Gestionar proyectos o actividades de tecnologías de información para dar soporte a la seguridad de la información de los procesos que involucran la gestión del crédito. - Mejorar las aplicaciones informáticas para la supervisión y el control con objetivos de mitigar los riesgos operacionales. - Implementar sistemas de comunicación para las nuevas tiendas.
Fidelizar el personal relacionado con las tecnologías de información.	- Entrenamiento e instrucción de los usuarios y del personal de TI - Concientización del personal referente a la seguridad de la información - Plan de incentivos y sanciones en relación al cumplimiento de políticas de seguridad de TI, gestión de riesgos y

	continuidad de procesos de TI

El apetito y tolerancia al riesgo se determina para cada uno de dichos objetivos:

Tabla N° 37: Determinación del apetito y la tolerancia al riesgo de TI por cada objetivo estratégico u operacional.

OBJETIVO OPERACIONAL	Mejorar los procesos de gestión de aprobación, desembolso, amortización y recuperación del crédito.	
Apetito de riesgo	– Causa el incumplimiento leve de una regulación – Causa una merma en la seguridad – de bajo interés para la competencia – bajo valor comercial – Causa interrupción de los servicios propios de CHANCAFE NORTE SAC – Dificulta la investigación de delitos – 1 hora < TOR < 4 horas	
Tolerancia de riesgo	– Causa el incumplimiento de una regulación – Causa un grave incidente de seguridad – de cierto interés para la competencia o – cierto valor comercial – Causa interrupción de los servicios propios de CHANCAFE NORTE SAC con impacto en otras entidades o en los clientes – Dificulta la investigación de delitos – 4 horas < TOR < 1 día	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física	Alto	Frecuente
Personal de TI	Medio	Normal
Gestión de proyectos	Bajo	Muy poco frecuente
Gestión de la seguridad	Bajo	Normal
Entrega y soporte de servicios de TI	Muy alto	Muy frecuente
Aplicaciones	Muy alto	Muy frecuente
Cumplimiento corporativo	Bajo	Poco frecuente
Cumplimiento legal	Bajo	Muy poco frecuente
Otros escenarios	Alto	Frecuente

OBJETIVO OPERACIONAL	Concientizar y fidelizar al recurso humano con la seguridad de la información.	
Apetito de riesgo	– Causa el incumplimiento leve de una regulación – Causa una merma en la seguridad – Disminuye la eficacia o seguridad de la misión operativa de manera local – Impide la operación efectiva de una parte de CHANCAFE NORTE SAC – Dificulta la investigación de delitos	
Tolerancia de riesgo	– Causa el incumplimiento de una regulación – Causa un grave incidente de seguridad – Disminuye la eficacia o seguridad de la misión operativa, repercute fuera del área local. – Impide la operación efectiva de más de una parte de CHANCAFE NORTE SAC – Dificulta la investigación de delitos	
Escenario de Riesgo de TI	**Impacto**	**Probabilidad de ocurrencia**
Infraestructura física	Bajo	Poco frecuente
Personal de TI	Muy alto	Frecuente
Gestión de proyectos	Muy bajo	Poco frecuente
Gestión de la seguridad	Alto	Normal
Entrega y soporte de servicios de TI	Bajo	Muy poco frecuente
Aplicaciones	Alto	Frecuente
Cumplimiento corporativo	Alto	Frecuente
Cumplimiento legal	Medio	Frecuente

4.6 Valoración del impacto y probabilidad de ocurrencia de las amenazas

Para la valoración del impacto y probabilidad de ocurrencia, y, en consecuencia, para obtener el nivel de riesgo al que está expuesto cada activo de TI, se realizó un levantamiento de información para evaluar los controles existentes actualmente y la efectividad de su implementación. El resultado se muestra a continuación:

Tabla N° 38: Valoración del Nivel de Riesgo Intrínseco (NRI).

N°	Activo (CODIGO)	Amenaza (CODIGO)	Vulnerabilidad (CODIGO)	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco (NRI)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
1	**ACT1**	**AME1**	**VULN1**	5	Muy alto	3	Normal	RI1	4	Alto
			VULN2	4	Alto	4	Frecuente	RI2	4	Alto
			VULN3	4	Alto	3	Normal	RI3	3	Medio
			VULN4	3	Medio	2	Poco frecuente	RI4	2	Bajo
2	**ACT2**	**AME2**	**VULN5**	4	Alto	2	Poco frecuente	RI5	2	Bajo
			VULN6	4	Alto	2	Poco frecuente	RI6	2	Bajo
		AME3	**VULN7**	4	Alto	3	Normal	RI7	3	Medio
			VULN8	4	Alto	3	Normal	RI8	3	Medio
			VULN9	3	Medio	3	Normal	RI9	3	Medio
			VULN10	5	Muy alto	4	Frecuente	RI10	5	Muy alto
3	**ACT3**	**AME4**	**VULN11**	3	Medio	3	Normal	RI11	3	Medio
4	**ACT4**	**AME5**	**VULN12**	4	Alto	3	Normal	RI12	3	Medio
			VULN13	3	Medio	2	Poco frecuente	RI13	2	Bajo
			VULN14	3	Medio	2	Poco frecuente	RI14	2	Bajo
			VULN15	4	Alto	3	Normal	RI15	3	Medio
			VULN16	3	Medio	3	Normal	RI16	3	Medio
			VULN17	4	Alto	3	Normal	RI17	3	Medio
			VULN18	5	Muy alto	4	Frecuente	RI18	5	Muy alto
		AME6	**VULN19**	3	Medio	3	Normal	RI19	3	Medio
			VULN20	3	Medio	2	Poco frecuente	RI20	2	Bajo
			VULN21	3	Medio	1	Muy poco frecuente	RI21	1	Muy bajo
5	**ACT5**	**AME7**	**VULN22**	4	Alto	2	Poco frecuente	RI22	2	Bajo

			VULN23	2	Bajo	2	Poco frecuente	RI23	2	Bajo
			VULN24	2	Bajo	3	Normal	RI24	2	Bajo
			VULN25	3	Medio	3	Normal	RI25	3	Medio
			VULN26	2	Bajo	3	Normal	RI26	2	Bajo
			VULN27	3	Medio	4	Frecuente	RI27	3	Medio
			VULN28	2	Bajo	3	Normal	RI28	2	Bajo
			VULN29	3	Medio	2	Poco frecuente	RI29	2	Bajo
			VULN30	4	Alto	4	Frecuente	RI30	4	Alto
6	**ACT6**	**AME8**	**VULN31**	3	Medio	3	Normal	RI31	3	Medio
7	**ACT7**	**AME9**	**VULN32**	5	Muy alto	3	Normal	RI32	4	Alto
			VULN33	3	Medio	3	Normal	RI33	3	Medio
		AME10	**VULN34**	2	Bajo	3	Normal	RI34	2	Bajo
			VULN35	3	Medio	3	Normal	RI35	3	Medio
			VULN36	2	Bajo	3	Normal	RI36	2	Bajo
			VULN37	4	Alto	3	Normal	RI37	3	Medio
8	**ACT8**	**AME11**	**VULN38**	5	Muy alto	3	Normal	RI38	4	Alto
9	**ACT9**	**AME12**	**VULN39**	4	Alto	3	Normal	RI39	3	Medio
			VULN40	2	Bajo	2	Poco frecuente	RI40	2	Bajo
			VULN41	5	Muy alto	4	Frecuente	RI41	5	Muy alto
			VULN42	3	Medio	3	Normal	RI42	3	Medio
10	**ACT10**	**AME13**	**VULN43**	3	Medio	2	Poco frecuente	RI43	2	Bajo
			VULN44	2	Bajo	3	Normal	RI44	2	Bajo
			VULN45	2	Bajo	3	Normal	RI45	2	Bajo
		AME14	**VULN46**	4	Alto	3	Normal	RI46	3	Medio
			VULN47	5	Muy alto	3	Normal	RI47	4	Alto
			VULN48	4	Alto	3	Normal	RI48	3	Medio
			VULN49	3	Medio	3	Normal	RI49	3	Medio

			VULN50	3	Medio	2	Poco frecuente	RI50	2	Bajo
11	**ACT11**	**AME15**	**VULN51**	2	Bajo	4	Frecuente	RI51	2	Bajo
			VULN52	3	Medio	3	Normal	RI52	3	Medio
		AME16	**VULN53**	3	Medio	2	Poco frecuente	RI53	2	Bajo
			VULN54	4	Alto	3	Normal	RI54	3	Medio
		AME17	**VULN55**	2	Bajo	2	Poco frecuente	RI55	2	Bajo
12	**ACT12**	**AME18**	**VULN56**	3	Medio	2	Poco frecuente	RI56	2	Bajo
			VULN57	4	Alto	3	Normal	RI57	3	Medio
			VULN58	5	Muy alto	4	Frecuente	RI58	5	Muy alto
			VULN59	3	Medio	2	Poco frecuente	RI59	2	Bajo
			VULN60	2	Bajo	2	Poco frecuente	RI60	2	Bajo
13	**ACT13**	**AME19**	**VULN61**	4	Alto	4	Frecuente	RI61	4	Alto
			VULN62	2	Bajo	3	Normal	RI62	2	Bajo
			VULN63	5	Muy alto	4	Frecuente	RI63	5	Muy alto
14	**ACT14**	**AME20**	**VULN64**	3	Medio	3	Normal	RI64	3	Medio
		AME21	**VULN65**	3	Medio	3	Normal	RI65	3	Medio
			VULN66	2	Bajo	2	Poco frecuente	RI66	2	Bajo
			VULN67	3	Medio	2	Poco frecuente	RI67	2	Bajo
			VULN68	3	Medio	3	Normal	RI68	3	Medio
15	**ACT15**	**AME22**	**VULN69**	3	Medio	3	Normal	RI69	3	Medio
16	**ACT16**	**AME23**	**VULN70**	3	Medio	3	Normal	RI70	3	Medio
			VULN71	3	Medio	3	Normal	RI71	3	Medio
			VULN72	4	Alto	3	Normal	RI72	3	Medio
		AME24	**VULN73**	3	Medio	2	Poco frecuente	RI73	2	Bajo
			VULN74	4	Alto	3	Normal	RI74	3	Medio

4.7 Identificación de los controles o salvaguardas.

Después de haber determinado los niveles de riesgo intrínseco, se procedió a definir las salvaguardas necesarias para el tratamiento de los mismos, y a la vez identificando la estrategia de su implementación.

Tabla N° 39: Identificación de los controles y salvaguardas de acuerdo al Nivel de Riesgo Intrínseco (NRI).

Nivel de Riesgo Intrínseco (NRI)			Control o salvaguarda		Estrategia de implementación
ID riesgo	Nivel	Categoría	Descripción	CODIGO	
RI1	4	Alto	Contar con un plan de contingencia para comunicaciones.	CO1	Estrategia de trasladar el riesgo a terceros
			Contar con reporte de averías como entregable de un sistema de monitoreo y escaneo de la red.	CO2	Estrategia de prevenir el aumento del riesgo
RI2	4	Alto	Gestionar y documentar los incidentes de la red mediante la implementación de un procedimiento formal.	CO3	Estrategia de prevenir el aumento del riesgo
RI3	3	Medio	La empresa cuenta con UPS, que le permite a los equipos seguir operando frente a una posible paralización o corte de energía eléctrica.	CO4	Estrategia de elegir el control
			Evaluar el funcionamiento de los equipos eléctricos mediante un plan de pruebas de operatividad.	CO5	Estrategia de prevenir el aumento del riesgo
			Planificación del mantenimiento del sistema eléctrico	CO6	Estrategia de prevenir el aumento del riesgo
RI4	2	Bajo	Contar a nivel de software con un cortafuergo.	CO7	Estrategia de elegir el control
RI5	2	Bajo	Los procesos de desarrollo de software se deben controlar por medio de la asignación de base de datos y código fuente relacionado con el requerimiento que se asigna.	CO8	Estrategia de prevenir el aumento del riesgo
			Implementar un procedimiento para la realización de backups de la información que se guarda en los terminales de desarrollo, las versiones deben ser controladas.	CO9	Estrategia de prevenir el aumento del riesgo
RI6	2	Bajo	Las pruebas de las modificaciones de código deben ser controladas en ambientes idóneos.	CO10	Estrategia de prevenir el aumento del riesgo
			La computadora de integración de desarrollo estará de forma independiente a la de la red de producción	CO11	Estrategia de prevenir el aumento del riesgo

			Realizar copias de respaldo del código fuente	CO12	Estrategia de prevenir el aumento del riesgo
RI7	3	Medio	Los procesos de desarrollo de software deben ser monitoreados por medio de la asignación de base de datos y código fuente relacionado con el requerimiento que se asigna.	CO13	Estrategia de prevenir el aumento del riesgo
RI8	3	Medio	Detallar todo lo que se cambia a nivel de código fuente, base de datos por medio de la documentación.	CO14	Estrategia de prevenir el aumento del riesgo
			Generar pruebas de integración y unitarias con la finalidad de asegurar la calidad en el desarrollo de software antes del pase a producción., documentarlas.	CO15	Estrategia de prevenir el aumento del riesgo
			Los usuarios finales deben intervenir en la certificación y validación del módulo antes de la puesta a producción y como parte de la prueba de calidad de software.	CO16	Estrategia de prevenir el aumento del riesgo
RI9	3	Medio	Generar contraseñas seguras en la reserva de copias de seguridad de los código fuente en desarrollo.	CO17	Estrategia de prevenir el aumento del riesgo
RI10	5	Muy alto	Implementar una política de que el personal de desarrollo y cambios sea diferente al de testeo.	CO18	Estrategia de prevenir el aumento del riesgo
			Detallar todo lo que se cambia a nivel de código fuente, base de datos por medio de la documentación.	CO19	Estrategia de prevenir el aumento del riesgo
			Revisar que el nuevo código no tenga incorporado código malicioso.	CO20	Estrategia de prevenir el aumento del riesgo
RI11	3	Medio	Se deben registrar los cambios (scripts, carga de datos, cambios en la base, registrar hardware en el inventario junto con sus configuraciones) ocurridos mediante la implementación de la Gestión de cambios de software.	CO21	Estrategia de prevenir el aumento del riesgo
RI12	3	Medio	Reglamentar la administración de asignaciones de usuarios a los sistemas por medio de perfiles.	CO22	Estrategia de prevenir el aumento del riesgo
RI13	2	Bajo	Procedimentar la generación de credenciales con un nivel alto de complejidad y seguridad (caracteres numéricos y alfanuméricos) por primer acceso.	CO23	Estrategia de prevenir el aumento del riesgo
RI14	2	Bajo	Incluir en la implementación de un reglamento de administración de usuarios, el periodo con que	CO24	Estrategia de prevenir el aumento del riesgo

			se deben realizar las revisiones de los perfiles.		
RI15	3	Medio	Deshabilitar el ingreso a la base de datos de aplicaciones en terminales de usuarios de carácter informático.	CO25	Estrategia de prevenir el aumento del riesgo
			Acceso a la base de datos por medio de contraseña.	CO26	Estrategia de elegir el control
RI16	3	Medio	Adquirir licencia de un sistema antimalware que sea administrable por medio de un servicio para la red en general y que cuente con actualizaciones en online.	CO27	Estrategia de prevenir el aumento del riesgo
RI17	3	Medio	Base de datos resguardados con credenciales.	CO28	Estrategia de prevenir el aumento del riesgo
			Gestionar procesos para usar carpetas compartidas.	CO29	Estrategia de prevenir el aumento del riesgo
RI18	5	Muy alto	Procedimentar la gestión de cambios donde se incluyan los cambios a la base de datos	CO30	Estrategia de prevenir el aumento del riesgo
RI19	3	Medio	Monitorear la capacidad de los discos en el servidor media software.	CO31	Estrategia de prevenir el aumento del riesgo
RI20	2	Bajo	Se hace el mantenimiento a la base de datos pero sin documentarlo.	CO32	Estrategia de prevenir el aumento del riesgo
RI21	1	Muy bajo	Adquirir licencia de un sistema antimalware que sea gestionable por medio de un servicio para la red en general y que cuente con actualizaciones en línea.	CO33	Estrategia de elegir el control
			Controlar el acceso al servidor mediante la administración de los puertos.	CO34	Estrategia de prevenir el aumento del riesgo
RI22	2	Bajo	Recursos Humanos tiene un proceso de calificación que aplica al nuevo personal.	CO35	Estrategia de elegir el control
			Tener un listado de proveedores de mantenimiento.	CO36	Estrategia de prevenir el aumento del riesgo
			Capacitar al personal mediante cursos de mantenimiento como plan de motivación.	CO37	Estrategia de prevenir el aumento del riesgo
RI23	2	Bajo	Realizar y actualizar el inventario de activos de TI. Revisar la operatividad y el tiempo de uso de los equipos.	CO38	Estrategia de prevenir el aumento del riesgo
RI24	2	Bajo	El plan de continuidad del negocio debe contar con un elaborado plan de mantenimiento preventivo de manera obligatoria.	CO39	Estrategia de prevenir el aumento del riesgo
RI25	3	Medio	Coordinar con gerencia un plan de mantenimiento de prevención del sistema eléctrico, equipos de TI sobre todo en los que se soportan los procesos críticos.	CO40	Estrategia de prevenir el aumento del riesgo

			Contar con red eléctrica estabilizada.	CO41	Estrategia de elegir el control
			Mantener conectados los equipos críticos a un UPS	CO42	Estrategia de prevenir el aumento del riesgo
			Realizar pruebas cada cierto periodo al sistema de respaldo eléctrico e incluirlo en el plan de mantenimiento de prevención.	CO43	Estrategia de prevenir el aumento del riesgo
			La revisión de las conexiones eléctricas se deben incorporar en el plan de mantenimiento de prevención.	CO44	Estrategia de prevenir el aumento del riesgo
RI26	2	Bajo	Determinar las configuraciones básicas que debe tener cada terminal informático.	CO45	Estrategia de prevenir el aumento del riesgo
RI27	3	Medio	Generar concientización sobre sobre el buen uso de los equipos informáticos a los usuarios de TI.	CO46	Estrategia de prevenir el aumento del riesgo
RI28	2	Bajo	Cada dependencia debe hacerse responsable de las condiciones ambientales y ergonómicas adecuadas para cada terminal informático. Cada terminal informático debe estar seguro en condiciones ambientales y ergonómicas. Cada área debe cumplir con las responsabilidades de uso y/o mantenimiento asignado en el inventario de activos.	CO47	Estrategia de aceptar el riesgo
RI29	2	Bajo	Para asegurar la continuidad de la operación el área de TI debe conocer los activos críticos, los controles y salvaguardas correspondientes en un inventario de activos de TI.	CO48	Estrategia de prevenir el aumento del riesgo
			Los equipos que según el inventario de TI se consideren como críticos deben generar backups de información que generan o almacenan ; además respaldar la información de su configuración.	CO49	Estrategia de prevenir el aumento del riesgo
RI30	4	Alto	Concientizar a los usuarios de TI por medio de actividades con la finalidad de que generen respaldos de archivos críticos de manera periódica en dispositivos externos o secundarios.	CO50	Estrategia de prevenir el aumento del riesgo
RI31	3	Medio	Instalación de Antivirus	CO51	Estrategia de prevenir el aumento del riesgo
RI32	4	Alto	Implementar controles por medio de políticas y/o procedimientos al acceso de áreas restringidas.	CO52	Estrategia de prevenir el aumento del riesgo

			Generar bitácora de acceso mediante los registros de los mismos al cuarto de servidores y al ambiente de TI.	CO53	Estrategia de prevenir el aumento del riesgo
			El personal del área debe acompañar al personal a realizar el mantenimiento.	CO54	Estrategia de prevenir el aumento del riesgo
			El acceso al data center o cuarto de servidores, debe ser restringido con una puerta con llave que debe ser manejado por el Jefe de sistemas y dependencia únicamente.	CO55	Estrategia de elegir el control
			La sala donde se encuentran los servidores es independiente a donde se encuentra el área de producción y desarrollo.	CO56	Estrategia de elegir el control
			Acondicionar un sistema de cámaras de video para la vigilancia en el ingreso del personal interno o externo al área.	CO57	Estrategia de prevenir el aumento del riesgo
RI33	3	Medio	La sala cuenta con equipo de aire acondicionado que no permite el recalentamiento de los equipos.	CO58	Estrategia de prevenir el aumento del riesgo
			Contar con extintores y sensores de humo	CO59	Estrategia de prevenir el aumento del riesgo
			La sala donde se encuentran los servidores es independiente a donde se encuentra el área de producción y desarrollo. Bajo llave	CO60	Estrategia de elegir el control
			Contar con luces de emergencia	CO61	Estrategia de prevenir el aumento del riesgo
			Mediante una bitácora se registra el acceso a la sala donde se encuentran los servidores.	CO62	Estrategia de prevenir el aumento del riesgo
			Acondicionar un sistema de cámaras de video para la vigilancia del ingreso del personal interno o externo al área de los servidores.	CO63	Estrategia de prevenir el aumento del riesgo
			Designar al personal para el manejo de llaves.	CO64	Estrategia de prevenir el aumento del riesgo
			Implementar una sala alterna de servidores.	CO65	Estrategia de prevenir el aumento del riesgo
			Diseñar un plan de mantenimiento para los equipos de seguridad	CO66	Estrategia de prevenir el aumento del riesgo
			Capacitar al personal en el uso de extintores	CO67	Estrategia de prevenir el aumento del riesgo
RI34	2	Bajo	Registrar los acceso a áreas restringidas.	CO68	Estrategia de prevenir el aumento del riesgo

RI35	3	Medio	Registrar los ingresos a la sala de servidores.	CO69	Estrategia de prevenir el aumento del riesgo
RI36	2	Bajo	Implementación de procedimientos para el mantenimientos de los equipos.	CO70	Estrategia de prevenir el aumento del riesgo
RI37	3	Medio	Registrar las entradas y salidas de equipos y la revisión de maletines mediante un registro.	CO71	Estrategia de prevenir el aumento del riesgo
RI38	4	Alto	Mediante un reglamento operativo definir los procedimientos y criterios para el etiquetado, traslado, almacenamiento y aseguramiento de los dispositivos que contienen los respaldos y backups ; en ambientes externos alternos.	CO72	Estrategia de prevenir el aumento del riesgo
RI39	3	Medio	La generación de backups se hacen mediante políticas , aunque no documentadas.	CO73	Estrategia de elegir el control
			Implementar y probar procedimientos para la restauración	CO74	Estrategia de prevenir el aumento del riesgo
			Controlar el estado de almacenamiento de los medios de backups o respaldo de manera trimestral.	CO75	Estrategia de prevenir el aumento del riesgo
			Se monitorea los procedimientos de respaldo.	CO76	Estrategia de elegir el control
			Implementación de un centro alterno de procesamiento de datos básico.	CO77	Estrategia de prevenir el aumento del riesgo
RI40	2	Bajo	Mejorar el proceso para verificar el estado de almacenamiento de los medios de respaldo.	CO78	Estrategia de prevenir el aumento del riesgo
RI41	5	Muy alto	Contar con una herramienta para comprimir la base de datos y realice una verificación automatizada de los mismos.	CO79	Estrategia de prevenir el aumento del riesgo
			Contar con un programa que grabe los archivos comprimidos y realice una verificación después de la misma.	CO80	Estrategia de prevenir el aumento del riesgo
			Mejorar el procedimiento para verificación del status de almacenamiento de los medios de respaldo.	CO81	Estrategia de prevenir el aumento del riesgo
RI42	3	Medio	Implementar un reglamento operativo para la generación de respaldos de la base de datos y/o aplicaciones.	CO82	Estrategia de prevenir el aumento del riesgo
RI43	2	Bajo	Establecer las responsabilidades que debe cumplir el personal en el manual de organización y funciones.	CO83	Estrategia de prevenir el aumento del riesgo
RI44	2	Bajo	El jefe de TI debe desarrollar y presentar un plan de capacitación.	CO84	Estrategia de prevenir el aumento del riesgo

RI45	2	Bajo	Se cuenta con recurso humano para reemplazo pero no está debidamente instruido.	CO85	Estrategia de aceptar el riesgo
RI46	3	Medio	Documentar mediante un procedimiento la administración de perfiles de usuario, seguir con la asignación de acuerdo a su función por usuario y puesto de trabajo.	CO86	Estrategia de elegir el control
			Generar bitácora de las transacciones realizadas por los usuarios para la auditoría de las mismas.	CO87	Estrategia de prevenir el aumento del riesgo
RI47	4	Alto	Establecer un procedimiento para la revisión periódica de la bitácora de las transacciones realizadas por los usuarios para la auditoría.	CO88	Estrategia de prevenir el aumento del riesgo
RI48	3	Medio	Establecer el procedimiento para la aceptación de acuerdos de confidencialidad por parte de la totalidad de los usuarios de TI y que serán revisados periódicamente para su cumplimiento.	CO89	Estrategia de prevenir el aumento del riesgo
RI49	3	Medio	Los intentos de accesos no autorizados se deben documentar.	CO90	Estrategia de prevenir el aumento del riesgo
			Definir y desarrollar políticas y reglamentos de seguridad de TI que incluyan las sanciones por incumplimiento de las mismas.	CO91	Estrategia de prevenir el aumento del riesgo
RI50	2	Bajo	Desarrollar un proceso para la gestión de altas, bajas y modificación de cuentas de usuarios en relación a los perfiles de los mismos.	CO92	Estrategia de prevenir el aumento del riesgo
RI51	2	Bajo	Todos los nuevos analistas de sistemas reciben una capacitación acerca de los procesos del negocio y los procesos automatizados, se le asigna gradualmente las tareas y requerimientos teniendo en cuenta el grado de experiencia en el desarrollo referente al proceso del negocio.	CO93	Estrategia de elegir el control
RI52	3	Medio	Los requisitos de implementación de los procesos más importantes se priorizan.	CO94	Estrategia de elegir el control
RI53	2	Bajo	Contar con un reglamento para el acceso a internet.	CO95	Estrategia de prevenir el aumento del riesgo
RI54	4	Medio	Limitar de acuerdo al nivel de acceso de los usuarios, el acceso a internet.	CO96	Estrategia de prevenir el aumento del riesgo
RI55	2	Bajo	Se realiza la capacitación introductoria de los procesos del negocio y de los automatizados del sistema.	CO97	Estrategia de elegir el control

RI56	2	Bajo	Implementar un plan preventivo de mantenimiento junto con procedimientos establecidos y debidamente documentados referente al mantenimiento correctivo de servidores.	CO98	Estrategia de prevenir el aumento del riesgo
RI57	3	Medio	Acuerdos mediante contratos de servicio de mantenimiento.	CO99	Estrategia de trasladar el riesgo a terceros
			Controles ambientales en la sala de servidores.	CO100	Estrategia de prevenir el aumento del riesgo
RI58	5	Muy alto	Contar con personal debidamente instruido en Windows server y la actualización de parches.	CO101	Estrategia de mitigar el riesgo
RI59	2	Bajo	Debe estar en el Plan de mantenimiento de los servidores	CO102	Estrategia de prevenir el aumento del riesgo
RI60	2	Bajo	El software cortafuegos instalado para toda la red , con actualizaciones que son automáticas.	CO103	Estrategia de prevenir el aumento del riesgo
			Están a disposición las copias de base de datos.	CO104	Estrategia de prevenir el aumento del riesgo
			Contar con un servidor de respaldo, el cual debe estar configurado y habilitado para la puesta en producción	CO105	Estrategia de prevenir el aumento del riesgo
			Contar con un centro adicional de procesamiento básico	CO106	Estrategia de prevenir el aumento del riesgo
RI61	4	Alto	El jefe de sistemas monitorea de manera mensual la bitácora de auditoría y las operaciones que se realizan en la base de datos.	CO107	Estrategia de elegir el control
RI62	2	Bajo	Establecer procedimientos de gestión de cambios y versiones.	CO108	Estrategia de prevenir el aumento del riesgo
			Procedimentar y documentar las pruebas de modificaciones antes de puesta en producción	CO109	Estrategia de prevenir el aumento del riesgo
RI63	5	Muy alto	Desactivar herramientas adicionales que permiten acceder a la base de datos. Los accesos a la base de datos mediante herramientas adicionales serán desactivados.	CO110	Estrategia de mitigar el riesgo
			Establecer protocolo referente a la fijación de contraseña para el ingreso a la base de datos. Contará con un nivel de complejidad que difiera a las contraseñas de los usuarios locales.	CO111	Estrategia de mitigar el riesgo
			Desarrollar un procedimiento para la administración de altas, bajas y modificación de cuentas	CO112	Estrategia de mitigar el riesgo

			de usuarios en relación a los perfiles de los mismos.		
RI64	3	Medio	Se informará por medio de telefonía y correo la incidencia presentada	CO113	Estrategia de elegir el control
RI65	3	Medio	El proveedor realiza las copias de respaldo de los correos y configuraciones.	CO114	Estrategia de elegir el control
RI66	2	Bajo	Se limita el espacio de cuenta correo de acuerdo al tipo de usuario en el hosting.	CO115	Estrategia de elegir el control
RI67	2	Bajo	Cuando el personal que administra el correo se retira, se actualizan las contraseñas.	CO116	Estrategia de elegir el control
			Procedimentar el cambio automatizado de las cuentas de usuario por primera vez con credenciales seguras.	CO117	Estrategia de prevenir el aumento del riesgo
RI68	3	Medio	Procedimentar y reglamentar el uso del correo institucional, y que se establezcan requerimientos para la creación de contraseñas seguras.	CO118	Estrategia de prevenir el aumento del riesgo
RI69	3	Medio	Mediante un reglamento operativo definir los procesos para el etiquetado, traslado, almacenamiento y resguardo de los dispositivos que contienen los respaldos y backups ; en ambientes externos alternos.	CO119	Estrategia de prevenir el aumento del riesgo
RI70	3	Medio	Se cuenta con validaciones para el registro de información en el sistema, la validación se ha realizado en la base de datos.	CO120	Estrategia de elegir el control
			En los perfiles del puesto, se ha designado el requerimiento que el personal cuente con conocimientos básicos de computación. Como requisito al personal se ha definido en el perfil del puesto que cuente con conocimientos básicos en computación	CO121	Estrategia de elegir el control
RI71	3	Medio	Establecer la criticidad de los equipos y controlar su operación, documentando los incidentes técnicos y de seguridad que se presenten en ellos.	CO122	Estrategia de prevenir el aumento del riesgo
			Contar con una lista de proveedores para el mantenimiento correctivo de los equipos críticos.	CO123	Estrategia de prevenir el aumento del riesgo
			Ante errores en las conexiones de red y equipos de TI , se debe capacitar al personal técnico para una inmediata solución ante estos escenarios.	CO124	Estrategia de prevenir el aumento del riesgo

RI72	3	Medio	Se cuenta con un sistema de alimentación ininterrumpida (UPS)	CO125	Estrategia de elegir el control
RI73	2	Bajo	Se realiza el mantenimiento de soporte a solicitud de los requerimientos de los usuarios y por mejoras en los procesos de manera continua.	CO126	Estrategia de elegir el control
RI74	3	Medio	El procedimiento de control de modificaciones en los sistemas informáticos en producción debe ser implementado y llevar un control de versiones en forma de documentación.	CO127	Estrategia de prevenir el aumento del riesgo

4.8 Valoración de las salvaguardas

Luego de haber identificado las salvaguardas y su estrategia de implementación; se valora de acuerdo a los criterios estipulados en el modelo para obtener la efectividad de los controles.

Tabla N° 40: Valoración de las salvaguardas de acuerdo a los criterios de efectividad.

Nivel de Riesgo Intrínseco (NRI)			Salvaguarda	ESTADO DE CONTROL		OPORTUNIDAD DE CONTROL		GRADO DE IMPLEMENTACION		NIVEL DE EFECTIVIDAD	
ID riesgo	Nivel	Categoría	Control (CODIGO)	Estado	Descripción	Estado	Descripción	Estado	Descripción	Estado	Descripción
RI1	4	Alto	CO1	1	Implementado	1	Preventivo	2	Semiautomatizado	5	Optimo
			CO2	0	No implementado	2	Detectivo	2	Semiautomatizado	1	Deficiente
RI2	4	Alto	CO3	0	No implementado	2	Detectivo	2	Semiautomatizado	1	Deficiente
RI10	5	Muy alto	CO18	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
			CO19	0	No implementado	3	Correctivo	1	Manual	1	Deficiente
			CO20	0	No implementado	2	Detectivo	2	Semiautomatizado	1	Deficiente
RI18	5	Muy alto	CO30	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
RI30	4	Alto	CO50	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
RI32	4	Alto	CO52	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
			CO53	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
			CO54	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
			CO55	1	Implementado	1	Preventivo	1	Manual	4	Bueno
			CO56	1	Implementado	1	Preventivo	1	Manual	4	Bueno
			CO57	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
RI38	4	Alto	CO72	0	No implementado	1	Preventivo	1	Manual	1	Deficiente
RI41	5	Muy alto	CO79	0	No implementado	1	Preventivo	3	Automatizado	1	Deficiente
			CO80	0	No implementado	1	Preventivo	3	Automatizado	1	Deficiente
			CO81	1	Implementado	3	Correctivo	2	Semiautomatizado	2	Regular
RI47	4	Alto	CO88	1	Implementado	2	Detectivo	2	Semiautomatizado	3	Más que regular

RI58	5	Muy alto	CO101	1	Implementado	3	Correctivo	1	Manual	2	Regular
RI61	4	Alto	CO107	1	Implementado	2	Detectivo	2	Semiautomatizado	3	Más que regular
RI63	5	Muy alto	CO110	1	Implementado	3	Correctivo	3	Automatizado	2	Regular
			CO111	1	Implementado	1	Preventivo	1	Manual	4	Bueno
			CO112	1	Implementado	1	Preventivo	1	Manual	4	Bueno

4.9 Estimación del estado de riesgo residual

Tomando en cuenta el valor del nivel de efectividad calculado anteriormente, es que se devuelve el impacto y la probabilidad residual.

Tabla N° 41: Valoración del Nivel de Riesgo Residual (NRR).

Nivel de Riesgo Intrínseco (NRI)			NIVEL DE EFECTIVIDAD		Impacto residual en los procesos		Probabilidad residual de que la amenaza explote la vulnerabilidad		Nivel de Riesgo Residual (NRR)		Apetito de Riesgo
ID riesgo	Nivel	Categoría	Estado	Descripción	Nivel	Categoría	Nivel	Categoría	Nivel	Categoría	
RI1	4	Alto	3	Más que regular	3	Medio	1	Muy poco frecuente	1	Muy bajo	Riesgo aceptado
RI2	4	Alto	1	Deficiente	4	Alto	4	Frecuente	4	Alto	No aceptable
RI10	5	Muy alto	1	Deficiente	5	Muy Alto	4	Frecuente	5	Muy alto	No aceptable
RI18	5	Muy alto	1	Deficiente	5	Muy Alto	4	Frecuente	5	Muy Alto	No aceptable
RI30	4	Alto	1	Deficiente	4	Alto	4	Frecuente	4	Alto	No aceptable
RI32	4	Alto	2	Regular	4	Alto	2	Poco frecuente	4	Bajo	Riesgo aceptado
RI38	4	Alto	1	Deficiente	5	Muy Alto	3	Normal	4	Alto	No aceptable
RI41	5	Muy alto	1	Deficiente	5	Muy Alto	4	Frecuente	5	Muy Alto	No aceptable
RI47	4	Alto	3	Más que regular	3	Medio	1	Muy poco frecuente	2	Muy bajo	Riesgo aceptado
RI58	5	Muy alto	2	Regular	4	Alto	3	Normal	3	Medio	Riesgo aceptado
RI61	4	Alto	3	Más que regular	2	Bajo	2	Poco frecuente	1	Bajo	Riesgo aceptado
RI63	5	Muy alto	3	Más que regular	3	Medio	2	Poco frecuente	1	Bajo	Riesgo aceptado

V. DISCUSIÓN DE RESULTADOS

5.1 Análisis del modelo por juicio de expertos

El diseño de esta investigación es de tipo descriptivo propositivo no experimental. Por lo que ha sido necesario diseñar y desarrollar a nivel propositivo un modelo de gestión de riesgos para la seguridad de TI que se ajuste a la necesidad de la empresa sin modificar su realidad actual.

Para valorar el modelo propuesto para CHANCAFE NORTE SAC se ha sometido a la evaluación de juicio de expertos (Método Delphi[4]) de profesionales familiarizados con el modelo del negocio y con la seguridad de TI; con la finalidad de verificar la validez y utilidad del modelo; para la valorización se ha contemplado cuatro aspectos: suficiencia, claridad, coherencia y relevancia en cada una de las actividades y tareas de cada etapa del modelo.

Con dicho método obtuvimos la opinión y el conocimiento de las personas encargadas de las funciones de:

- Jefatura de TI de CHANCAFE NORTE SAC.
- Jefatura de la Unidad de Riesgos de una empresa comercial externa.

Para su aplicación se consideró las siguientes características:

- La aplicación se realizó de manera anónima, ninguna de las personas que evaluaron el modelo tuvieron conocimiento que el otro también lo estaba haciendo, para que ninguno se vea influenciado por el otro.
- Se presentó el mismo cuestionario a todos los evaluadores de manera individual.
- La información que se presenta son de todas las opiniones y/o resultados indicando la evaluación obtenida por cada uno de los participantes en el método.

El procedimiento realizado fue el siguiente:

1. Se elaboró un cuestionario de validación incluyendo los criterios de suficiencia, claridad, coherencia y relevancia en todas las etapas y actividades desarrolladas en el modelo.
2. Se explicó a los profesionales que participaron de la evaluación de manera individual todas las actividades y tareas que se contemplan en el modelo.

3. Posteriormente por medio de un correo electrónico se le envió a cada profesional de manera individual, un archivo donde se adjuntó el desarrollo del modelo propuesto, el cuestionario para la validación del modelo propuesto (Ver Anexo Nº 1), y los criterios para la validación.

[4] Norman Dalkey y Olaf Hermes, dos matemáticos norteamericanos, diseñaron en 1963 la técnica que llamaron "Delphi" el cual tiene como finalidad establecer el consenso de expertos con respecto a un tema o problema complejo

5.2 Indicadores de cada criterio para la valoración del modelo de gestión de riesgos de TI enviado a los profesionales seleccionados.

Tabla N° 42: Pesos e indicadores para la valoración del modelo de Gestión de Riesgos de TI.

CRITERIO	VALOR	CALIFICACION	INDICADOR
SUFICIENCIA La actividad descrita es suficiente para aportar en el logro del objetivo de la etapa del modelo de gestión de riesgos propuesto.	1	El criterio no se cumple	Los procedimientos no son suficientes para el logro de la actividad
	2	El criterio se cumple en un nivel bajo	Los procedimientos miden algún aspecto de actividad pero no corresponden con la actividad total.
	3	El criterio se cumple en nivel moderado	Se deben incrementar algunos procedimientos para poder evaluar la actividad completamente.
	4	El criterio se cumple en un nivel alto	Los procedimientos son suficientes
CLARIDAD La actividad está descrita de una manera simple y entendible, de tal forma que no es necesario tener experiencia o tener conocimiento detallado sobre el tema.	1	El criterio no se cumple	Los procedimientos no son claros
	2	El criterio se cumple en un nivel bajo	Los procedimientos requieren bastantes modificaciones en el uso de las palabras de acuerdo con su significado o por el ordenamiento de las mismas.
	3	El criterio se cumple en nivel moderado	Se requiere un cambio muy específico de algunos de los términos de los procedimientos.
	4	El criterio se cumple en un nivel alto	Los procedimientos son claros, tienen estructura y sintaxis adecuada.
COHERENCIA La actividad ha sido diseñada de tal forma que es coherente con los marcos de referencia utilizados.	1	El criterio no se cumple	Los procedimientos no tiene relación lógica con la actividad
	2	El criterio se cumple en un nivel bajo	Los procedimientos tiene una relación tangencial con la actividad
	3	El criterio se cumple en nivel moderado	Los procedimientos tiene una relación moderada con la actividad
	4	El criterio se cumple en un nivel alto	Los procedimientos se encuentran completamente relacionado con la actividad
RELEVANCIA La actividad	1	El criterio no se cumple	Los procedimientos pueden ser eliminados sin que se vea

aporta en la solución del problema			afectada la medición de la actividad
	2	El criterio se cumple en un nivel bajo	Los procedimientos tienen alguna relevancia, pero otro actividad puede estar incluyendo lo que mide éste.
	3	El criterio se cumple en nivel moderado	Los procedimientos son relativamente importantes.
	4	El criterio se cumple en un nivel alto	Los procedimientos son muy relevantes y deben estar incluidos.

Fuente: Elaboración propia

5.3 Resultados obtenidos

A. Etapa **IDENTIFICACIÓN DEL RIESGO:**

- Criterio de **SUFICIENCIA**: Las actividades descritas son suficientes para aportar en el logro del objetivo de la etapa del modelo de gestión de riesgos propuesto.

Tabla N° 43: Resultados del criterio de suficiencia en la etapa de identificación del riesgo.

ETAPA	ACTIVIDAD	SUFICIENCIA		PROMEDIO
Identificación del riesgo	Identificar y tipificar los activos de la información	4	4	4
	Valorar las dimensiones de los activos de la información	4	4	4
	Priorizar los activos de la información	4	4	4
	Identificar amenazas de los activos de la información	4	4	4

Fuente: Elaboración propia

- Criterio de **CLARIDAD**: Las actividades de esta etapa se describieron de forma simple y entendible. Pero se debe mejorar la terminología utilizada en las actividades de identificación y tipificación de los activos de información.

Tabla N° 44: Resultados del criterio de claridad en la etapa de identificación del riesgo.

ETAPA	ACTIVIDAD	CLARIDAD		PROMEDIO
Identificación del riesgo	Identificar y tipificar los activos de la información	4	2	3
	Valorar las dimensiones de los activos de la información	4	4	4
	Priorizar los activos de la información	4	4	4
	Identificar amenazas de los activos de la información	4	4	4

Fuente: Elaboración propia

- Criterio de **COHERENCIA**: Las actividades descritas se encuentran completamente relacionado con esta etapa.

Tabla N° 45: Resultados del criterio de coherencia en la etapa de identificación del riesgo.

ETAPA	ACTIVIDAD	COHERENCIA		PROMEDIO
Identificación del riesgo	Identificar y tipificar los activos de la información	3	4	4
	Valorar las dimensiones de los activos de la información	3	4	4
	Priorizar los activos de la información	4	4	4
	Identificar amenazas de los activos de la información	4	4	4

Fuente: Elaboración propia

- Criterio de **RELEVANCIA**: Las actividades descritas son importantes para el desarrollo de esta etapa. En la actividad que corresponde a la valoración de dimensiones de activos de la información, se podrían considerar un número menor de dimensiones para su valoración.

Tabla N° 46: Resultados del criterio de relevancia en la etapa de identificación del riesgo.

ETAPA	ACTIVIDAD	RELEVANCIA		PROMEDIO
Identificación del riesgo	Identificar y tipificar los activos de la información	4	4	4
	Valorar las dimensiones de los activos de la información	3	3	3
	Priorizar los activos de la información	4	4	4
	Identificar amenazas de los activos de la información	4	4	4

Fuente: Elaboración propia

B. Etapa **ANÁLISIS Y EVALUACIÓN DEL RIESGO**:

- Criterio de **SUFICIENCIA**: Las actividades descritas son suficientes para aportar en el logro del objetivo de la etapa del modelo de gestión de riesgos propuesto.

Tabla N° 47: Resultados del criterio de suficiencia en la etapa de análisis y evaluación del riesgo.

ETAPA	ACTIVIDAD	SUFICIENCIA		PROMEDIO
Análisis y evaluación del riesgo	Priorización de amenazas según el nivel de riesgo	4	4	4
	Definir Impacto derivado de la materialización de las amenazas	4	4	4
	Definir Probabilidad de materialización de las amenazas	4	4	4
	Estimar el nivel de riesgo intrínseco	4	4	4

Fuente: Elaboración propia

- Criterio de **CLARIDAD**: Las actividades de esta etapa se describieron de forma simple y entendible.

Tabla N° 48: Resultados del criterio de claridad en la etapa de análisis y evaluación del riesgo.

ETAPA	ACTIVIDAD	CLARIDAD		PROMEDIO
Análisis y evaluación del riesgo	Priorización de amenazas según el nivel de riesgo	4	4	4
	Definir Impacto derivado de la materialización de las amenazas	4	4	4
	Definir Probabilidad de materialización de las amenazas	4	4	4
	Estimar el nivel de riesgo intrínseco	4	4	4

Fuente: Elaboración propia

- Criterio de **COHERENCIA**: Las actividades descritas se encuentran completamente relacionadas con esta etapa.

Tabla N° 49: Resultados del criterio de coherencia en la etapa de análisis y evaluación del riesgo.

ETAPA	ACTIVIDAD	COHERENCIA		PROMEDIO
Análisis y evaluación del riesgo	Priorización de amenazas según el nivel de riesgo	3	4	4
	Definir Impacto derivado de la materialización de las amenazas	4	3	4
	Definir Probabilidad de materialización de las amenazas	4	3	4
	Estimar el nivel de riesgo intrínseco	4	3	4

Fuente: Elaboración propia

- Criterio de **RELEVANCIA**: Las actividades descritas son importantes para el desarrollo de esta etapa.

Tabla N° 50: Resultados del criterio de relevancia en la etapa de análisis y evaluación del riesgo.

ETAPA	ACTIVIDAD	RELEVANCIA		PROMEDIO
Análisis y evaluación del riesgo	Priorización de amenazas según el nivel de riesgo	4	4	4
	Definir Impacto derivado de la materialización de las amenazas	4	3	4
	Definir Probabilidad de materialización de las amenazas	4	3	4
	Estimar el nivel de riesgo intrínseco	4	3	4

Fuente: Elaboración propia

C. Etapa **TRATAMIENTO DEL RIESGO:**

- Criterio de **SUFICIENCIA**: La definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección, el impacto residual y estimación del nivel de riesgo residual, pueden complementarse con otras actividades para mayor detalle en esta etapa.

Tabla N° 51: Resultados del criterio de suficiencia en la etapa de tratamiento del riesgo.

ETAPA	ACTIVIDAD	SUFICIENCIA		PROMEDIO
Tratamiento del riesgo	Proponer mecanismos de protección	4	4	4
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	3	3
	Definir la probabilidad residual de materialización de amenazas	4	4	4
	Definir Impacto residual de materialización de amenazas	4	2	3
	Estimar el nivel de riesgo residual	3	3	3

Fuente: Elaboración propia

- Criterio de **CLARIDAD**: Las actividades de esta etapa se describieron en forma simple y entendible. Pero en cuanto a las actividades de definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección y estimación del nivel de riesgo residual, podrían mejorar la terminología que utilizan, para una mayor claridad.

Tabla N° 52: Resultados del criterio de claridad en la etapa de tratamiento del riesgo.

ETAPA	ACTIVIDAD	CLARIDAD		PROMEDIO
Tratamiento del riesgo	Proponer mecanismos de protección	4	4	4
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	4	2	3
	Definir la probabilidad residual de materialización de amenazas	4	4	4
	Definir Impacto residual de materialización de amenazas	2	4	3
	Estimar el nivel de riesgo residual	3	3	3

Fuente: Elaboración propia

- Criterio de **COHERENCIA**: Las actividades descritas se encuentran completamente relacionado con esta etapa.

Tabla N° 53: Resultados del criterio de coherencia en la etapa de tratamiento del riesgo.

ETAPA	ACTIVIDAD	COHERENCIA		PROMEDIO
Tratamiento del riesgo	Proponer mecanismos de protección	4	4	4
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	4	3	4
	Definir la probabilidad residual de materialización de amenazas	4	4	4
	Definir Impacto residual de materialización de amenazas	4	4	4
	Estimar el nivel de riesgo residual	4	3	4

Fuente: Elaboración propia

- Criterio de **RELEVANCIA**: Las actividades descritas son importantes para el desarrollo de esta etapa.

Tabla N° 54: Resultados del criterio de relevancia en la etapa de tratamiento del riesgo.

ETAPA	ACTIVIDAD	RELEVANCIA		PROMEDIO
Tratamiento del riesgo	Proponer mecanismos de protección	4	4	4
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	4	3	4
	Definir la probabilidad residual de materialización de amenazas	4	4	4
	Definir Impacto residual de materialización de amenazas	4	4	4
	Estimar el nivel de riesgo residual	4	3	4

Fuente: Elaboración propia

Según los resultados obtenidos se puede considerar lo siguiente:

- Etapa **IDENTIFICACIÓN DEL RIESGO**: El desarrollo de esta etapa se realizó en forma clara y coherente, la etapa del modelo considera suficientes actividades que permiten la plena identificación de los activos, sus vulnerabilidades y amenazas. Se considera que podría mejorar la terminología específica que se utiliza en la etapa de identificación de los activos de la información. Las actividades que se consideran en esta etapa son relevantes para el desarrollo del modelo de gestión de riesgos propuesto.

- Etapa **ANÁLISIS Y EVALUACIÓN DEL RIESGO**: El desarrollo de esta etapa se realizó en forma clara y coherente, la etapa del modelo considera suficientes actividades que permitan priorizar correctamente las amenazas según el nivel de riesgo y estimando el nivel de riesgo intrínseco en función de los niveles de probabilidad e impacto de materialización de amenazas. Las actividades que se consideran en esta etapa son relevantes para el desarrollo del modelo de gestión de riesgos propuesto.
- Etapa de **TRATAMIENTO DEL RIESGO**: El desarrollo de esta etapa se realizó en forma clara y coherente, la etapa del modelo considera suficientes actividades que permitan proponer mecanismos de protección ante amenazas, definir los criterios para obtener el nivel de eficiencia de estos mecanismos de protección, Las actividades que se consideran en esta etapa son relevantes para el desarrollo del modelo de gestión de riesgos propuesto. Sin embargo, se podría mejorar la terminología utilizada en esta etapa e incrementar algunas sub tareas que aporten claridad y suficiencia para definir criterios que permitan medir la eficiencia de los mecanismos de control y estimar el riesgo residual.

CONCLUSIONES Y RECOMENDACIONES

1. Se ha diseñado un modelo de gestión de riesgos de TI que contempla todos los elementos necesarios y sus relaciones para la gestión de los riesgos de TI, como la identificación, tipificación y valorización de los activos de TI; identificación de las amenazas y vulnerabilidades; definición del impacto y la probabilidad de la materialización de las amenazas, estimación del nivel del riesgo intrínseco y priorización de las amenazas de acuerdo al nivel del riesgo. Además, propone mecanismos de protección y define criterios para obtener el nivel de efectividad de las salvaguardas. Finalmente, el modelo contempla la definición del impacto y probabilidad residual de la materialización de las amenazas y estimación del nivel de riesgo residual en los activos de TI.

2. Se ha logrado proponer una metodología para la implementación del modelo de gestión de riesgos de TI que ayude a dar soporte a la seguridad de la información de los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE SAC basado en MAGERIT, que contempla tres etapas de la gestión de riesgos de TI, como son: (1) la identificación del riesgo de TI, (2) análisis y evaluación del riesgo de TI; y (3) tratamiento del riesgo de TI.

3. La evaluación del modelo a través del método Delphi permitió obtener la opinión de profesionales con autoridad en la gestión de los riesgos operacionales de TI, acorde a tres etapas: (1) la identificación del riesgo de TI, (2) análisis y evaluación del riesgo de TI; y (3) tratamiento del riesgo de TI.Los resultados demuestran que las actividades de dichas etapas del modelo son aceptables según los criterios de suficiencia , claridad , coherencia y relevancia , por tanto puede ser generalizado para otras empresas del mismo sector.

Recomendaciones:

1. Dado que el modelo tiene un alcance a nivel propositivo se recomienda a la empresa que éste sea implementado a un corto plazo con la finalidad de ayudar a dar soporte a la seguridad de TI de sus procesos críticos.

2. Dado que la evaluación de los riesgos es permanente se recomienda que el modelo de matriz de riesgos que se propone sea implementado en una aplicación informática, que permita actualizaciones más dinámicas, con posibilidades de generar indicadores/resultados gráficos y generación de escenarios.

3. Es recomendable que gerencia y el área de TI en conjunto designen responsabilidades que permitan, mediante la automatización de la propuesta metodológica, alimentar permanentemente de la información necesaria por los verdaderos dueños de los procesos: lista de procesos/servicios críticos, activos, riesgos, amenazas, vulnerabilidades, controles, etc., de tal forma que permita obtener rápidamente la información del nivel de criticidad de sus procesos, porcentaje de desviación de riesgo de los activos o procesos, capital necesario a invertir en la protección de un activo o proceso, entre otra información relevante.

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Mollehuanca , D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* tesis pregrado, Pontificia Universidad Católica del Perú., Lima.

Alvarez Sosa, Y. M. (2013). Diseño de una Metodologia para el Analisis de Riesgo en los Sistemas de Gestión de Seguridad de Informacion en las Universidades de Barquisimeto Estado Lara (Marisgsi).

Asociación Española de Normalización. (2008). *UNE 71504*. Obtenido de https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430

Asociacion Española de Normalización. (Marzo de 2018). *UNE*. Obtenido de https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0059900

Bernal Vallejos, H. H., & Villar Soberon, J. E. (2017). *Dashboard para la Gestión de Riesgos de TI en cumplimiento de las exigencias de la SBS en la Edpyme alternativa –chiclayo, lambayeque*. Lambayeque.

Bureau Veritas España. (16 de 02 de 2018). *Bureau Veritas España*. Recuperado el 09 de 2019, de https://www.bureauveritas.es/home/news/iso-31000-2018-renovada-gestion-riesgos

Castro, M. (2010). El Nuevo Estándar para la Gestión de Riesgos.

Crespo Rin, M. d. (2013). El Análisis de Riesgos dentro de una Auditoría Informática: Pasos y Posibles Metodologías.

Deloitte. (2016). *Deloitte.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/risk/cl-information-technology-risk-in-fs.pdf

Gobierno de España, Ministerio de Hacienda y Administraciones Publicas. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método.* Madrid.

Gobierno de España, Ministerio de Hacienda y Administraciones Publicas. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos.* Madrid.

Gomez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (s.f.). *Metodología y gobierno de la gestión de riesgos de tecnologías de la información.*

Instituto de Auditores Internos de España. (2012). Definición e implantación de Apetito de Riesgo. España.

International Organization for Standardization. (2005). ISO/IEC 27001:2005.

International Organization for Standardization. (2009). ISO/IEC 31000:2009.

International Organization for Standardization. (2013). ISO/IEC 27001:2013.

International Organization for Standardization. (2013). ISO/IEC 27002:2013.

International Organization for Standardization. (2018). ISO/IEC 31000:2018.

Vásquez, K. d. (2013). Aplicación De La Metodología Magerit Para El Análisis Y Gestión De Riesgos De La Seguridad De La Información Aplicada a la Empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala.

ANEXOS

ANEXO N° 1

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE GESTION DE RIESGOS DE TI QUE DAN SOPORTE A LOS PROCESOS DE EVALUACION, FINANCIAMIENTO Y COBRANZA DE LA EMPRESA CHANCAFE NORTE S.A.C. BASADA EN LA METODOLOGÍA MAGERIT.

ETAPA	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Identificación del riesgo	Identificar y tipificar los activos de la información					
	Valorar las dimensiones de los activos de la información					
	Priorizar los activos de la información					
	Identificar amenazas de los activos de la información					
Análisis y evaluación del riesgo	Priorización de amenazas según el nivel de riesgo					
	Definir Impacto derivado de la materialización de las amenazas					
	Definir Probabilidad de materialización de las amenazas					
	Estimar el nivel de riesgo intrínseco					
Tratamiento del riesgo	Proponer mecanismos de protección					
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección					
	Definir la probabilidad residual de materialización de amenazas					
	Definir Impacto residual de materialización de amenazas					
	Estimar el nivel de riesgo residual					

Fuente: Elaboración propia

ANEXO N° 2

CUESTIONARIO DE LA ENTREVISTA PARA LA RECOPILACIÓN DE LA INFORMACIÓN

ACTIVO	PREGUNTAS	COMENTARIOS
SERVIDORES	¿Cómo protege el cuarto de comunicaciones o data center, manejan control de acceso?	
	¿De qué manera se prevé el corte de energía eléctrica o variaciones de voltaje?	
	¿Qué ocurre cuando se produce la destrucción o fallo de un componente crítico?	
	¿Cuentan con equipos de respaldo en caso se presenten fallas de configuración?	
	¿Cómo protegen a los equipos de factores ambientales (temperaturas elevadas, incendios, etc.) ?	
	¿Han adquirido nuevos equipos en los últimos años?	
	¿Cuentan con algún plan de mantenimiento para los equipos ?	
	¿Cuentan con algún seguro contra robo para los equipos de cómputo?	
	¿Cómo están protegidos contra virus los equipos de cómputo?	
BASE DE DATOS	¿De qué manera respaldan la información?	
	¿Cuentan con capacidad suficiente para el almacenamiento de la información?	
	¿Qué medidas de seguridad utilizan en caso de pérdida o falla de los backups?	
	¿Cómo controlan el acceso a la base de datos?	
	¿Quiénes tienen acceso a los directorios de la base de datos?	
	¿Qué medidas de seguridad utilizan para prevenir el sabotaje de información?	
	¿Cómo están protegidos los servidores?	
SOFTWARE Y SISTEMAS OPERATIVOS	¿Cuentan con licencias vigentes para el uso de los software?	
	¿De qué manera prevén los errores de configuración?	
	¿Qué políticas han implementado para contrarrestar la mala administración de control de accesos?	
	¿Qué medidas utilizan para evitar la pérdida de datos?	
	¿Cómo están protegidos los software y sistemas operativos?	
BACKUPS	¿Quiénes están autorizados a generar los respaldos?	
	¿Cómo realizan el procedimiento de restore ?	
	¿Qué medios de almacenamiento utilizan para respaldar la información?	
	¿Cómo proceden a validar los respaldos?	
	¿Cuentan con disponibilidad inmediata de los medios de datos?	
	¿Quiénes cuentan con acceso a los backups?	
	¿Qué medidas de seguridad emplean para prevenir el sabotaje de los respaldos?	

CABLEADO	¿En qué condiciones se encuentra el cableado de las redes informáticas?	
	¿En qué condiciones se encuentra el cableado de energía ?	
	¿Cómo protegen al cableado de factores ambientales (temperaturas elevadas, incendios, etc.) ?	
	¿Los cables de red cumplen los estándares establecidos por alguna norma?	
RED	¿Hay un adecuado mantenimiento de los puertos?	
	¿Hay una adecuada configuración de los componentes de red?	
	¿Qué errores de operación se presentan con mayor relevancia?	
	¿Es apropiado el uso de los servicios de la red?	
USUARIOS	¿Qué políticas emplean para restringir el acceso al sistema?	
	¿Son apropiadas las medidas de seguridad en cuanto a las claves de acceso?	
	¿Son apropiadas las condiciones de trabajo (ergonomía, ubicaciones de los equipos, etc.) ?	
	¿De qué manera se protege el acceso a la base de datos por parte de los usuarios en caso de destrucción negligente?	
	¿Cuentan con manuales que sirvan de instructivo para dominar el sistema?	
	¿Cómo se cautela el acceso a los ambientes del sistema?	
	¿Se tiene un adecuado conocimiento del sistema?	
	¿Qué herramientas se aplican para auditar el uso del sistema?	
	¿De qué manera determinan responsabilidades en cuanto al mal uso del sistema?	
	¿Es frecuente la actualización de usuarios para aquellos en condiciones de alta y baja?	
DOCUMENTACION DEL SISTEMA	¿Qué área está encargada del acceso a la documentación?	
	¿La documentación es de libre acceso?	
	¿A quiénes se les otorgan copias de la documentación?	
	¿Cómo se registran los archivos y programas?	
	¿Se han implementado manuales?	
	¿De qué manera está almacenada la documentación?	
	¿Con qué frecuencia se actualiza la documentación?	
SISTEMA CONTABLE ,FINANCIERO Y COMPLEMENTARIO	¿Cómo se maneja el control de cambios?	
	¿De qué manera se atienden los requerimientos correspondientes a la funcionalidad del sistema?	
	¿Quiénes tienen acceso a los programas fuentes del sistema?	
	¿Qué políticas de seguridad se han implementado para el acceso al sistema?	

Fuente: Elaboración propia

ANEXO N° 3

TIPIFICACIÓN DE ACTIVOS DENTRO DE UNA JERARQUÍA SEGÚN MAGERIT *(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)*

Tipo de activo		**Sub clasificación**			**Descripción de aclaración**
[essential]	Activos esenciales	[info] información	[adm] datos de interés para la administración pública		
			[vr] datos vitales (registros de la organización)		Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización.
			[per] datos de carácter personal	[A] nivel alto	Dícese de cualquier información concerniente a personas físicas identificadas o identificables.
				[M] nivel medio	
				[B] nivel bajo	
			[classified] datos clasificados	[C] nivel confidencial	Dícese de aquellos sometidos a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante.
				[R] difusión limitada	
				[UC] sin clasificar	
				[pub] de carácter público	
		[service] servicio			
[arch]	Arquitectura del sistema	[sap] punto de [acceso al] servicio			Establece una frontera entre la prestación de un servicio (proveedor) y el usuario (consumidor).
		[ip] punto de interconexión			Establece una frontera inter-pares: cuando dos sistemas se interconectan para intercambiar información.

		[ext] proporcionado por terceros			Establece una frontera inferior, cuando para la prestación de nuestros servicios recurrimos a un tercero.
[D]	Datos / Información	[files] ficheros			
		[backup] copias de respaldo			
		[conf] datos de configuración			Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información.
		[int] datos de gestión interna			
		[password] credenciales			
		[auth] datos de validación de credenciales			
		[acl] datos de control de acceso			
		[log] registro de actividad			Los registros de actividad sustancian los requisitos de trazabilidad.
		[source] código fuente			
		[exe] código ejecutable			
		[test] datos de prueba			
[K]	Claves criptográficas	[info] protección de la información	[encrypt]	[shared_secret] secreto compartido (clave simétrica)	Por ejemplo, DES, 3-DES, AES, etc.
				[public_encryption] clave pública de cifra	Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc.
				[public_decryption] clave privada de descifrado	
			[sign]	[shared_secret] secreto compartido (clave simétrica)	
				[public_signature] clave privada de firma	Por ejemplo, RSA, Diffie-Hellman, curvas elípticas, etc.
				[public_verification] clave pública de verificación de firma	

		[com] protección de las comunicaciones	[channel] claves de cifrado del canal	
			[authentication] claves de autenticación	
			[verification] claves de verificación de autenticación	
		[disk] cifrado de soportes de información	[encrypt] claves de cifra	
		[x509] certificados de clave pública		
[S]	Servicios	[anon] anónimo		
		[pub] al público en general		
		[ext] a usuarios externos		
		[int] interno		
		[www] world wide web		
		[telnet] acceso remoto a cuenta local		
		[email] correo electrónico		
		[file] almacenamiento de ficheros		
		[ftp] transferencia de ficheros		
		[edi] intercambio electrónico de datos		
		[dir] servicio de directorio		Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado.
		[idm] gestión de identidades		Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización.
		[ipm] gestión de privilegios		Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.

		[pki] PKI - infraestructura de clave pública		
[SW]	Software - Aplicaciones informáticas	[prp] desarrollo propio		Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático.
		[sub] desarrollo a medida		
		[std] estándar	[browser] navegador web	
			[www] servidor de presentación	
			[app] servidor de aplicaciones	
			[email_client] cliente de correo electrónico	
			[email_server] servidor de correo electrónico	
			[file] servidor de ficheros	
			[dbms] sistema de gestión de bases de datos	
			[tm] monitor transaccional	
			[office] ofimática	
			[av] anti virus	
			[os] sistema operativo	
			[hypervisor] gestor de máquinas virtuales	
			[ts] servidor de terminales	
			[backup] sistema de backup	
[HW]	Equipamiento informático (hardware)	[host] grandes equipos		Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.
		[mid] equipos medios		Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.

		[pc] informática personal		Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.
		[mobile] informática móvil		Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.
		[pda] agendas electrónicas		
		[vhost] equipo virtual		
		[backup] equipamiento de respaldo		Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
		[peripheral] periféricos	[print] medios de impresión	Dícese de impresoras y servidores de impresión.
			[scan] escáneres	
			[crypto] dispositivos criptográficos	
		[bp] dispositivo de frontera		Son los equipos que se instalan entre dos zonas de confianza.
		[network] soporte de la red	[modem] módems	Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.
			[hub] concentradores	
			[switch] conmutadores	
			[router] encaminadores	
			[bridge] pasarelas	
			[firewall] cortafuegos	
			[wap] punto de acceso inalámbrico	
		[pabx] centralita telefónica		
		[ipphone] teléfono IP		

[COM]	Redes de comunicaciones	[PSTN] red telefónica		Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
		[ISDN] rdsi (red digital)		
		[X25] X25 (red de datos)		
		[ADSL] ADSL		
		[pp] punto a punto		
		[radio] comunicaciones radio		
		[wifi] red inalámbrica		
		[mobile] telefonía móvil		
		[sat] por satélite		
		[LAN] red local		
		[MAN] red metropolitana		
		[Internet] Internet		
[Media]	Soportes de información	[electronic] electrónicos	[disk] discos	En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
			[vdisk] discos virtuales	
			[san] almacenamiento en red	
			[disquette] disquetes	
			[cd] cederrón (CD-ROM)	
			[usb] memorias USB	
			[dvd] DVD	
			[tape] cinta magnética	
			[mc] tarjetas de memoria	
			[ic] tarjetas inteligentes	
		[non_electronic] no electrónicos	[printed] material impreso	
			[tape] cinta de papel	
			[film] microfilm	
			[cards] tarjetas perforadas	
[AUX]	Equipamiento auxiliar	[power] fuentes de alimentación		En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
		[ups] sistemas de alimentación ininterrumpida		
		[gen] generadores eléctricos		
		[ac] equipos de climatización		

		[cabling] cableado	[wire] cable eléctrico	
			[fiber] fibra óptica	
		[robot] robots	[tape] ... de cintas	
			[disk] ... de discos	
		[supply] suministros esenciales		
		[destroy] equipos de destrucción de soportes de información		
		[furniture] mobiliario: armarios, etc		
		[safe] cajas fuertes		
[L]	Instalaciones	[site] recinto		En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.
		[building] edificio		
		[local] cuarto		
		[mobile] plataformas móviles	[car] vehículo terrestre: coche, camión, etc.	
			[plane] vehículo aéreo: avión, etc.	
			[ship] vehículo marítimo: buque, lancha, etc.	
			[shelter] contenedores	
		[channel] canalización		
		[backup] instalaciones de respaldo		
[P]	Personal	[ue] usuarios externo		En este epígrafe aparecen las personas relacionadas con los sistemas de información.
		[ui] usuarios internos		
		[op] operadores		
		[adm] administradores de sistemas		
		[com] administradores de comunicaciones		
		[dba] administradores de BBDD		
		[sec] administradores de seguridad		
		[des] desarrolladores / programadores		
		[sub] subcontratas		
		[prov] proveedores		

ANEXO N° 4

TABLAS DE REFERENCIA PARA LA VALORACIÓN DE LA CRITICIDAD DE LOS ACTIVOS DE TI SEGÚN MAGERIT (Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)

Descripción de las dimensiones de seguridad de la información.

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

Definición de escala de valoración de la criticidad de los activos de TI.

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	2.pi1	pudiera causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación

3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales
		relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad
		de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones

	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización
		con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	alteración sería del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa
		o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo
		llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma
		excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma
		excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente

		a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente
		a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente
		a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente
		a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos
[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO
[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar
[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

ANEXO N° 5

CATALOGO DE AMENAZAS SOBRE ACTIVO Y DIMENSION DE SEGURIDAD DE LA INFORMACION SEGÚN MAGERIT *(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)*

[N]	**Desastres naturales**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**

[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I.*]	Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	[D] disponibilidad	- [SW] aplicaciones (software) - [HW] equipos informáticos (hardware)

		En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.		- [Media] soportes de información - [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información (electrónicos) - [AUX] equipamiento auxiliar
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	- [COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	- [AUX] equipamiento auxiliar
[I.10]	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	- Media] soportes de información
[I.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.	[C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] media - [AUX] equipamiento auxiliar

		Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación		- [L] instalaciones
[E]	**Errores y fallos no intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información
[E.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	- [D.log] registros de actividad

[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	- [D.conf] datos de configuración
[E.7]	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	- [P] personal
[E.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- SW] aplicaciones (software)
[E.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	

[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[E.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	- D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones - [P] personal (revelación)
[E.20]	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	- [SW] aplicaciones (software)

[E.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	- [SW] aplicaciones (software)
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes electrónicos - [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[E.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	- [P] personal interno
[A]	**Ataques intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**

[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	- [D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	- [D.log] registros de actividad
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, puede ocasionar problemas.	[C] confidencialidad [I] integridad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- [SW] aplicaciones (software)

[A.9]	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.	[C] confidencialidad	- [COM] redes de comunicaciones
[A.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.	[I] integridad	- S] servicios - [D.log] registros de actividad

		Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	(trazabilidad)	
[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	- [COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [Media] soportes de información - [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información

				- [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	- [SW] aplicaciones (software)
[A.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	- [HW] equipos - [Media] soportes de información - [AUX] equipamiento auxiliar
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[A.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones

[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	- [L] instalaciones
[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	- [P] personal interno
[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno

ANEXO N° 6

CATALOGO DE SALVAGUARDAS SOBRE ACTIVO Y DIMENSION DE SEGURIDAD DE LA INFORMACION SEGÚN MAGERIT *(Gobierno de España, Ministerio de Hacienda y Administraciones Publicas, 2012)*

Protecciones generales u horizontales
H Protecciones Generales H.IA Identificación y autenticación H.AC Control de acceso lógico H.ST Segregación de tareas H.IR Gestión de incidencias H.tools Herramientas de seguridad H.tools.AV Herramienta contra código dañino H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión H.tools.CC Herramienta de chequeo de configuración H.tools.VA Herramienta de análisis de vulnerabilidades H.tools.TM Herramienta de monitorización de tráfico H.tools.DLP DLP: Herramienta de monitorización de contenidos H.tools.LA Herramienta para análisis de logs H.tools.HP Honey net / honey pot H.tools.SFV Verificación de las funciones de seguridad H.VM Gestión de vulnerabilidades H.AU Registro y auditoría
Protección de los datos / información
D Protección de la Información D.A Copias de seguridad de los datos (backup) D.I Aseguramiento de la integridad D.C Cifrado de la información D.DS Uso de firmas electrónicas D.TS Uso de servicios de fechado electrónico (time stamping)
Protección de las claves criptográficas
K Gestión de claves criptográficas K.IC Gestión de claves de cifra de información K.DS Gestión de claves de firma de información K.disk Gestión de claves para contenedores criptográficos K.comms Gestión de claves de comunicaciones K.509 Gestión de certificados
Protección de los servicios
S Protección de los Servicios S.A Aseguramiento de la disponibilidad S.start Aceptación y puesta en operación S.SC Se aplican perfiles de seguridad S.op Explotación S.CM Gestión de cambios (mejoras y sustituciones) S.end Terminación S.www Protección de servicios y aplicaciones web S.email Protección del correo electrónico S.dir Protección del directorio S.dns Protección del servidor de nombres de dominio (DNS)

S.TW Teletrabajo S.voip Voz sobre IP
Protección de las aplicaciones (software)
SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.start Puesta en producción SW.SC Se aplican perfiles de seguridad SW.op Explotación / Producción SW.CM Cambios (actualizaciones y mantenimiento) SW.end Terminación
Protección de los equipos (hardware)
HW Protección de los Equipos Informáticos HW.start Puesta en producción HW.SC Se aplican perfiles de seguridad HW.A Aseguramiento de la disponibilidad HW.op Operación HW.CM Cambios (actualizaciones y mantenimiento) HW.end Terminación HW.PCD Informática móvil HW.print Reproducción de documentos HW.pabx Protección de la centralita telefónica (PABX)
Protección de las comunicaciones
COM Protección de las Comunicaciones COM.start Entrada en servicio COM.SC Se aplican perfiles de seguridad COM.A Aseguramiento de la disponibilidad COM.aut Autenticación del canal COM.I Protección de la integridad de los datos intercambiados COM.C Protección criptográfica de la confidencialidad de los datos intercambiados COM.op Operación COM.CM Cambios (actualizaciones y mantenimiento) COM.end Terminación COM.internet Internet: uso de ? acceso a COM.wifi Seguridad Wireless (WiFi) COM.mobile Telefonía móvil COM.DS Segregación de las redes en dominios
Protección en los puntos de interconexión con otros sistemas
IP Puntos de interconexión: conexiones entre zonas de confianza IP.SPP Sistema de protección perimetral IP.BS Protección de los equipos de frontera
Protección de los soportes de información
MP Protección de los Soportes de Información MP.A Aseguramiento de la disponibilidad MP.IC Protección criptográfica del contenido MP.clean Limpieza de contenidos MP.end Destrucción de soportes
Protección de los elementos auxiliares

AUX Elementos Auxiliares AUX.A Aseguramiento de la disponibilidad AUX.start Instalación AUX.power Suministro eléctrico AUX.AC Climatización AUX.wires Protección del cableado
Seguridad física – Protección de las instalaciones
L Protección de las Instalaciones L.design Diseño L.depth Defensa en profundidad L.AC Control de los accesos físicos L.A Aseguramiento de la disponibilidad L.end Terminación
Salvaguardas relativas al personal
PS Gestión del Personal PS.AT Formación y concienciación PS.A Aseguramiento de la disponibilidad
Salvaguardas de tipo organizativo
G Organización G.RM Gestión de riesgos G.plan Planificación de la seguridad G.exam Inspecciones de seguridad
Continuidad de operaciones
BC Continuidad del negocio BC.BIA Análisis de impacto (BIA) BC.DRP Plan de Recuperación de Desastres (DRP)
Externalización
E Relaciones Externas E1 Acuerdos para intercambio de información y software E2 Acceso externo E3 Servicios proporcionados por otras organizaciones E4 Personal subcontratado
Adquisición y desarrollo
NEW Adquisición / desarrollo NEW.S Servicios: Adquisición o desarrollo NEW.SW Aplicaciones: Adquisición o desarrollo NEW.HW Equipos: Adquisición o desarrollo NEW.COM Comunicaciones: Adquisición o contratación NEW.MP Soportes de Información: Adquisición NEW.C Productos certificados o acreditados