FACULTAD DE POSTGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA DE GESTIÓN DE COBRANZAS

AUTORES

ROSITA LORENA CHAVEZ CABRERA
CARLOS STEVEN MOYA GAMBOA

AÑO

2022

FACULTAD DE POSGRADOS

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA DE GESTIÓN DE COBRANZAS

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magíster en Gestión de la Seguridad de la Información

Profesor

Juan Carlos López Molina

Autores

ROSITA LORENA CHAVEZ CABRERA

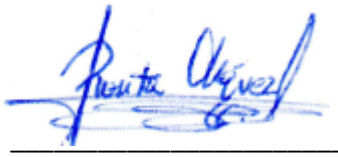
CARLOS STEVEN MOYA GAMBOA

AÑO

2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”



ROSITA LORENA CHAVEZ CABRERA

1717525172

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

CARLOS STEVEN MOYA GAMBOA

1804571576

AGRADECIMIENTO

Mi agradecimiento infinito a DIOS por haber sido mi guía y por darme la fortaleza, el entusiasmo y la sabiduría necesaria para concluir exitosamente esta etapa de mis estudios profesionales.

ROSITA LORENA CHAVEZ CABRERA

AGRADECIMIENTO

Agradezco a Dios por darme sabiduría y a mis padres que me apoyaron para lograr este sueño.

CARLOS STEVEN MOYA GAMBOA

DEDICATORIA

Con mucho cariño a mi hijo, a
quién amo con todo mi corazón y
quien ha sido mi fuente de energía
e inspiración en todo momento.
Además, para mis padres y hermano
por su apoyo y motivación constante

ROSITA LORENA CHAVEZ CABRERA

DEDICATORIA

Dedico este trabajo a mis padres.

Es por su esfuerzo y sacrificio que

pude llegar a este momento.

CARLOS STEVEN MOYA GAMBOA

Resumen

El presente proyecto tiene como objetivo elaborar un programa de seguridad de la información aplicado en una empresa de cobranzas, para proteger sus activos de información en cuanto a su confidencialidad, integridad y disponibilidad.

Inicia con la evaluación de la situación actual de la empresa respecto a seguridad de la información, utilizando los lineamientos de la norma ISO 27001 y el uso de una herramienta de evaluación de madurez de autoría propia, identificando que no se tiene un sistema de gestión de seguridad de la información y que su nivel de madurez es bajo con respecto a los requisitos de la norma.

A continuación, para clasificar la información, se identifican partes interesadas, los tipos de información y, conforme a los pilares de seguridad de la información, se determina su nivel de criticidad y apetito del riesgo institucional, los niveles de probabilidad, impacto y el etiquetado de información. Producto de esto se reconoce como información crítica de la empresa a la información de sus clientes tanto de carteras propias como de servicio, pues son la base de sus procesos de negocio.

Posteriormente, se identifican los activos empresariales asociados al procesamiento de información, evaluándolos con base en los principales criterios de seguridad de la información. De los activos analizados, se consideran la base de datos del CRM, el Firewall y una base de datos para cargas automáticas como los más críticos para el negocio y de los cuales se selecciona dos como objeto del caso de estudio.

En la siguiente etapa se identifican las amenazas y vulnerabilidades asociadas tanto para la base de datos del CRM como para el Firewall, determinando su riesgo inherente; además, se realiza un análisis de riesgos y se evalúan los controles existentes, obteniendo riesgos críticos como la destrucción de información, errores de mantenimiento y administración, abuso de privilegios, etc.

Finalmente, se crea el programa de seguridad de la información para la empresa teniendo como resultado un conjunto de actividades que incluyen capacitación y concientización del personal, procedimientos para gestión de cambios y vulnerabilidades técnicas, etc.

Abstract

The purpose of this project is to develop an information security program applied in a collection company, to protect its information assets in terms of confidentiality, integrity and availability.

It begins with the evaluation of the current situation of the company regarding information security, using the guidelines of ISO 27001 standard and a self-authored maturity assessment tool, identifying that it does not have an Information Security Management System and its level of maturity is low in respect to the requirements of the standard.

Next, in order to classify the company's information, stakeholders and the types of information are identified, according to the information security criteria. Also, their level of criticality and institutional risk appetite, the levels of probability, impact and information labeling. As a result, it is identified that the critical information of the company corresponds to own wallets client's information and service wallets, because there are the foundation of its business processes.

Subsequently, the business assets associated with information processing are identified and evaluated according to the main information security criteria. Of the assets analyzed, the CRM database, the Firewall and a database for automatic uploads are considered the most critical assets for the business and two of the assets are selected for this case study.

In the next stage, the associated threats and vulnerabilities are identified for the CRM database and Firewall**,** determining their inherent risk; In addition, a risk analysis is carried out based on the evaluation of existing controls, obtaining critical risks such as the destruction of information, maintenance and administration errors, abuse of access privileges, and others.

Finally, the information security program for the company is created, resulting in a set of activities that includes training and awareness of workers, procedures for change management and technical vulnerabilities, etc.

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Los incidentes informáticos tales como infección con códigos maliciosos, robo de información, accesos indebidos a los sistemas de información, etc., han aumentado considerablemente en los últimos años. Según el reporte de seguridad (ESET, 2021), en Latinoamérica, comparando el primer trimestre de 2020 contra el cuarto trimestre del mismo año, se registra un aumento de 704% en el número de detecciones de los ataques de fuerza bruta y un incremento de 196% en el número de usuarios con accesos remotos comprometidos. Con base en estas y otras estadísticas de seguridad, la empresa de gestión de cobranzas ha tomado conciencia de estos y otros riesgos informáticos que podrían comprometerla, por lo cual decide implementar mejoras en su nivel de seguridad de la información.

Por tal motivo, el presente proyecto brinda una propuesta de un sistema de gestión de seguridad de la información, basado en los requisitos y necesidades de la empresa. Para ello, se analiza la situación actual de la organización con respecto a seguridad de la información apoyado en la norma internacional ISO/IEC 27001:2013. Además, se realiza un análisis de los riesgos informáticos de dos de sus activos críticos usando como marco de referencia la metodología MAGERIT y la evaluación a los controles que a la fecha la empresa ha implementado para su seguridad. Adicionalmente, se evaluarán dichas acciones y se propondrán políticas y mejoras en los controles apoyadas en la norma ISO 27002.

DESARROLLO DEL PROYECTO

Objetivos

Objetivo General

Determinar las políticas, prácticas y/o lineamientos internos de Seguridad de la información de la empresa de gestión de cobranzas para proteger los activos de información de la divulgación, la modificación mal intencionada, el uso no autorizado o la indisponibilidad, para de este modo garantizar su confidencialidad, integridad y disponibilidad.

Objetivos específicos

- Determinar la situación actual de la empresa de estudio con respecto a seguridad de la información utilizando una herramienta basada en la norma ISO 27001.
- Identificar los activos de información de la organización y su nivel de criticidad.
- Analizar el riesgo asociado a dos activos críticos de la organización basados en la metodología de gestión de riesgos MAGERIT e ISO 27005.
- Evaluar los controles actuales de los activos de información críticos de la empresa.
- Proponer mejoras a los controles con base en la norma ISO 27002 para mitigar los riesgos identificados.
- Establecer políticas de seguridad de la información de alto nivel para la empresa de cobranzas.

Alcance del Proyecto

El alcance del presente proyecto es proteger la información de la empresa de gestión de cobranzas durante su ciclo de vida desde la creación, el almacenamiento y su procesamiento, así como el transporte, consulta, masificación y destrucción, para lo cual se contemplan las siguientes fases:

FASE 1.- Diagnóstico
FASE 2.- Clasificación de la información
FASE 3.- Inventario de Activos de información
FASE 4.- Análisis de amenazas y vulnerabilidades de dos activos de información críticos
FASE 5.- Programa del SGSI

Desarrollo

FASE 1.- DIAGNÓSTICO

La fase de diagnóstico tiene como objetivo conocer el estado actual de la organización con respecto a seguridad de la información. Para ello se plantea el caso de negocio de la empresa, donde se indica la problemática a resolver, los beneficios y el cronograma del proyecto. Posteriormente, mediante una herramienta diseñada por los autores y basada en la Norma ISO 27001, se determina el nivel de madurez de la empresa con respecto a seguridad de la información. Finalmente, se presenta un informe sobre el estado actual del Sistema de Gestión de Seguridad de la Información de la organización.

1.1 Análisis del Caso de Negocio

1.1.1 Problemática a resolver

En esta primera etapa se realizó una reunión preliminar con las partes interesadas de la empresa de cobranza, con el fin de identificar sus principales problemáticas, entre las cuales se encontraban:

- Accesos no autorizados a información confidencial
- Alteración de la información empresarial
- Carencia de un proceso de concientización en los trabajadores sobre la seguridad de la información
- Ataques informáticos

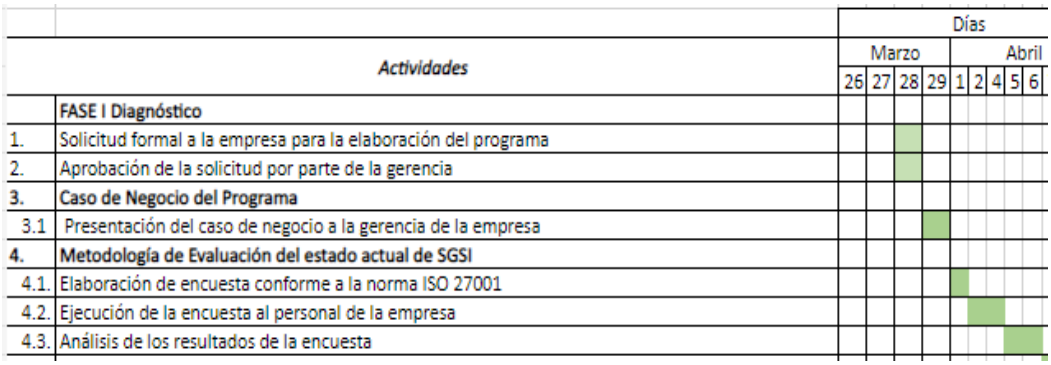
1.1.2 Beneficios del proyecto

Entre los principales beneficios de los cuales gozará la organización al final de la elaboración del presente proyecto están:

- Garantizar que únicamente el personal autorizado acceda a la información.
- Proteger a la información para evitar alteraciones indebidas.
- Concientización a los trabajadores sobre la importancia de la seguridad de la información que manejan.
- Reducir el impacto causado por las amenazas de seguridad informática.
- Disminuir la probabilidad de que los riesgos de seguridad se materialicen.
- Desarrollar la capacidad de adaptación a los cambios del entorno futuro.
- Fortalecer la competitividad empresarial al cumplir con normas y regulaciones.
- Asegurar la continuidad de los procesos críticos del negocio, mediante el diseño de una hoja de ruta que oriente a la organización respecto a la gestión de la seguridad de la información.

1.1.3 Cronograma

Con base en las etapas definidas, se plantea el cronograma, el mismo se encuentra en la sección de Anexos. En la Figura 1 se presenta un extracto.



	Actividades	Días							
		Marzo				Abril			
		26	27	28	29	1	2	4	5	6
	FASE I Diagnóstico									
1.	Solicitud formal a la empresa para la elaboración del programa									
2.	Aprobación de la solicitud por parte de la gerencia									
3.	**Caso de Negocio del Programa**									
3.1	Presentación del caso de negocio a la gerencia de la empresa									
4.	**Metodología de Evaluación del estado actual de SGSI**									
4.1.	Elaboración de encuesta conforme a la norma ISO 27001									
4.2.	Ejecución de la encuesta al personal de la empresa									
4.3.	Análisis de los resultados de la encuesta									

Figura 1 Cronograma del Proyecto (Anexo 1).

1.1.4 Conclusiones del Caso de Negocio

- Los riesgos de seguridad de la información, la necesidad de evolucionar y adaptarse a los cambios tecnológicos son los principales motivadores de la organización para la elaboración del presente programa.
- El caso de negocio brinda una visión rápida sobre las tareas a ejecutar en cada fase cumpliendo con los objetivos y alcance planteados.
- Para la elaboración del caso de negocio se requiere comprender el contexto de la empresa de estudio, para lo cual se utilizó el modelo de negocio CANVAS. Se identificaron las actividades clave de la empresa, la transparencia e innovación constante en las estrategias de cobro ofertadas a los clientes. Además, se reconocieron como recursos clave tanto los recursos físicos, como humanos e intelectuales. Así mismo, se determinó que la propuesta de valor de la organización es ofrecer un amplio y variado portafolio de opciones de pago y canales de comunicación, tanto en las carteras propias como carteras de servicio.

1.2 Evaluación del Estado Actual

En esta sección se definió el punto de partida para el desarrollo del sistema de gestión. Se analizan fortalezas y debilidades de la empresa en materia de seguridad de la información utilizando, como base de la evaluación, marcos de referencia. En esta etapa se describe la herramienta utilizada, la metodología planteada y las posibles acciones de mejora.

1.2.1 Metodología de evaluación

La herramienta diseñada para la evaluación del nivel de madurez del sistema de gestión de seguridad de la información (SGSI) de la empresa de cobranzas se basa en las cláusulas de la norma ISO/IEC 27001:2013. La Figura 2 ilustra la herramienta utilizada.

		NIVEL DE CUMPLIMIENTO					
	Pregunta	INCOMPLETO	EJECUTADO	ADMINISTRADO	DEFINIDO	GESTIONADO CUANTITATIVAMENTE	OPTIMIZADO
4	CONTEXTO DE LA ORGANIZACIÓN						
4.1	Entender a la organización y su contexto						
	¿Se han identificado los factores externos e internos pertinentes para el propósito de la organización y como afectan a la capacidad de la organización para lograr los resultados del SGSI?			X			
4.2	Entender las necesidades y expectativas de las partes interesadas						
	¿Se han determinado las partes interesadas y los requisitos relevantes para el SGSI?		X				

Figura 2 Herramienta de Evaluación (Anexo 2).

Además, se plantea un esquema de evaluación para cada una de las cláusulas, cuya calificación es otorgada de acuerdo con el nivel de cumplimiento de la empresa, respecto a cada ítem de la norma. El planteamiento de este esquema se respalda en el Modelo de Madurez de la Capacidad (CMMI) (Becerra, 2021). A continuación, se describen los niveles definidos para el uso en la herramienta de evaluación:

Tabla 1. Niveles del esquema de evaluación

Nivel	NOMBRE	DESCRIPCIÓN	Puntuación
Nivel 0	Incompleto	Cuando el proceso no se ejecuta o se hace parcialmente.	0
Nivel 1	Ejecutado	El proceso se ejecuta o es parte de una iniciativa dentro de la organización, pero no existe algo definido, por lo cual no es de cumplimiento obligatorio.	1
Nivel 2	Administrado	El proceso que se evidencia es básico, ha sido comunicado a los involucrados y es de cumplimiento obligatorio dentro de la organización.	2
Nivel 3	Definido	El proceso es proactivo y cuenta con documentación formal. Se guía en estándares de la industria o sector y es conocido por la organización	3
Nivel 4	Gestionado cuantitativamente	La calidad y rendimiento del proceso es medido y controlado para su mejora continua.	4

Nivel	NOMBRE	DESCRIPCIÓN	Puntuación
Nivel 5	Optimizado	El proceso dentro de la organización se ha convertido en un referente dentro de la industria y la empresa está centrada solo en la mejora continua	5

Adaptado de Becerra,2021

Con base en la calificación obtenida por la organización en cada pregunta de los subtemas de las cláusulas de la norma, se calcula el promedio correspondiente para conseguir el valor del **Nivel actual** de dicha cláusula. A su vez, el promedio de la calificación de cada cláusula, indica el **nivel de madurez actual de la empresa**.

Para cada una de las cláusulas se han establecido **planes de acción**. Adicionalmente, en la columna **Documentación según ISO 27001**, se refleja el nombre del documento, que debería presentar la empresa, en caso de cumplir con esa cláusula en un nivel 3 o superior. La Figura 3 muestra la estructura de la herramienta de evaluación ejecutada y la herramienta completa se encuentra en el Anexo 2.

	NIVEL DE CUMPLIMIENTO						OBSERVACIONES	NIVEL ACTUAL	NIVEL DE MADUREZ ACTUAL DE LA EMPRESA
Pregunta	INCOMPLETO	EJECUTADO	ADMINISTRADO	DEFINIDO	GESTIONADO CUANTITATIVAMENTE	OPTIMIZADO			1,137
CONTEXTO DE LA ORGANIZACIÓN								1,25	
Entender a la organización y su contexto								2	

Figura 3 Estructura de la herramienta de evaluación (Anexo 2).

1.2.2 Análisis de los resultados de la evaluación

En la tabla 2 se muestran los valores obtenidos por cada una de las cláusulas de la norma ISO 27001 evaluadas en la herramienta. La columna "**Calificación**" muestra el valor numérico obtenido por cada cláusula; mientras que, en la columna "**Porcentaje de Cumplimiento**" su equivalente en porcentaje con respecto a la norma.

Tabla 2. Resultados de la evaluación de la empresa de Cobranzas

Dominios	**Calificación**	**Porcentaje de Cumplimiento ISO 27001**
4 CONTEXTO DE LA ORGANIZACIÓN	1.25	3.57
5 LIDERAZGO	0.99	2.84
6 PLANIFICACIÓN	1	2.86
7 SOPORTE	1.67	4.76
8 OPERACIÓN	0.75	2.14
9 EVALUACIÓN DEL DESEMPEÑO	0.8	2.29
10 MEJORA	1.5	4.29
NIVEL DE MADUREZ EMPRESARIAL	**1.14**	**22.74**

En la Tabla 2 se aprecia que:

- La sección “Operación” obtiene la calificación más baja, por lo tanto, requiere la implementación de acciones de mejora.
- La sección “Evaluación del desempeño” cuenta con una valoración de 0.8 por lo que, al igual que la sección “Operación, requiere atención. De la misma forma, se recalca una gran necesidad de cuidado en la cláusula de “Liderazgo empresarial” cuya calificación es 0.99.
- En el resto de las cláusulas, tales como: contexto de la organización, planificación, soporte y mejora se obtienen calificaciones iguales o superiores a 1; sin embargo, ninguna alcanza una puntuación igual o superior a 2.

En conclusión, se identifica que la empresa de cobranzas tiene un nivel de madurez actual “**Ejecutado**”, puesto que muchas de las tareas referentes a seguridad de la información se ejecutan o son parte de una iniciativa dentro de

la organización; sin embargo, no se encuentran formalizadas y en su mayoría no son de cumplimiento obligatorio.

Las medidas implementadas en cuanto a seguridad de la información no tienen fundamento en un estándar o en una norma, se basan en la experiencia y conocimiento de quienes la implementaron; por lo tanto, deben adoptarse mejoras basadas en marcos de referencia que faciliten a la organización el planteamiento de políticas y lineamientos para preservar la confidencialidad, integridad y disponibilidad de la información.

FASE 2.- CLASIFICACIÓN DE LA INFORMACIÓN

En esta fase del proyecto se reconocen los tipos de información que maneja la institución y su grado de sensibilidad conforme a los procesos de negocio. Así también, se establecen los niveles de impacto, probabilidad y el apetito del riesgo empresarial conforme a los límites que considere tolerables o no la alta gerencia. Finalmente, se define la criticidad de los tipos de información determinados.

2.1 Identificación de las entidades de información

Conforme el contexto adquirido se identifica que en la organización se atienden dos grandes mundos de clientes que son: las carteras de servicio y las carteras propias. Con esta premisa se procede a listar cada una de las partes interesadas del negocio, entre las que se encuentran:

- Clientes Carteras Propias
- Clientes Carteras de Servicios
- Organización
- Proveedores
- Exclientes Carteras Propias (Naturales, Jurídicos)
- Exclientes Cartera de Servicios
- Empleados (Administradores, Operativos)
- Exempleados (Administradores, Operativos)
- Accionistas
- Entidades Reguladoras

2.2 Determinación de los tipos de información

A continuación, en conjunto con los responsables directos de cada dominio, se validan el tipo o tipos de datos contenidos dentro de cada entidad, con lo cual se procede a listarlos y con ello se elabora una breve descripción que nos servirá más adelante para su clasificación. La Figura 4 muestra una parte del Anexo 3.

Dominios o Entidades	Descripción del Dominio o Entidad	Tipo de información	Descripción
Clientes Carteras Propias	Clientes (Naturales, Jurídicos) de las carteras de propiedad de la empresa de cobranzas	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, ciudad
		Información de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Número de teléfono móvil, Número de telefono convencional, Dirección de domicilio, Dirección de trabajo.
		Datos de la deuda del cliente	Saldo de la deuda
		Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	El tipo de negociación que el cliente puede pactar para cubrir su deuda. Ejemplo: Promesas de Pago: Fecha de la Promesa de pago, Valor de la promesa de Pago Acuerdo de Pago: Fecha del acuerdo, descuento, Entrada, Número de Cuotas, Valor de las cuotas.

Figura 4 Dominios y Tipos de Información con su descripción (Anexo 3)

2.3 Definición del Apetito de Riesgo Empresarial

Para poder definir el apetito del riesgo dentro de la empresa se tomó como referencia los parámetros de tipología de impacto de la norma de Riesgo Operativo, los mismos se pueden observar en la Tabla 3.

Tabla 3. Parámetros de tipología de Impacto - Norma de Riesgo Operativo

A. Parámetros para Tipología de Impacto
1. Pérdidas financieras.
2. Multas y Sanciones de los Organismos de Control.
3. Interrupción de operaciones parciales y/o totales.
4. Pérdida / Degradación de la imagen institucional.
5. Demandas judiciales, afectación legal.
6. Pérdidas / Destrucción / afectación de bienes materiales.
7. Pérdida de vida / afectación de la salud de las personas.
8 Lucro cesante.
9. Observaciones de auditoría internas o externas.
10. Afectación al clima laboral.

A partir de ellos, se consideró otros tipos de impacto que actualmente aquejan la realidad de la organización, para lo cual los parámetros elegidos para este estudio fueron:

- Interrupción de Operaciones.
- Modificaciones de la información.
- Divulgación de la información.

Para esta definición también es importante resaltar el concepto de Aceptación del Riesgo que no es más que la decisión informada de tomar o no un riesgo particular. La aceptación del riesgo puede ocurrir sin el tratamiento de un riesgo o durante el proceso del tratamiento de riesgos. (Global Trust Association, 2022)

Por tal motivo, en reunión con personal administrativo de la empresa se plantearon tres niveles para la aceptación de un riesgo determinado, estos son:

- Aversión.
- Neutral.
- Agresivo.

Con estos insumos se define el apetito del riesgo de la empresa de gestión de cobranzas, conforme al detalle de la Figura 5.

APETITO DEL RIESGO			
Impacto	**Aversión**	**Neutral**	**Agresivo**
Interrupción de operaciones		Dependiendo del tiempo de interrupción	
Modificaciones de la información		Depende si la modificación fue o no autorizada y del tipo de información que se modifique.	
Divulgación de información		Depende del tipo de información divulgada.	

Figura 5 Apetito del Riesgo Empresarial (Anexo 4).

2.4 Tipología de impacto

Basados en el apetito del riesgo plateado en la sección anterior, en la Figura 6 se detalla el tipo de impacto que puede causar en la organización y sus diferentes niveles.

Niveles	Interrupción de operaciones	Modificaciones de la información	Divulgación de información
CATASTRÓFICO	Implica malestar en los clientes internos y externos por paralización total de las operaciones empresariales	Se realizan modificaciones no autorizadas de la información confidencial de los clientes internos y externos de la empresa.	Cuando se ha divulgado información confidencial de los clientes internos y externos de la empresa.
MAYOR	Implica malestar en los clientes internos y externos por paralización parcial de las operaciones de la gestión de cobranza	Cuando se realizan modificaciones no autorizadas de la información restringuida de los clientes internos y externos de la empresa.	Cuando se ha divulgado información restringuida de los clientes internos y externos de la empresa
MODERADO	Implica malestar al interior de la organización por problemas de paralización de operaciones	Cuando se realizan modificaciones no autorizadas de la información privada de los clientes internos y externos de la empresa.	Cuando se ha divulgado información privada de los clientes internos y externos de la empresa.
MENOR	Implica malestar en un área específica dentro de la empresa por paralización de sus actividades	Cuando se realizan modificaciones no autorizadas de la información de uso interno de la empresa.	Cuando se ha divulgado información de uso interno de la empresa.
INSIGNIFICANTE	Implica malestar de una persona al interior de la empresa por paralización de sus actividades.	Cuando se realizan modificaciones no autorizadas de la información de uso público de la empresa	Cuando se ha divulgado información de uso público de la empresa

Figura 6 Tipología de impacto (Anexo 5).

2.5 Etiquetado de la información

La empresa de cobranzas maneja distintos tipos de información de sus clientes como: nombres, números de teléfono de contacto, convenios de pago, etc. Cada dato cuenta con un nivel de importancia diferente y su divulgación no autorizada involucra un impacto distinto para la empresa. Según el nivel asignado en la confidencialidad, se clasificó la información de la empresa con una etiqueta acorde a lo ilustra la Figura 8.

Niveles	ETIQUETADO
CATASTRÓFICO	CONFIDENCIAL
MAYOR	RESTRINGIDA
MODERADO	PRIVADA
MENOR	USO INTERNO
INSIGNIFICANTE	PÚBLICO

Figura 7 Etiquetado de la información (Anexo 6).

2.6 Calificación del tipo de información

Para asignar una calificación a cada tipo de información, se analizó el impacto de cada uno con respecto a la disponibilidad, integridad y confidencialidad utilizando la escala numérica de la Figura 8.

Niveles	Disponibilidad	Integridad	Confidencialidad
CATASTRÓFICO	5	5	5
MAYOR	4	4	4
MODERADO	3	3	3
MENOR	2	2	2
INSIGNIFICANTE	1	1	1

Figura 8 Escala numérica para calificación.

Para determinar la calificación asignada a cada tipo de información se obtuvo una valoración media de los tres objetivos de seguridad de la información, de acuerdo con los criterios establecidos en la Figura 9, se asignó la valoración correspondiente.

Niveles	Condición
CATASTRÓFICO	Si la valoración media es superior a 4
MAYOR	Si la valoración media es superior o igual a 3 y menor o igual a 4
MODERADO	Si la valoración media es superior o igual a 2 y menor a 3
MENOR	Si la valoración media es superior o igual a 1 y menor a 2
INSIGNIFICANTE	Si la valoración media es superior o igual a 0 y menor a 1

Figura 9 Criterios de valoración para tipos de información.

Finalmente, se indica el dueño o responsable de la entidad estudiada y la fecha de actualización del tipo de información. En el Anexo 3, se puede observar la tabla de calificación y cada uno de los aspectos evaluados anteriormente. La Figura 10 muestra parte del anexo.

Dominios o Entidades	Descripción del Dominio o Entidad	Tipo de información	Descripción	Disponibilidad Asegurar el acceso y uso de la información y los sistemas en el momento oportuno	Integridad Preservación de la información	Confidencialidad La protección de la información de accesos no autorizados
Clientes Carteras Propias	Clientes (Naturales, Jurídicos) de las carteras de propiedad de la empresa de cobranzas	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, ciudad	CATASTRÓFICO	MAYOR	MAYOR
		Información de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Número de teléfono móvil, Número de telefono convencional, Dirección de domicilio, Dirección de trabajo.	CATASTRÓFICO	MAYOR	CATASTRÓFICO
		Datos de la deuda del cliente	Saldo de la deuda	CATASTRÓFICO	CATASTRÓFICO	MAYOR
		Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	El tipo de negociación que el cliente puede pactar para cubrir su deuda. Ejemplo: Promesas de Pago: Fecha de la Promesa de pago, Valor de la promesa de Pago Acuerdo de Pago: Fecha del acuerdo, descuento, Entrada, Número de Cuotas, Valor de las cuotas.	CATASTRÓFICO	MAYOR	MAYOR

Figura 10 Tabla de tipos de información y su calificación (Anexo 3)

2.7 Resultados de la clasificación de la información

De acuerdo con el análisis realizado y los valores obtenidos en la clasificación de la información se determinó que:

- En la entidad “Organización”, los datos de las proyecciones de estrategia de sus clientes sean de carteras de servicios o propias, tienen una criticidad mayor a diferencia de los datos de las compras de carteras propias y los datos de las asignaciones de carteras de servicios cuya criticidad es catastrófica. Además, los datos de actas y decisiones de juntas directivas o comités son importantes y deben estar disponibles en cualquier momento, razón por la cual cuentan con una criticidad moderada.

- En la entidad “Proveedores” se determinó que, el tipo de información con un nivel de criticidad mayor corresponde al código fuente del CRM que utiliza la organización.

- Conforme al apetito de riesgo de la organización, los tipos de información asociados a las entidades “Exclientes Carteras Propias” y “Exclientes Cartera de Servicios” cuentan con una criticidad menor y moderada respectivamente.

- La información de empleados, accionistas y entidades reguladoras tienen una clasificación “moderada” y requiere ser considerada ya que al ser información de la formación, avances y finanzas de la empresa necesita estar protegida.

- La información relacionada con la entidad “Exempleados” cuenta con una clasificación de tipo de información “menor”, al ser información histórica.

- Finalmente, los dominios Clientes Carteras Propias y Clientes Carteras de Servicios son los más importantes para la empresa. En estas entidades el impacto de la divulgación no autorizada de los tipos de información, referentes a los datos de contacto, es “Catastrófico”. La disponibilidad e integridad de esta información, dependiendo el tipo de dato, tendría un impacto “mayor” o “catastrófico”. Sin lugar a duda, esta información es la más valiosa para la empresa de cobranzas, lo cual resulta lógico al tratarse de los datos de sus clientes y de las deudas que mantienen. Adicionalmente, la información contenida en estas entidades es de carácter restringido y confidencial, razón por la cual en el presente proyecto se consideró analizar y proteger los activos de información que las contienen.

FASE 3.- Inventario de Activos de información

En esta etapa del proyecto se analizan los activos asociados a los tipos de información que maneja la empresa. Se establece una codificación tanto para el tipo de información como para el activo. De acuerdo con la evaluación grupal de la clasificación del tipo de información, se determina la criticidad del activo. Finalmente, se asigna un custodio para cada activo y una dependencia en el caso de existir.

3.1 Listado de activos empresariales

La empresa de cobranzas cuenta con una amplia cantidad de activos; sin embargo, para el presente trabajo, se profundiza en los que se encuentran asociados a los dominios “Clientes Carteras Propias” y “Clientes Carteras Servicios” al ser los principales dominios de la empresa. Para reconocer a cada activo de información se le asignó un número como en el ejemplo de la Figura 11.

Código del activo	Nombre del Activo de información
1	Base de datos del CRM
2	Base de datos Analítica
3	Base de Datos – Cargas Automáticas
4	DOCSERVER
5	BPM
6	CRM

Figura 11 Codificación de activos. (Anexo 7)

3.2 Identificación de los tipos de información en cada activo

Cada activo de la empresa contiene uno o varios tipos de información. Para el estudio, a cada tipo de información se la asignó un código alfanumérico diferente y se los ubicó dentro de su activo correspondiente. En la Figura 12 se muestra un extracto.

Codificación del Tipo de información	Tipo de Información
BBDE-ACCP-001	Datos Personales del cliente
BBDE-ACCP-002	Información de Contacto del cliente
BBDE-ACCP-003	Datos de la deuda del cliente
BBDE-ACCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)
BBDE-ACCS-001	Nombres y apellidos, Número de cédula o RUC, estado civil, ciudad
BBDE-ACCS-002	Correo electrónico personal, correo electrónico laboral, Numeros de teléfono móvil, Numeros de telefono convencional, Dirección de domicilio, Dirección de
BBDE-ACCS-003	Saldos de la deuda (Saldos Total, Saldo Ajustado)
BBDE-ACCS-004	Promesas o Acuerdos donde se detalla el método de pago del cliente.
BBDE-XCCP-001	Datos Personales del cliente

Figura 12 Codificación de los tipos de Información (Anexo 7)

3.3 Determinación de la criticidad de los activos de información

Para definir la criticidad de cada activo se tomó en cuenta la clasificación de los tipos de información que contiene. El nivel de criticidad asignado depende del nivel de la clasificación del tipo de información más relevante; por ejemplo, si al menos uno de los tipos de información es catastrófico, por consiguiente, la criticidad del activo también lo será. Además, se señaló al custodio de cada activo y la dependencia de cada uno con respecto a otro activo, en el caso de que exista. La Figura 13 ilustra un ejemplo de lo mencionado.

Código del activo	Nombre del Activo de información	Codificación del Tipo de información	Tipo de Información	Clasificación del tipo de información	Criticidad del activo	Dependencia	Custodio
1	Base de datos del CRM	BBDE-ACCP-001	Datos Personales del cliente	CATASTRÓFICO	CATASTRÓFICO	9	Coordinador de Estrategias de Carteras Propias (CECP) / Gerente de Operaciones (GO) /Gerente de TI
		BBDE-ACCP-002	Información de Contacto del cliente	CATASTRÓFICO			
		BBDE-ACCP-003	Datos de la deuda del cliente	CATASTRÓFICO			
		BBDE-ACCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	CATASTRÓFICO			
		BBDE-ACCS-001	Nombres y apellidos, Número de cédula o RUC, estado civil, ciudad	CATASTRÓFICO			Coordinador de Estrategias de Carteras de Servicios (CECS) / Gerente de Operaciones (GO) / Gerente de TI
		BBDE-ACCS-002	Correo electrónico personal, correo electrónico laboral, Numeros de teléfono móvil, Numeros de telefono convencional, Dirección de domicilio, Dirección de	CATASTRÓFICO			
		BBDE-ACCS-003	Saldos de la deuda (Saldos Total, Saldo Ajustado)	CATASTRÓFICO			
		BBDE-ACCS-004	Promesas o Acuerdos donde se detalla el método de pago del cliente.	CATASTRÓFICO			

Figura 13 Activos de Información con criticidad, dependencia y custodio (Anexo 7)

3.4 Conclusiones de la fase Inventario de Activos de información

Finalizado el análisis del inventario de activos, se presentan los siguientes hallazgos:

- El activo “Base de datos del CRM” está conformado por 16 tipos de información y la mitad de ellos cuenta con una clasificación “Catastrófico”, por lo que la criticidad del activo es “Catastrófico”. Este activo tiene dependencia del activo 9 “Servidor de la base de datos del CRM” y cada tipo de información tiene un custodio distinto dependiendo de la información que se trate (Para mayor detalle consulte el anexo 7)
- El activo “Firewall” cuenta con un solo tipo de información correspondiente a las reglas de seguridad de la red empresarial; por ende, su clasificación y criticidad es “Catastrófico” y no tiene dependencia con ningún otro activo de la empresa.
- El activo “Servidor de la base de datos del CRM” contiene a la base de datos del CRM y por lo tanto a los 16 tipos de información de dicha base, la información correspondiente a los exclientes de carteras propias tiene una clasificación “Menor”; no obstante, ocho de ellos poseen clasificación “Catastrófico”, por lo cual se vuelve un activo con criticidad “Catastrófico”.
- Los activos Base de datos Analítica, el CRM, APP – Domiciliarios, Servidor de Base de datos de Analítica, Servidor web del CRM y Servidor

web de App – Domiciliarios cuentan con una criticidad “Mayor”, puesto que se trata de activos necesarios para la operación de la organización.

- Los activos DOCSERVER, BPM y el Servidor BPM cuentan con una criticidad “Moderado”, puesto que la información que manejan es de uso propio de la organización y no impactan en los procesos críticos del negocio.

En resumen, se determina que la base de datos del CRM es uno de los activos de la organización con el mayor grado de criticidad, Catastrófico. Por tal motivo, para el presente proyecto se decide ejecutar el análisis de riesgos de la base de datos del CRM y, como segundo elemento se seleccionó al Firewall ya que tiene el mismo tipo de criticidad. De este modo, se analizará el riesgo tanto para un implemento de hardware como para uno de software.

FASE 4.- Análisis de Amenazas y Vulnerabilidades de activos críticos

En esta etapa del proyecto se describen y evalúan las amenazas y vulnerabilidades asociadas a los dos activos de información seleccionados, determinando el impacto organizacional causado y el impacto en cuanto a la disponibilidad, confidencialidad e integridad de la información. Las amenazas y vulnerabilidades se asocian a un riesgo y este se analiza para obtener el impacto, probabilidad y severidad inherentes. Posteriormente, se examinan los controles con los que cuenta la empresa referente a dichos riesgos y se determina el nivel de mitigación del riesgo en cuanto a probabilidad e impacto para obtener el riesgo residual.

4.1 Identificación de las amenazas y vulnerabilidades

En este punto es indispensable tener presente los conceptos de **amenaza** que es la causa potencial de un incidente no deseado que puede ocasionar daño al sistema u organización. Así como el concepto de **vulnerabilidad** como la debilidad de un activo o control que puede ser explotada por una o más amenazas. (Normaiso27001, s.f.)

Estos conceptos son la base para la elección adecuada de las amenazas y vulnerabilidades. Adicionalmente, se utilizó el anexo D de la Norma ISO 27005 y los tipos de activos de la metodología MAGERIT 3.0, de tal manera que se identificó el tipo de activo al que pertenece, ya sea la base de datos o el Firewall, sus amenazas, el origen y el impacto que generan en cuanto a disponibilidad, integridad y confidencialidad.

Igualmente, dentro del análisis se consideró el impacto organizacional, para el cual se planteó las siguientes categorías: Financiero, operacional, legal y reputacional. La Figura 14, muestra parte de lo indicado:

Nombre del Activo de información	Tipo de Activo	Amenazas	Origen	Cod. Vulnerabilidad	Vulnerabilidades	Impacto en	Impacto Organizacional
Base de datos del CRM	[D] Datos / Información	Destrucción de información	D	V1.1.1	- Falta de concienciación en el personal que administra los datos (sobre integridad, disponibilidad, confidencialidad de la información)	Disponibilidad	Financiero, Operacional
				V1.1.2	- Falta de procedimientos para el manejo de información clasificada		
				V1.1.3	- Información sin encriptación		
		Divulgación de información	D,A	V1.1.1	- Falta de concienciación en el personal que administra los datos (sobre seguridad y privacidad de la información)	Confidencialidad	Financiero, Legal, Reputación
				V1.1.2	- Falta de procedimientos para el manejo de información clasificada		
				V1.2.1	- Falta de mecanismos de monitoreo establecidos para violaciones de seguridad lógica		

Figura 14 Amenazas, Vulnerabilidades, Impacto en Seguridad de la información e Impacto Organizacional. (Anexo 8)

Previo a iniciar el estudio de riesgos de las amenazas y vulnerabilidades identificadas se establece los niveles de impacto y probabilidad descritos en las secciones subsiguientes que servirán para la obtención de los riesgos tanto inherente como residual.

4.2 Niveles de Impacto

Se plantea los niveles de impacto basados en el grado de tolerancia al riesgo por parte de la empresa. Dentro de cada nivel se establece una breve descripción conforme el tipo de impacto correspondiente, de acuerdo con lo descrito en la Figura 15.

Niveles de Impacto	Descripción
CATASTRÓFICO	internos y externos por paralización total de las operaciones empresariales
MAYOR	interno y externos por paralización parcial de las operaciones de la gestión de cobranza
MODERADO	Implica malestar al interior de la organización por problemas por paralización de operaciones
MENOR	Implica malestar en un área específica dentro de la empresa por paralización de sus actividades
INSIGNIFICANTE	Implica malestar de una persona al interior de la empresa por paralización de sus actividades

Figura 15 Niveles de Impacto empresa de cobranzas (Anexo 6)

4.3 Niveles de Probabilidad

Considerando a la probabilidad como la certeza o no de que un evento ocurra (Normaiso27001, s.f.), se plantearon los siguientes niveles de probabilidad que constan en la Figura 16, para usarlos a lo largo de este trabajo:

Nivel de Probabilidad	Descripción
CIERTO	Cuando se tiene certeza del 80% de la ocurrencia de la amenaza
PROBABLE	Cuando se tiene certeza entre el 50 y 79% de la ocurrencia de la amenaza
POSIBLE	Cuando la certeza de la materialización de la amenaza está entre el 30% y 49%
IMPROBABLE	Cuando la certeza de la ocurrencia de la amenaza está entre el 6% y 29%
EXCEPCIONAL	Cuando la certeza de la materialización de la amenaza es menor al 5%

Figura 16 Niveles de Probabilidad empresa de cobranzas (Anexo 6).

4.4 Creación del Mapa de Calor

Para esta etapa se establecieron tres niveles de severidad de la Figura 17:

NIVEL SEVERIDAD	DESCRIPCIÓN
CRÍTICA	- Cuando el riesgo tiene un impacto grande (catastrófico, mayor) y es muy probable que ocurra (cierto, probable, posible) - Requiere acciones inmediatas de la gerencia general - Incluye pérdidas financieras que pueden provocar el cierre de la empresa.
MODERADA	- Cuando el riesgo causa cualquier tipo de impacto que depende de su probabilidad de ocurrencia - Requiere acción de mandos medios (jefes de área)
BAJA	- Cuando el riesgo tiene un impacto moderado, menor, insignificante y su probabilidad de ocurrencia es improbable, excepcional -Requiere controles rutinarios

Figura 17 Niveles de Severidad (Anexo 6)

Tomando en cuenta los niveles de impacto planteados en el apartado 4.2 y los niveles de probabilidad de la sección 4.3, se formó el mapa de calor, tal cual lo ilustra la Figura 18:

		IMPACTO				
		CATASTRÓFICO	MAYOR	MODERADO	MENOR	INSIGNIFICANTE
PROBABILIDAD	CIERTO	CRÍTICA	CRÍTICA	MODERADA	MODERADA	MODERADA
	PROBABLE	CRÍTICA	CRÍTICA	MODERADA	MODERADA	MODERADA
	POSIBLE	CRÍTICA	MODERADA	MODERADA	MODERADA	MODERADA
	IMPROBABLE	MODERADA	MODERADA	BAJA	BAJA	BAJA
	EXCEPCIONAL	MODERADA	MODERADA	BAJA	BAJA	BAJA

Figura 18 Mapa de Calor

4.5 Determinación del riesgo inherente de los activos críticos

En esta sección, a cada vulnerabilidad y riesgo identificados por cada activo crítico se asignó un código y se procedió a calificar el Nivel de Impacto y Probabilidad inherentes para, con base en ellos obtener el nivel de severidad del riesgo inherente, tal como el ejemplo de la Figura 19:

Identificación del riesgo	INHERENCIA		
ID Riesgo	IMPACTO RI	PROBABILIDAD RI	SEVERIDAD RI
R1.1	CATASTRÓFICO	PROBABLE	CRÍTICA
R1.2	MODERADO	PROBABLE	MODERADA
R1.3	CATASTRÓFICO	CIERTO	CRÍTICA

Figura 19 Calificación Riesgo Inherente. (Anexo 8)

Al mismo tiempo, se construyó el mapa de calificación de este análisis, parte del resultado se evidencia en la Figura 20.

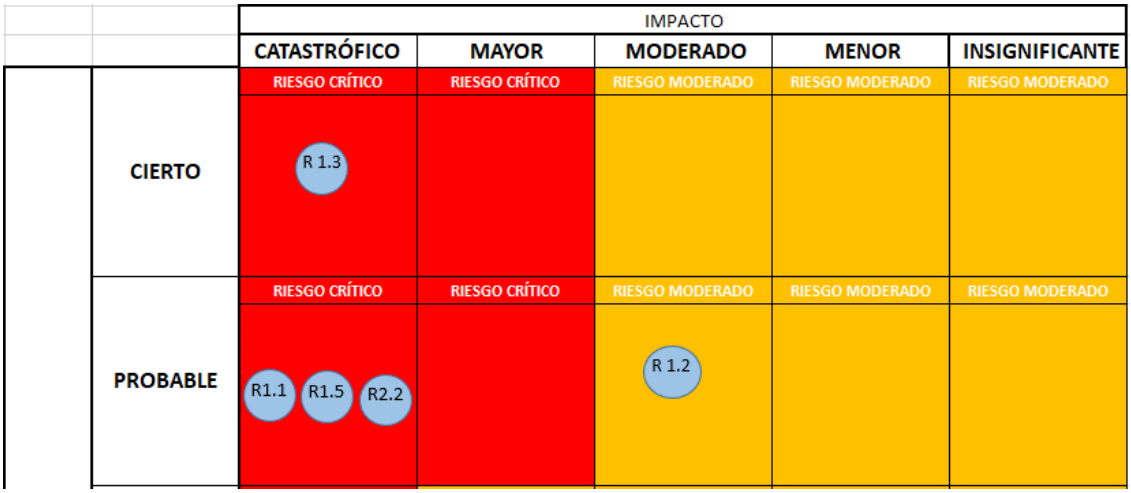


Figura 20 Mapa de Calificación Riesgo Inherente (Anexo 9)

4.6 Evaluación de los Controles Existentes

Para determinar la fortaleza de los controles ya implementados por la empresa en la mitigación de los riesgos inherentes, se identificaron los controles y posteriormente se realizó una evaluación a los mismos considerando las siguientes características:

Vulnerabilidades controladas

En esta columna se enlistan todas las vulnerabilidades en las cuales el control es aplicado. Se tomó en cuenta que un control puede influenciar en una o varias vulnerabilidades, un ejemplo en la Figura 21:

Cód. Control	Controles (que existen ahorita relacionados con la vulnerabilidad)	Vulnerabilidades que Controla
CON-001	Campañas de concientización sobre phishing.	V.1.1.1 V.1.1.3 V.1.2.1 V.1.4.3

Figura 21 Criterio Vulnerabilidades Controladas

Tipo de control

Para este criterio se consideró si el control es preventivo, detectivo o correctivo y se asignó un valor numérico de acuerdo con la Figura 22:

Criterio de Calificación por Preventivo, Correctivo, Detectivo
Preventivo=3 Detectivo=2 Correctivo=1

Figura 22 Criterio de calificación por Tipo de Control.

Automatización

De acuerdo con la Figura 23, los controles fueron evaluados con base en su automatización y dependiendo del tipo se asignó un valor numérico, así:

Criterio de Calificación por Automatización
Automático= 3 Mixto=2 Manual=1

Figura 23 Criterio de calificación para automatización.

Segregación de funciones

En caso de que el control permita la segregación de funciones, se le asignó un valor de “2” puntos; mientras que, en caso de no permitirlo, un valor de “0” puntos, como se evidencia en la Figura 24:

Criterio de Calificación por Segregación de Funciones
Si= 2 No=0

Figura 24 Criterio de calificación para segregación de funciones.

Cumplimiento obligatorio

Para este criterio se consideró si el control es de cumplimiento obligatorio dentro de la organización; se asignó un valor según la escala numérica de la Figura 25.

Criterio de Calificación por Cumplimiento
Si= 2
No=0

Figura 25 Criterio de calificación para cumplimiento.

Número de vulnerabilidades controladas

La calificación se asignó conforme los criterios de la Figura 26. Así, mientras mayor sea el número de vulnerabilidades controladas, mayor es el valor numérico.

Criterio de Calificación por Vulnerabilidades Contrarestadas
cubre 10 o más vulnerabilidades = 4
cubre 5 a 9 vulnerabilidades =3
cubre entre 3 y 4 vulnerabilidades = 2
cubre entre 1 y 2 vulnerabilidades= 1

Figura 26 Criterio de calificación por número de vulnerabilidades controladas.

Mitigación

En este criterio se analizó si el control disminuye el nivel de impacto, probabilidad o ambos del riesgo inherente. La asignación numérica se realizó con los criterios de la Figura 27:

Criterio de Calificación por mitigación
AMBOS= 3
PROBABILIDAD=2
IMPACTO=1
NADA= 0

Figura 27 Criterio de calificación por mitigación

Calificación y fortaleza del control

Finalmente, se obtiene una valoración final de todos los criterios evaluados y se determina la fortaleza del control.

Mediante los criterios de la Figura 28 se determinó si el control es débil, moderado o fuerte.

Criterio de Fortaleza del control
Calificación de >=5 y < 10 DÉBIL Calificación >=10 y <15 MODERADO Calificación >=15 FUERTE

Figura 28 Criterio de fortaleza del control

En la Figura 29, se observa el parte del resultado final de la evaluación de los controles. En el Anexo 10, se describen con mayor detalle los valores obtenidos en la evaluación de cada uno de los controles.

			Tipo de Control				Otros Criterios de Evaluación de Controles	
Cód. Control	Controles (que existen ahorita relacionados con la vulnerabilidad)	Vulnerabilidades que Controla	Preventivo	Detectivo	Correctivo	Automatización	Segregación de Funciones	Cumplimiento Obligatorio?
CON-001	Campañas de concientización sobre phishing.	V.1.1.1 V.1.1.3 V.1.2.1 V.1.4.3	X			Semi-Automático	N/A	NO
CON-002	Acuerdos de confidencialidad con el personal de la empresa	V.1.3.3 V.1.4.2 V.2.3.1	X			Manual	NO	SI
CON-003	Monitoreo periódico de los respaldos de base de datos	V.1.1.3 V.1.3.1	X	X		Semi-Automático	NO	NO

Figura 29 Evaluación de controles existentes (Anexo 10).

4.7 Calificación del Grupo de Controles

En esta sección se agrupan los controles dependiendo el riesgo que resuelven, de tal forma que nos permita definir la mitigación de impacto y probabilidad conforme a la valoración de la Figura 30:

Valoración del GC
GC tiene 1 a 2 controles que mitigan impacto o probabilidad es DÉBIL
Si GC tiene 3 a 4 controles que mitigan impacto o probabilidad es MODERADO
Si GC tiene 5 controles en adelante que mitigan impacto o probabilidad es FUERTE

Figura 30 Valoración para los grupos de controles

En la Figura 31, se puede observar un extracto del proceso de calificación realizado a los grupos de controles de los activos de estudio. El detalle completo de esta valoración consta en el Anexo 11.

RIESGO	PROMEDIO CALIFICACION GC	CONTROLES SELECCIONADOS	Reduce	CANTIDAD IMPACTO	CANTIDAD PROBABILIDAD	CANTIDAD AMBOS	MITIGACION PROBABILIDAD	MITIGACION IMPACTO
R. 1.1	11.6	CON-001	Probabilidad	0	2	3	FUERTE	MODERADO
		CON-002	Probabilidad					
		CON-003	Ambos					
		CON-004	Ambos					
		CON-005	Ambos					
R. 1.2	12.25	CON-001	Probabilidad	0	2	2	MODERADO	DÉBIL
		CON-002	Probabilidad					
		CON-004	Ambos					
		CON-005	Ambos					
R. 1.3	13	CON-002	Probabilidad	0	1	3	MODERADO	MODERADO
		CON-003	Ambos					
		CON-004	Ambos					
		CON-005	Ambos					

Figura 31 Calificación de los grupos de controles (Anexo 11)

4.8 Determinación del riesgo residual de los activos críticos

Una vez identificadas las fortalezas de los controles existentes en la empresa de cobranzas, en la matriz de riesgos, se volvió a evaluar cada uno de los riesgos de los dos activos críticos, teniendo en cuenta que, al aplicar controles, los niveles de impacto o la probabilidad de ocurrencia varían de acuerdo con la Figura 32:

Definición para el cálculo del Riesgo Residual
Si la mitigación de impacto o probabilidad es fuerte entonces baja dos niveles
Si la mitigación de impacto o probabilidad es moderada entonces baja 1 nivel
Si la mitigación de impacto o probabilidad es débil el nivel de riesgo se mantiene

Figura 32 Criterios para calificación del Riesgo Residual

Aplicando los criterios antes indicados. Se obtuvieron los resultados de los riesgos residuales. La Figura 33, contiene un ejemplo y en el Anexo 8 se encuentra el detalle completo.

Identificación del riesgo	INHERENCIA			GRUPO DE CONTROLES		RESIDUAL		
ID Riesgo	IMPACTO RI	PROBABILIDAD RI	SEVERIDAD RI	Mitigación de Probabilidad	Mitigación de Impacto	IMPACTO RR	PROBABILIDAD RR	SEVERIDAD RR
R1.1	CATASTRÓFICO	PROBABLE	CRÍTICA	FUERTE	MODERADO	MAYOR	IMPROBABLE	MODERADA
R1.2	MODERADO	PROBABLE	MODERADA	MODERADO	DÉBIL	MODERADO	POSIBLE	MODERADA

Figura 33 Calificación Riesgo Residual (Anexo 8)

Finalmente, se representó estos riesgos en el mapa de calor del presente análisis, como se muestra en la Figura 34.

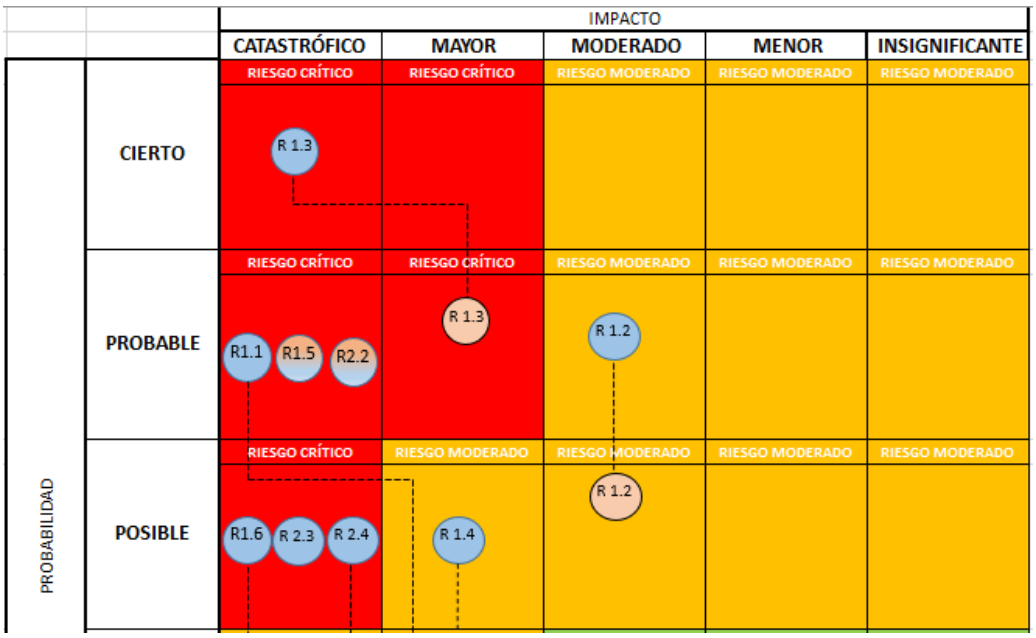


Figura 34 Mapa de Calificación de Riesgo Residual (Anexo 12)

4.8 Resultados del Análisis de Amenazas y Vulnerabilidades de los activos críticos

Primer Activo Crítico: Base de datos del CRM

Se trata de un tipo de activo de la categoría Datos / Información, el cual tiene como amenazas:

- La destrucción de la información tiene un origen “Deliberado”; además, dentro de la empresa, se ha identificado: falta de concientización en el personal que administra los datos, falta de procedimientos para el manejo de información clasificada e información sin encriptación, lo cual causaría impacto en la disponibilidad de los datos junto con un impacto operacional y financiero inherentemente crítico, frente al cual los controles adoptados son fuertes para mitigar la probabilidad y moderado en cuanto a mitigación del impacto, lo cual transforma la severidad residual de este riesgo en moderada.
- La divulgación de información, cuyo origen es deliberado y accidental. Se ha identificado que existe por: falta de concientización en el personal que administra los datos, falta de procedimientos para el manejo de información clasificada y falta de mecanismos de monitoreo establecidos para violaciones de seguridad lógica. Esta amenaza tiene un impacto en la confidencialidad de la información; igualmente presenta un impacto organizacional que afecta los aspectos: financiero, legal y a la reputación, dando una severidad inherente “Moderada”. Los controles adoptados por la empresa presentan una mitigación moderada y débil en cuanto a probabilidad e impacto respectivamente. La fortaleza de los controles presenta una disminución tan solo en la probabilidad del riesgo residual; por lo tanto, la severidad se mantiene en “Moderada”.
- La pérdida parcial o total de la información, cuyo origen es deliberado, accidental y ambiental. Puede ocasionarse por: Administración inadecuada de los respaldos de información, falta de mecanismos de identificación y autenticación de usuarios y falta de un procedimiento

formal para el alta y baja de usuarios. Todo ello conlleva a que exista un impacto en la disponibilidad de la información, además de un impacto organizacional financiero y operacional, determinando así que la severidad inherente es “Crítica”. Los controles adoptados por la empresa presentan una mitigación moderada en el impacto y en la probabilidad. A pesar de que el riesgo residual disminuye a mayor y probable en impacto y probabilidad, respectivamente, la severidad inherente sigue siendo crítica.

- Alteración y/o modificación no autorizada de la información por parte del personal de la empresa, cuyo origen es deliberado y accidental. Existe por: falta de procedimientos formales para control de cambios, falta de responsabilidades de seguridad de la información en las descripciones de puestos de trabajo y mala gestión de contraseñas, lo que conlleva a un impacto en la integridad de la información. Además, presenta un impacto organizacional en la reputación, en el ámbito legal y operacional. Su severidad inherente se identifica como “Moderada”. Los controles con los que cuenta la empresa proporcionan una mitigación fuerte en cuanto a la probabilidad y moderada en cuanto al impacto, resultando en una disminución de la severidad a baja.
- Abuso de privilegios de acceso, cuyo origen es deliberado y ambiental. Se ha identificado que existe: Mala administración de los perfiles y permisos de usuario, falta de un proceso formal y periódico de revisión de los derechos de acceso y falta de revisiones periódicas a los logs de la base de datos. Esto implica un impacto en la confidencialidad, integridad y disponibilidad de la información, además genera un impacto organizacional tanto legal como reputacional. La severidad inherente con la que cuenta es crítica. Los controles organizacionales ya establecidos presentan una mitigación débil, tanto para la probabilidad como para el impacto, manteniendo el nivel de severidad residual en crítica.
- Errores del administrador, cuyo origen es deliberado y ambiental. Se presentarían por: falta de aplicación de actualizaciones en el motor de base datos, instalación incorrecta del software de base de datos y

configuración incorrecta de parámetros, lo que ha derivado en un impacto a la confidencialidad, integridad y disponibilidad de la información; además de implicar impacto organizacional operacional y financiero. La severidad inherente es “Crítica”. Los controles con los que cuenta la organización presentan una mitigación moderada tanto en impacto como en probabilidad lo que permite que, el impacto residual cambie a mayor y la probabilidad a improbable y como resultado la severidad es “Moderada”.

El activo “Base de datos del CRM” a pesar de los controles adoptados por la empresa cuenta con dos riesgos residuales con severidad crítica que son la pérdida parcial o total de información y el abuso de privilegios de acceso, para ellos se trabajará en la mejora de los controles con la formulación de planes de acción. Además, aún se tienen tres riesgos residuales con severidad moderada y un riesgo residual con severidad baja.

Segundo Activo Crítico:

Se trata de un tipo de activo de la categoría Equipamiento informático (Hardware), el cual tiene como amenazas:

- Desastres naturales como: fuego, daños por agua y otros. Esta amenaza tiene un origen ambiental. Se ha identificado que se materializaría por: Mal funcionamiento del sistema contraincendios, ubicación del data center en una zona susceptible a inundaciones y deterioro de instalaciones físicas del edificio. Esto implica un impacto en la disponibilidad de la información y un impacto organizacional financiero y operacional. La severidad inherente es moderada. Los controles con los que cuenta la organización para hacer frente a este riesgo son débiles, por lo que la severidad residual se mantiene.
- Avería de origen físico o lógico, cuyo origen es deliberado y accidental. Puede existir por: Falta de mantenimientos preventivos al equipo, inestabilidad en la red de energía eléctrica, susceptibilidad a variaciones de temperatura y falta de recursos en el equipo, derivando en un impacto

a la disponibilidad de la información y un impacto organizacional financiero y operacional. La severidad inherente es crítica. Además, los controles con los que cuenta la organización son débiles en cuanto a la mitigación del impacto y la probabilidad, por lo que, la severidad residual se mantiene en crítica.

- Errores del administrador, cuyo origen es deliberado y accidental. Se ha evidenciado que pueden darse por: falta de procedimientos formales para control de cambios, configuración incorrecta de parámetros y falta de concienciación en el personal que administra el equipo. Esta amenaza presenta un impacto en la confidencialidad, integridad y disponibilidad de la información; además, tiene un impacto organizacional en el aspecto financiero y operacional. Su severidad inherente es crítica y ha preocupado a la organización, por tal razón los controles con los que cuenta tienen una mitigación moderada tanto en el impacto como en la probabilidad, reduciendo a la severidad residual a moderada.
- Errores de mantenimiento / actualización de equipos, esta amenaza tiene un origen deliberado y puede materializarse por falta de mantenimientos preventivos al equipo, incorrecta aplicación de actualizaciones de software, así como por demora en la instalación de parches liberados por el fabricante, con lo cual causaría impacto en la disponibilidad mientras el impacto organizacional sería financiero y operacional. En el caso de presentarse este riesgo, tendría una severidad inherente moderada. La empresa no ha establecido controles fuertes, por lo cual la mitigación de impacto y probabilidad es débil ocasionando que su severidad residual se mantenga.
- Abuso de privilegios de acceso, tiene un origen deliberado y accidental y es una amenaza que se daría por una posible mala administración de los perfiles y permisos de usuario, por falta de un proceso formal y periódico de revisión de los derechos de acceso y por la falta de revisiones periódicas a los logs del equipo afectando la confidencialidad, disponibilidad y la integridad. Por ende, ocasionaría un impacto financiero y operacional en la empresa debido a su severidad inherente moderada.

Frente a esta amenaza se tienen controles débiles en cuanto a mitigación de impacto y probabilidad, por lo cual su severidad residual sigue siendo moderada.

- Robo, se trata de una amenaza de origen deliberado que se materializaría por un inadecuado control de los accesos físicos a las instalaciones, falta de protección física del edificio, puertas y ventanas o por la falta de mecanismos de monitoreo establecidos para violaciones de seguridad física afectando a la disponibilidad y confidencialidad y produciendo un impacto organizacional financiero y operacional. Tiene una severidad moderada inherente y la empresa cuenta con controles que mitigan la probabilidad y el impacto transformándolos en nivel moderado y débil, con lo cual su severidad residual mantiene el valor de moderada.

El activo “Firewall” mantiene un riesgo residual con severidad crítica que es la avería de origen físico o lógico, pues lamentablemente por más controles que la organización implemente se trata de una amenaza no controlable por la empresa. El resto de las amenazas de este activo tienen severidad residual moderada, es decir que la empresa con los controles implementados redujo la probabilidad de ocurrencia más no el impacto que causarían, por lo cual se plantearán nuevos planes de acción, en la siguiente etapa de este trabajo.

FASE 5.- Programa del SGSI

En esta fase se propone el programa de seguridad de la información para la empresa de cobranzas, en donde se establecen objetivos, alcance, políticas de alto nivel junto con responsables y los planes de acción obtenidos del diagnóstico y el análisis de riesgos ejecutados.

5.1 Objetivo del programa

Determinar las políticas, prácticas y/o lineamientos internos de seguridad de la información de la empresa de gestión de cobranzas para proteger todos y cada uno de los activos de información de la divulgación, la modificación mal intencionada, el uso no autorizado o la indisponibilidad, para de este modo garantizar su confidencialidad, integridad y disponibilidad.

5.2 Alcance del programa

El programa permitirá conocer, gestionar y minimizar los posibles riesgos a los que se encuentra expuesta la información de los activos críticos de la empresa de cobranzas que son objeto de este estudio, mediante la creación, mejora de los controles adoptados o definición de políticas que permitan mantener la seguridad en el ciclo de vida de la información de la organización y en todos los sistemas de la empresa.

5.3 Políticas del SGSI

En la presente sección se plantean las políticas que, conforme al estudio realizado, deben adoptarse en el SGSI de la empresa de cobranzas. En cada una de ellas se establece el responsable y el lineamiento a seguir para cumplir con la política. Entre las políticas planteadas tenemos las que se muestran en la Figura 35. El documento completo de las políticas se encuentra en el Anexo 13.

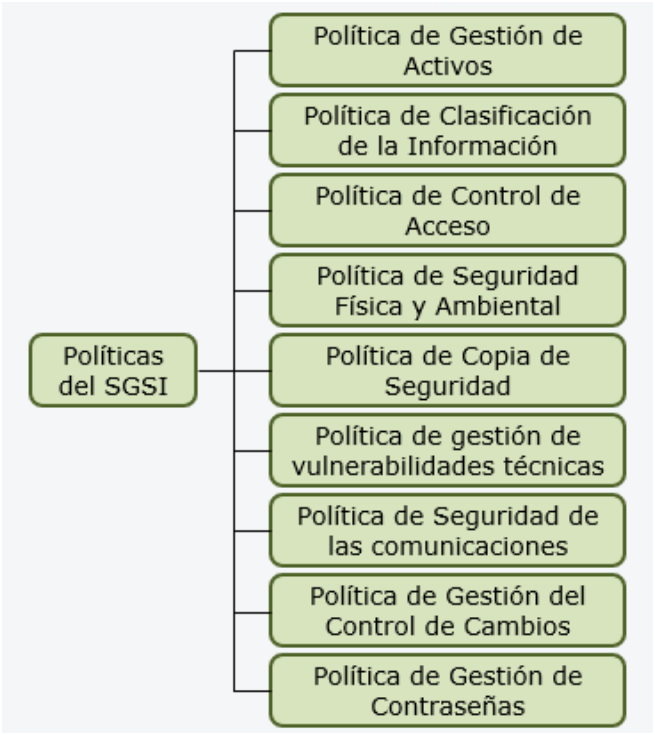


Figura 35 Listado de políticas planteadas. (Anexo 13)

5.4. Planes de acción

La lista de los planes de acción que se presenta a continuación constituye la propuesta de mejora para los controles que actualmente tiene la empresa, así como la implementación de nuevos controles, en el caso de que no existan, frente a las vulnerabilidades encontradas durante el análisis.

Para la elaboración de este listado se contempló un plan de acción para cada vulnerabilidad identificada en los activos críticos del estudio, junto con el tiempo de ejecución que puede tomar su implementación y el tipo de plan que se propone sea una mejora o implementación. Además, tal cual la Figura 36, se indica el alcance de cada plan de acción junto con el responsable de su ejecución. Para mayor detalle se puede consultar el Anexo 14.

Plan de acción											
Vulnerabilidad asociada	COD. CONTROL	Descripción del control	Fortaleza del control	Severidad RI	Severidad RR	Vulnerabilidad	Plan de acción	Capacidad de ejecución	Tipo	Alcance	Responsable
V.1.1.1 V.1.1.3 V.1.2.1 V.1.4.3	CON-001	Campañas de concientización sobre phishing.	DÉBIL	CRÍTICA	MODERADA	V.1.1.1	Adquirir un software para la automatización de campañas y entrenamientos sobre pishing.	Mediano Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área Financiera - Área de
						V.1.1.1	Diseñar un plan semestral de capacitación sobre phishing que contemple campañas de simulacros.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología.
						V.1.1.1	Evaluar periódicamente mediante los resultados de las campañas de phishing para reforzar concientización en los	Mediano Plazo	Mejora del Control	Autónomo	Responsable de la seguridad de la información
V.1.1.2 V.1.1.3 V.1.2.1 V.1.3.3 V.1.4.2 V.2.3.1	CON-002	Acuerdos de confidencialidad con el personal de la empresa	MODERADO	MODERADA	MODERADA	v.1.1.2	Diseñar procedimientos de manejo de la información conforme su nivel de clasificación.	Mediano Plazo	Mejora del Control	Autónomo	Responsable de la seguridad de la información
						v.1.3.3	Crear y cumplir políticas para el alta y baja de usuarios.	Mediano Plazo	Mejora del Control	Organizacional	- Área de Recursos Humanos - Área de
						v.1.4.2 v.1.5.2	Revisión anual de los derechos de acceso del personal de acuerdo a su cargo y función	Corto Plazo	Mejora del Control	Organizacional	- Área de Recursos Humanos - Área de Tecnología

Figura 36 Planes de Acción. (Anexo 14)

5.5 Conclusiones sobre el programa del SGSI

Las políticas planteadas en el programa del SGSI permiten satisfacer las necesidades de la empresa de cobranzas, considerando que:

- Los lineamientos establecidos en la política de gestión de activos facilitan el control de estos ya que se cuenta con un inventario actualizado.
- Clasificar la información de acuerdo con su importancia facilita la implementación de controles de protección, logrando cumplir con requisitos legales y evitando que la misma sea revelada o alterada sin consentimiento.
- Al controlar el acceso mediante la asignación y revocatoria de privilegios, mecanismos de autenticación y monitoreos constantes, se disminuye la probabilidad de alteraciones o modificaciones no autorizadas de la información por parte del personal de la empresa.
- Mediante delimitaciones físicas, bloqueos de acceso, distribución de áreas y capacitación frente a amenazas, la empresa disminuye el impacto y la probabilidad frente a robos, desastres naturales y divulgación de información.
- Al establecer lineamientos referentes a la copia de seguridad de la información, la organización cuenta con un soporte en caso de sufrir

pérdidas parciales o totales de información, ya fueren estas causadas de manera dolosa, intencional o ambiental.

- Cuando los procesos de gestión de vulnerabilidades se encuentran actualizados se garantiza un menor impacto en el caso de que una amenaza explote una vulnerabilidad técnica y resulta importante que el personal conozca sus responsabilidades y funciones a ejecutar.
- Al contar con procedimientos, responsabilidades y controles para la seguridad de las comunicaciones, la empresa disminuye el riesgo presente en la transmisión de información.
- Los lineamientos formales establecidos para el control de cambios disminuyen los errores en la administración ya sea de los equipos o en los sistemas de la empresa y al contar con documentación actualizada sobre los procedimientos de cambios se mantiene un registro detallado de cada uno de los cambios realizados.
- Utilizar contraseñas distintas y cambiarlas periódicamente reduce la probabilidad y el impacto de escenarios causados por accesos no autorizados en los sistemas empresariales.

Dentro de los planes de acción propuestos se ha contemplado:

- Reforzar las campañas de phishing, la forma de impartirlas y la evaluación de resultados, logrando mejorar el grado de concientización del personal en la institución.
- Mejoras en el proceso de obtención de respaldos y el uso de encriptación para proteger la confidencialidad e integridad de los datos de los clientes, las deudas y la gestión de cobranzas ejecutada.
- Lineamientos para estandarizar el proceso correspondiente a la gestión de control de cambios, gestión de contraseñas, gestión de accesos y gestión de vulnerabilidades
- Perfeccionamiento de políticas de aplicación de actualizaciones o ejecución de mantenimientos, no solo de software específico sino también de hardware y de los sistemas o infraestructura del centro de datos.

- Al no contar con un área de seguridad de la información dentro de la empresa, el área de tecnología y el responsable de seguridad de la información estarán inmersos de manera directa en la implementación de los planes de acción propuestos y trabajarán de la mano con el área de recursos humanos, área de mantenimiento y área financiera para ejecutarlos.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Al finalizar el presente proyecto se tienen las siguientes conclusiones:

- Utilizando como base la norma ISO/IEC 27001:2013 se logró desarrollar una herramienta que permitió diagnosticar el nivel de madurez de la empresa de cobranzas. Al considerar cada una de las cláusulas y evaluarlas de manera individual, se logró establecer las fortalezas y debilidades de la organización, en cuanto a seguridad de la información. En el caso de la empresa de estudio se determinó que no se cuenta con un sistema de gestión de seguridad de la información y actualmente la protección de información de la institución no se enfoca en mantener la confidencialidad, disponibilidad e integridad de la información. Así como la norma existen otros marcos de referencia que se pueden utilizar ya que este es el objetivo de su creación
- Durante el estudio se identifica que la información más importante para la empresa de gestión de cobranzas corresponde a la información de los clientes de carteras de servicios y carteras propias ya que se produciría un impacto catastrófico si en algún momento no llega a estar disponible, por ello se deduce que se trata de información delicada, de la cual se debe cuidar la integridad. Por ende, resulta sumamente importante protegerla de accesos no autorizados.
- Conocer qué tipo de información se encuentra asociada a cada activo y asignarle una codificación permitió determinar y seleccionar con mayor facilidad los dos activos críticos de la organización. En el caso de la empresa de cobranzas fueron la base de datos del CRM y el Firewall. La base de datos del CRM contiene distintos tipos de información, varios de ellos con criticidad menor o moderada; sin embargo, al existir uno o más de criticidad catastrófica, el activo que la contiene tendrá una criticidad catastrófica. En el caso del Firewall, su criticidad radica en que es el equipo encargado de controlar la seguridad en el tráfico de la red de datos

de la organización. Si este activo falla, la empresa se encuentra desprotegida ante cualquier tipo de amenaza externa.

- La empresa de gestión de cobranzas posee varias vulnerabilidades en sus activos de información. El análisis ejecutado resalta a la pérdida parcial o total de información como una de las principales amenazas ya que tiene un nivel muy alto de riesgo, con un impacto catastrófico y una probabilidad de ocurrencia cierta. Por lo tanto, es importante tomar acciones correctivas al respecto pues se trata de un dolor presente en la organización.
- La falta de un SGSI puede llevar a la empresa a innumerables pérdidas no solo económicas sino también reputacionales. Por tal motivo, el programa del sistema de gestión de seguridad de la información planteado para la empresa de cobranzas cubre las falencias o brechas encontradas durante el análisis de riesgos efectuado, para lograr establecer políticas, responsables, funciones y un plan de acción acorde a las necesidades y requerimientos de la organización.

RECOMENDACIONES

Entre las recomendaciones que podemos emitir se tienen:

- Se sugiere para cada proyecto de seguridad de la información se elabore un caso de negocio, mismo que evolucionará con el avance del trabajo para ajustarse a la realidad empresarial y que permitirá tener una visión clara de los antecedentes o bases que impulsan el programa, así como los beneficios, recursos y cronograma del proyecto.
- La herramienta utilizada para el diagnóstico inicial del nivel de madurez de la empresa de cobranzas se basa en la norma ISO/IEC 27001:2013. Se recomienda que en futuros estudios se consideren los cambios establecidos en las nuevas versiones de la norma ISO.
- En el análisis de riesgos realizado a la empresa de cobranzas se consideraron los dos activos de información con mayor criticidad. Se

recomienda realizar el análisis al resto de los activos con el fin de disminuir las brechas de seguridad derivadas de estos.

- Se recomienda la implementación de políticas o herramientas de control como la encriptación de datos, procesos de copias de seguridad aisladas, con el fin de proteger la información de la empresa de cobranzas de la pérdida parcial o total de información que fue una de las amenazas que obtuvo el mayor nivel de riesgo durante el análisis realizado.
- Las políticas, roles, responsabilidades y planes de acción propuestos en el programa del SGSI cubren las falencias actuales identificadas en la empresa de cobranzas. Se recomienda mejorarlo y actualizarlo constantemente, de tal forma que se adapte a los cambios que se presenten en la organización.

Referencias

Becerra, J. (4 de Junio de 2021). *CIO México*. Obtenido de https://cio.com.mx/que-es-cmmi-un-modelo-para-optimizar-los-procesos-de-desarrollo/

ESET. (2021). *welivesecurity*. Obtenido de https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Global Trust Association. (18 de 04 de 2022). *Believe Candidate Global-Trust-Association.* Obtenido de Believe Candidate Global-Trust-Association: https://believecandidate.global-trust-association.org/

Normaiso27001. (s.f.). Obtenido de https://normaiso27001.es/referencias-normativas-iso-27000/#terminos

Anexos

Anexo 1 Cronograma del proyecto

	Actividades	Días										Semanas																					
		Marzo				Abril						Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre	
		26	27	28	29	1	2	4	5	6	7	8	9	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
	FASE I Diagnóstico																																		
1.	Solicitud formal a la empresa para la elaboración del programa																																		
2.	Aprobación de la solicitud por parte de la gerencia																																		
3.	**Caso de Negocio del Programa**																																		
3.1	Presentación del caso de negocio a la gerencia de la empresa																																		
4.	**Metodología de Evaluación del estado actual de SGSI**																																		
4.1.	Elaboración de encuesta conforme a la norma ISO 27001																																		
4.2.	Ejecución de la encuesta al personal de la empresa																																		
4.3.	Análisis de los resultados de la encuesta																																		
5.	**Elaboración del Informe de estado actual de SGSI**																																		
	FASE II Clasificación de la información																																		
6.	**Clasificación de Tipos de Información**																																		
6.1	Identificación y Clasificación de los tipos de información manejados por la empresa																																		
6.2	Definición del Apetito del Riesgo, Niveles de Impacto y Probabilidad, Etiquetado																																		
6.3	Determinación de la criticidad de los tipos de información																																		
	FASE III Inventario de Activos de información																																		
7.	**Identificación de activos críticos**																																		
7.1	Elaboración del Inventario de activos de la empresa																																		
7.2	Determinación de los activos críticos de la empresa en base a los tipos de información																																		
	FASE IV Análisis de amenazas y vulnerabilidades de activos de información críticos																																		
8.	**Análisis de Riesgos**																																		
8.1	Identificación de Amenazas y Vulnerabilidades																																		
8.2	Determinación de Riesgo Inherente, Evaluación de Controles y Riesgo Residual																																		
	FASE V Programa del SGSI																																		
9.	**Desarrollo de políticas de alto nivel**																																		
9.1	Determinar objetivos y alcance del programa de seguridad																																		
9.2	Definición de las políticas del programa de SGSI																																		
10.	**Definición del Programa de SGSI**																																		
10.1	Roadmap (Hoja de Ruta) de planes de acción																																		
10.2	Informe final del programa																																		

Anexo 2 Herramienta de Evaluación

		NIVEL DE CUMPLIMIENTO						OBSERVACIONES	NIVEL ACTUAL	NIVEL DE MADUREZ ACTUAL DE LA EMPRESA	PLAN DE ACCION	DOCUMENTACION SEGÚN ISO 27001
	Pregunta	INCOMPLETO	EJECUTADO	ADMINISTRADO	DEFINIDO	GESTIONADO CUANTITATIVAMENTE	OPTIMIZADO					
4	CONTEXTO DE LA ORGANIZACIÓN								1,25	1,137		
4.1	Entender a la organización y su contexto								2			
	¿Se han identificado los factores externos e internos pertinentes para el propósito de la organización y como afectan a la capacidad de la organización para lograr los resultados del SGSI?			x				Se tienen identificados los factores externos e internos pero en un nivel específico y orientado a tecnologías de la información ya que se cuenta con un documento a nivel de infraestructura, donde se identificaron puntos de vulnerabilidad como resultado de un test de caja negra y blanca realizado por una empresa de seguridad informática externa, en el cual se identificaron los factores de riesgo.	2		Basado en un marco de referencia, documentar los factores externos e internos pertinentes y como afectan estos a la organización en su capacidad para lograr los resultados del SGSI.	
4.2	Entender las necesidades y expectativas de las partes interesadas								1			
	¿Se han determinado las partes interesadas y los requisitos relevantes para el SGSI?		x					Se ha realizado el ejercicio de conocer las partes interesadas. No se cuenta con un documento formal.	1		Elaborar la documentación, donde se listen las partes interesadas y sus requisitos relevantes referentes al SGSI.	
								No se encuentran listados los requisitos de las partes interesadas.				
4.3	Determinar el alcance del SGSI								1			
	¿Se encuentran definidos y documentados los límites y la aplicabilidad del sistema de gestión de seguridad de la información?		x					Se definen los límites y la aplicabilidad de los procesos de seguridad informática, mas no del sistema de seguridad de la información.	1		Basado en los requisitos de la norma, realizar un documento donde se determine el alcance, los límites y aplicabilidad del SGSI considerando: - Factores externos e internos - Requisitos de las partes interesadas - Dependencias de las actividades de la organización con respecto a otras del sector.	Alcance del SGSI
4.3.1	El sistema de gestión de seguridad cubre los factores internos y externos que lo pueden afectar?		x					Se han identificado los factores externos e internos del proceso de TI. Faltan los del SGSI.	1			
4.3.2	El sistema de gestión de seguridad cumple con los requisitos de las partes interesadas?		x						1			
4.4	Sistema de Gestión de Seguridad de la Información								1			
	¿Se ha establecido, implementado y se mejora continuamente el sistema de gestión de la seguridad de la información?		x					Se cuenta con indicadores para medir el cumplimiento de procesos de seguridad informática, mas no de un sistema de gestión de seguridad de la información.	1		Establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información, de acuerdo con los requisitos de la norma ISO 27001 y documentar el progreso del mismo.	
5	LIDERAZGO								0,992592593			
5.1	Liderazgo y Compromiso								1,777777778			
	¿La alta dirección demuestra liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información?			x				La alta dirección ha realizado casos de negocio e inversiones en infraestructura tecnológica para cubrir temas de seguridad informática.	2		Desarrollar un documento que contenga: - La política del SGSI adecuada al propósito de la organización y que sea compatible con la dirección estratégica de la organización. -Los objetivos de seguridad de la información compatibles con la dirección estrategica y alineados con los procesos de la empresa. - El compromiso de la alta direccion de asegurar los recursos necesarios y el apoyo a los roles de la dirección del SGSI El documento final deberá ser comunicado dentro de la organización, concientizando su importancia y estar disponible para las partes interesadas, de tal manera que se consigan los resultados previstos del SGSI y su mejora continua.	
5.1.1	¿Se encuentran los objetivos de la seguridad de la información alineados con los objetivos del negocio?		x					Los objetivos de la seguridad de la información no se encuentran alineados con los objetivos de negocio.	1			
5.1.2	¿El sistema de seguridad de la información está integrado con los procesos de la organización?		x					No se encuentran integrados los procesos con el SGSI.	1			
5.1.3	¿La alta dirección ha destinado los recursos necesarios para el sistema de gestión de seguridad de la información?			x					2			
5.1.4	¿Se ha difundido la importancia y los requisitos de la seguridad de la información en la organización?			x				Constantemente se realiza difusión sobre la importancia de la seguridad de la información a todos los usuarios de la organización. Se han implementado herramientas educativas pero no se mide la efectividad de esta tarea.	2			
5.1.5	¿Los altos directivos se han asegurado de que el sistema de seguridad de la información cumple con los resultados esperados?			x				La alta gerencia realiza seguimiento de todos los procesos, tareas y proyectos ejecutados a nivel organizacional.	2			
5.1.6	¿ La alta dirección apoya a su personal para que el sistema de gestión de seguridad de la información sea eficaz?			x				La gerencia dota de recursos financieros para la adquisición de equipos tecnológicos según la necesidad de los proyectos de seguridad.	2			
5.1.7	¿La alta dirección promueve la mejora continua del sistema de gestión de seguridad de la información?			x				En los proyectos de seguridad se solicita oportunamente mejoras en base a los resultados que se presentan a la gerencia y comité. La solicitud de mejoras no se basa en ningún estándar.	2			
5.1.8	¿La alta dirección ha dotado de autoridad a los encargados del sistema de gestión de seguridad de la información?			x				Se cuenta con herramientas para gestión de activos y gestión de incidentes. Se desconoce el alcance de la autoridad de seguridad de la información.	2			
5.2	Política								0,2			

	¿Se ha establecido una política de seguridad de la información en la organización y la misma se encuentra documentada y ha sido comunicada o difundida?		X					Existe una política de seguridad que no cumple con los requisitos de la norma.	1			Política de Seguridad de la información
5.2.1	¿La política se encuentra alineada al propósito de la organización?	X							0			
5.2.2	¿La política incluye los objetivos de seguridad de la información?	X							0			
5.2.3	¿La política incluye el compromiso de garantizar la confidencialidad, integridad y disponibilidad de la información?	X							0			
5.2.4	¿La política se compromete con la mejora continua del sistema de gestión de seguridad de la información?	X							0			
5.3	**Roles y Responsabilidades**								1			
5.3.1	¿La alta dirección ha asignado y comunicado a la organización las autoridades y sus tareas dentro del sistema de gestión de seguridad de la información?		X					Existe un documento que indica los responsables de seguridad y su función. En el documento no consta la descripción del cargo y tareas a ejecutar.	1		Desarrollar un documento que describa: - Los roles, responsabilidades y autoridades pertinentes del SGSI y comunicarlo dentro de la organización. En este documento se debe asegurar los requisitos de la norma ISO 27001 y que el responsable informe a la alta dirección sobre el comportamiento del SGSI.	
5.3.2	¿El encargado de la seguridad de la información notifica constantemente a la dirección sobre el sistema de gestión de seguridad de la información?		X					Se realiza notificación a la alta gerencia sobre las tareas de seguridad implementadas.	1			
6	**PLANIFICACIÓN**								**1**			
6.1	**Acciones para tratar los riesgos y oportunidades**								1			
	¿En la planificación del SGSI se han considerado los factores internos y externos, los requisitos de las partes interesadas y los riesgos y oportunidades?		X					Se ha realizado identificación de riesgos de TI pero está desactualizado. Falta identificación de riesgos en alto nivel.	1		Elaborar, diseñar, aplicar y documentar - Un análisis de riesgos del SGSI. - Una metodología de evaluación y tratamiento de riesgos basado en un marco de referencia. - Un proceso de tratamiento de riesgos que contenga objetivos e indicadores. - Justificar la aplicabilidad de los controles implementados.	Metodología de evaluación y tratamiento de riesgos
6.1.2	¿La organización ha definido y aplicado un proceso de apreciación y criterios de aceptación de riesgos de seguridad de la información?		X						1			
6.1.3	¿La organización tiene definido un proceso de tratamiento de los riesgos de seguridad de la información y ha elaborado una Declaración de aplicabilidad de los controles adoptados?		X					No se tiene la Declaración de aplicabilidad de los riesgos identificados.	1			Declaración de aplicabilidad
6.2	**Objetivos de seguridad de la información y planificación para su consecución**								1			
	¿Los objetivos de la seguridad de la información son coherentes, medibles, consideran los requisitos de seguridad de la información? ¿Han sido comunicados? ¿Están actualizados?		X					Se tienen objetivos definidos para los procesos de TI. Faltan objetivos de seguridad de la información.	1			Plan de tratamiento del riesgo.
6.2.1	¿ Se han identificado responsables, tiempos, recursos y métodos de evaluación de los resultados de los objetivos de la seguridad de la información planteados y se encuentran documentados?		X						1			
7	**SOPORTE**								**1,666666667**			
7.1	**Recursos**								2			
	¿La organización determina y proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI?			X				Se cuenta con asignación financiera para recursos de seguridad. Se ha adquirido infraestructura tecnológia para apoyar a la seguridad de la información.	2			
7.2	**Competencia**								1			
	¿La organización ha determinado las competencias necesarias de las personas que realizan un trabajo que afecta a la seguridad de la información?		x					No se ha documentado las competencias y perfiles del personal en seguridad de la información.	1		Documentar y actualizar constantemente una matriz de competencias para asegurar que el personal cuenta con los conocimientos relacionados a la seguridad de la información. Capacitar al personal constantemente para asegurar que cuentan con las habilidades y competencias necesarias.	Registros de capacitación, habilidades, experiencia y calificaciones
7.3	**Concienciación**								1			
	¿El personal de la organización ha sido concientizado sobre la política de seguridad, su aporte y las implicaciones de no cumplir con el SGSI?		X					Se realizan campañas sobre la importancia de la seguridad informática. No se tiene una política general de alta dirección sobre la seguridad de la información.	1		Difundir internamente la política de seguridad de la información para concientizar al personal sobre las consecuencias positivas y negativas de la misma.	
7.4	**Comunicación**								2			
	¿ Se han determinado las necesidades de comunicación internas y externas del SGSI?			X				Se cuenta con un documento de contingencia o continuidad de negocio, donde consta un mínimo viable sobre las acciones de comunicación que se deben cumplir.	2		Determinar las necesidades de comunicacion internas y externas del SGSI, que incluyan: - El contenido de la comunicación - Cuándo comunicar; - A quién comunicar; - Quién debe comunicar; - Los procesos por los que debe efectuarse la comunicación.	
7.5	**Información Documentada**								2,333333333			
	¿ La organización cuenta con documentación necesaria para cumplir eficientemente con el sistema de gestión de seguridad de la información? (Documentos de la norma y la requerida por la empresa:política, procesos)			X				Sobre los temas de seguridad tratados o implementados en la empresa, el area de calidad y procesos posee la documentación respectiva	2		Elaborar toda la documentación obligatoria conforme la norma ISO 27001 y la documentación que dentro de la organización se considere escencial.	
7.5.2	¿La documentación del sistema de gestión de seguridad de la información cuenta con una identificación, formato y ha sido revisada y aprobada?				X			Se cuenta con un sistema de registro revisión y aprobación con un formato establecido.	3		- Mantener y actualizar de manera oportuna el sistema de registro de la revisión y aprobación de los documentos de la empresa	

7.5.3	¿La distribución, acceso, almacenamiento y cambios de la documentación del sistema de gestión de seguridad de la información se encuentra controlada?			X				Cada documento tiene una sección donde se lleva un control de cambios y se han definido accesos a la información. No se lleva un control de la distribución y almacenamiento de la documentación.	2		de los documentos de la empresa. - Mantener y actualizar de manera oportuna el control de cambios, distribución, acceso y almacenamiento a la documentación de la empresa.	
8	**OPERACIÓN**								**0,75**			
8.1	**Planificación y control operacional**								1			
	¿La organización planifica, implementa y controla los procesos necesarios para cumplir con los requisitos del SGSI?		X					Se cuenta con procesos definidos de forma empírica, se encuentran documentados. Los procesos no se basan en un estándar.	1		Desarrollar un documento que contenga: - Inventario de activos - Uso aceptable de activos	Inventario de Activos Uso aceptable de activos
8.2	**Apreciación de los riesgos de seguridad de la información**								1			
	¿La organización realiza la apreciación periódica de los riesgos de la seguridad de la información y se encuentra documentada?		X					La apreciación de los riesgos se encuentra desactualizada. No existe explicación o respaldo de los criterios de apreciación del riesgo utilizados.	1		Ejecutar y documentar en un informe la evaluación de riesgos basándose en una metodología estandarizada.	Informe sobre evaluación de riesgos
8.3	**Tratamiento de riesgos de la Seguridad de la Información**								1			
	¿La organización cuenta con el plan de tratamiento de los riesgos de seguridad de la información y sus resultados son documentados?		X					Se cuenta con una iniciativa de tratamiento de riesgos. No existe un plan documentado para el tratamiento de los mismos.	1		Desarrollar un documento que contenga: - El plan de tratamiento de riesgos - Los resultados del tratamiento de los riesgos.	Informe sobre el tratamiento de riesgos
9	**EVALUACIÓN DEL DESEMPEÑO**								**0,8**			
9.1	**Seguimiento, medición, análisis y evaluación**								0,4			
	¿La organización evalúa el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información y se encuentra documentada?		X					Existe documentación formal sobre ciertos indicadores de seguridad establecidos en la organización. Los indicadores planteados no se basan en un estándar	1		Implementar indicadores para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI basados en un estandar donde se determine: - Los procesos y controles de seguridad de la información a medir. - Métodos de seguimiento, medición, análisis y evaluación del SGSI - Periodo y responsables del Seguimiento y medición del SGSI - Periodo y responsables del Análisis y evaluación de los resultados del SGSI	
9.1.1	¿La organización ha identificado los procesos y controles de seguridad de la información que se deben medir?		X						1			
9.1.2	¿La organización ha implementado métodos de seguimiento, medición, análisis y evaluación del SGSI?	X						No se tiene métodos de seguimiento, medición, análisis y evaluación.	0			
9.1.3	¿Se han identificado período y responsables para llevar a cabo el seguimiento y medición del sistema de gestión de seguridad de la información?	X						No se tiene periodos y responsables de medición del SGSI	0			
9.1.4	¿Se han identificado período y responsables para llevar a cabo el análisis y evaluación de los resultados del seguimiento y medición del sistema de gestión de seguridad de la información?	X							0			
9.2	**Auditoría interna**								1			
	¿La organización lleva a cabo auditorías internas a intervalos planificados del sistema de gestión de la seguridad de la información?		X					Se realizan auditorías de los procesos internos que involucran seguridad. No se tienen auditorías de un SGSI.	1		Planificar auditorías internas al SGSI planteado y documentar su ejecución donde se cumpla con: - Los requisitos de la organización y de la norma ISO - Criterios y su alcance - Objetividad e imparcialidad del proceso de auditoría.	
9.2.1	¿En los resultados de la auditoría interna se pueden observar los requisitos de la organización para su sistema de gestión de seguridad de la información?		X						1			
9.2.2	¿El sistema de gestión de seguridad de la información se encuentra implementada y mantenida de manera eficaz?		X						1			
9.2.3	¿ Se cuentan con programas periódicos de auditoría con criterios y alcance definidos?		X						1			
9.2.4	¿Se dispone con información documentada de los procesos de auditoría ejecutados y los mismos son informados a la dirección?		X						1			
9.3	**Revisión de la dirección**								1			
9.3	¿La alta dirección revisa continuamente el sistema de gestión de seguridad de la información para asegurarse de su conveniencia, adecuación y eficacia continuas. ?		X					Se realizan revisiones de los procesos internos y proyectos de seguridad, mas no de un SGSI	1		Desarrollar documentación de las revisiones del SGSI por parte de la alta dirección que contenga: - Estado de las acciones de revisiones anteriores - Los cambios en las cuestiones externas e internas del SGSI. - Información sobre el comportamiento de la seguridad de la información. - Comentarios de las partes interesadas. - Resultados de la apreciación de los riesgos y el estado del plan de tratamiento de riesgos. - Oportunidades de mejora continua.	
10	**Mejora**								**1,5**			
10.1	**No conformidad y acciones correctivas**								1			
10.1	¿Frente a las no conformidades la organización toma acciones correctivas y las documenta?		X					Se realizan acciones correctivas producto de las auditorías ejecutadas. No todo está documentado	1		Elaborar un documento de las no conformidades que contenga: - La naturaleza de las no conformidades - Acciones ante la no conformidad. - Los resultados de las acciones correctivas aplicadas	
10.2	**Mejora Continua**								2			
10.2	¿La organización mejora de manera continua la idoneidad, adecuación y eficacia del SGSI?			X				Si se ejecutan mejoras en cuanto a seguridad informática pero no están basadas en un estándar.	2		Definir un período para la ejecución de mejoras del SGSI.	

Anexo 3 Tipos de información de la empresa de cobranzas y su criticidad.

Dominios o Entidades	Descripción del Dominio o Entidad	Tipo de información	Descripción	Disponibilidad Asegurar el acceso y uso de la información y los sistemas en el momento oportuno	Integridad Preservación de la información	Confidencialidad La protección de la información de accesos no autorizados	Calificación Disponibilidad	Calificación Integridad	Calificación Confidencialidad	Criticidad (Numérica)	Etiqueta Confidencialidad	Clasificación del Tipo de Información	Dueño de la Entidad: Responsable	Actualización del tipo de información: A que fecha esta actualizado
Clientes Carteras Propias	Clientes (Naturales, Jurídicos) de las carteras de propiedad de la empresa de cobranzas	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, ciudad	CATASTRÓFICO	MAYOR	MAYOR	5	4	4	4,33	RESTRINGIDA	CATASTRÓFICO	Coordinador de Estrategias de Carteras Propias (CECP) / Gerente de Operaciones (GO) /Gerente de TI	8/5/2022
		Información de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Número de teléfono móvil, Número de telefono convencional, Dirección de domicilio, Dirección de trabajo.	CATASTRÓFICO	MAYOR	CATASTRÓFICO	5	4	5	4,67	CONFIDENCIAL	CATASTRÓFICO		8/5/2022
		Datos de la deuda del cliente	Saldo de la deuda	CATASTRÓFICO	CATASTRÓFICO	MAYOR	5	5	4	4,67	RESTRINGIDA	CATASTRÓFICO		8/5/2022
		Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	puede pactar para cubrir su deuda. Ejemplo: Promesas de Pago: Fecha de la Promesa de pago, Valor de la promesa de Pago Acuerdo de Pago: Fecha del acuerdo, descuento, Entrada, Número de	CATASTRÓFICO	MAYOR	MAYOR	5	4	4	4,33	RESTRINGIDA	CATASTRÓFICO		8/5/2022
Clientes Carteras de Servicios	Clientes de los clientes que han contratado los servicios de gestión de cobranzas de la empresa	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, estado civil, ciudad	CATASTRÓFICO	CATASTRÓFICO	MAYOR	5	5	4	4,67	RESTRINGIDA	CATASTRÓFICO	Coordinador de Estrategias de Carteras de Servicios (CECS) / Gerente de Operaciones (GO) / Gerente de TI	8/5/2022
		Datos de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Numeros de teléfono móvil, Numeros de telefono convencional, Dirección de domicilio, Dirección de trabajo.	CATASTRÓFICO	MAYOR	CATASTRÓFICO	5	4	5	4,67	CONFIDENCIAL	CATASTRÓFICO		8/5/2022
		Datos de la deuda del cliente	Saldos de la deuda (Saldos Total, Saldo Ajustado)	CATASTRÓFICO	CATASTRÓFICO	MAYOR	5	5	4	4,67	RESTRINGIDA	CATASTRÓFICO		8/5/2022
		Datos de la negociación del cliente de servicios(Promesas, Acuerdos)	Promesas o Acuerdos donde se detalla el método de pago del cliente.	CATASTRÓFICO	MAYOR	MAYOR	5	4	4	4,33	RESTRINGIDA	CATASTRÓFICO		8/5/2022
Organización	Empresa de gestión de cobranzas que maneja carteras propias y carteras de servicios	Datos de las proyecciones de estrategia de carteras de servicios	Cedente(nombre cliente),sector, tipos_de_cartera, estrategia_mensual, honorarios	MAYOR	MAYOR	MAYOR	4	4	4	4,00	RESTRINGIDA	MAYOR	Gerente de Negocios y Analítica	8/5/2022
		Datos de las proyecciones de estrategia de carteras propias	Segmento, tipo_de_cartera, estrategia_mensual, producto1, producto2	MAYOR	MAYOR	MAYOR	4	4	4	4,00	RESTRINGIDA	MAYOR		8/5/2022
		Datos de las compras de carteras propias y asignaciones de carteras de	número_cuenta, monto_pagar, cédula, números_contacto, direcciones, datos_deuda	MAYOR	CATASTRÓFICO	CATASTRÓFICO	4	5	5	4,67	CONFIDENCIAL	CATASTRÓFICO	Gerente de TI	8/5/2022
		Datos de actas y decisiones de juntas directivas o comités mantenidos	numero_acta,asistentes,descripción, tareas y responsables, resultados	MODERADO	MENOR	MENOR	3	2	2	2,33	USO INTERNO	MODERADO	Gerente General	8/5/2022
Proveedores	Personas naturales o jurídicas que brindan o brindaron servicio a la organización	Datos del proveedor	Razón social, RUC, telefonos, dirección, Numero_cuenta, SLA's,contratos	MENOR	MENOR	MENOR	2	2	2	2,00	USO INTERNO	MODERADO	Gerente Financiero	8/5/2022
		Código Fuente CRM	Archivos y librerías de la aplicación web del CRM, aplicación de cobranza domiciliaria	CATASTRÓFICO	MENOR	MENOR	5	2	2	3,00	USO INTERNO	MAYOR	Gerente de Tecnología de la Información	8/5/2022
Ex Clientes Carteras Propias (Naturales, Jurídicos)	Personas que en algún momento tuvieron una deuda con la empresa que se encuentra solventada	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, estado civil	INSIGNIFICANTE	MENOR	MENOR	1	2	2	1,67	USO INTERNO	MENOR	Coordinador de Estrategias de Carteras Propias (CECP)	8/5/2022
		Información de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Número de teléfono móvil, Número de telefono convencional, Dirección de domicilio, Dirección de trabajo.	INSIGNIFICANTE	MENOR	MENOR	1	2	2	1,67	USO INTERNO	MENOR		8/5/2022
		Datos de la deuda del cliente	Saldo de la deuda	INSIGNIFICANTE	MENOR	MENOR	1	2	2	1,67	USO INTERNO	MENOR		8/5/2022
		Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	Acuerdos donde se detalla el método de pago del cliente hacia la empresa.	INSIGNIFICANTE	MENOR	MENOR	1	2	2	1,67	USO INTERNO	MENOR		8/5/2022
Ex Clientes (Cartera de Servicios)	Personas que en algún momento tuvieron una deuda con el cliente que ha contaratado los servicios de gestión de cobranzas de la empresa	Datos Personales del cliente	Nombres y apellidos, Número de cédula o RUC, estado civil	MENOR	MODERADO	MODERADO	2	3	3	2,67	PRIVADA	MODERADO	Coordinador de Estrategias de Carteras Propias (CECP)	8/5/2022
		Información de Contacto del cliente	Correo electrónico personal, correo electrónico laboral, Número de teléfono móvil, Número de telefono convencional, Dirección de domicilio, Dirección de trabajo.	MENOR	MODERADO	MODERADO	2	3	3	2,67	PRIVADA	MODERADO		8/5/2022
		Datos de la deuda del cliente	Saldo de la deuda	MENOR	MODERADO	MODERADO	2	3	3	2,67	PRIVADA	MODERADO		8/5/2022
		Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	Acuerdos donde se detalla el método de pago del cliente hacia la empresa.	MENOR	MODERADO	MODERADO	2	3	3	2,67	PRIVADA	MODERADO		8/5/2022
Empleados (Administradores, Operativos)	Personas que trabajan en la empresa actualmente	Datos Personales del colaborador	Cédula, estado civil, cargas familiares, profesión, cargo, remuneración	MENOR	MENOR	MENOR	2	2	2	2,00	USO INTERNO	MODERADO	Analista de Nómina / Gerente de Talento Humano	8/5/2022
Exempleados (Administradores, Operativos)	Personas que alguna vez trabajaron en la organización	Datos personales del ex-colaborador	Cédula, estado civil, cargas familiares, profesión, cargo, remuneración	INSIGNIFICANTE	MENOR	MENOR	1	2	2	1,67	USO INTERNO	MENOR	Gerente de Talento Humano	8/5/2022

Anexo 4 Apetito del riesgo de la empresa de cobranzas

Impacto	Aversión	Neutral	Agresivo
Interrupción de operaciones		Dependiendo del tiempo de interrupción	
Modificaciones de la información		Depende si la modificación fue o no autorizada y del tipo de información que se modifique.	
Divulgación de información		Depende del tipo de información divulgada.	

Anexo 5 Tipología de Impacto de la empresa de cobranzas

Niveles	Interrupción de operaciones	Modificaciones de la información	Divulgación de información
CATASTRÓFICO	Implica malestar en los clientes internos y externos por paralización total de las operaciones empresariales	Se realizan modificaciones no autorizadas de la información confidencial de los clientes internos y externos de la empresa.	Cuando se ha divulgado información confidencial de los clientes internos y externos de la empresa.
MAYOR	Implica malestar en los clientes internos y externos por paralización parcial de las operaciones de la gestión de cobranza	Cuando se realizan modificaciones no autorizadas de la información restringuida de los clientes internos y externos de la empresa.	Cuando se ha divulgado información restringuida de los clientes internos y externos de la empresa
MODERADO	Implica malestar al interior de la organización por problemas de paralización de operaciones	Cuando se realizan modificaciones no autorizadas de la información privada de los clientes internos y externos de la empresa.	Cuando se ha divulgado información privada de los clientes internos y externos de la empresa.
MENOR	Implica malestar en un área específica dentro de la empresa por paralización de sus actividades	Cuando se realizan modificaciones no autorizadas de la información de uso interno de la empresa.	Cuando se ha divulgado información de uso interno de la empresa.
INSIGNIFICANTE	Implica malestar de una persona al interior de la empresa por paralización de sus actividades.	Cuando se realizan modificaciones no autorizadas de la información de uso público de la empresa	Cuando se ha divulgado información de uso público de la empresa

Anexo 6 Nivel de Probabilidad, Impacto y etiquetado de la información

Nivel de Probabilidad	Descripción
CIERTO	Cuando se tiene certeza del 80% de la ocurrencia de la amenaza
PROBABLE	Cuando se tiene certeza entre el 50 y 79% de la ocurrencia de la amenaza
POSIBLE	Cuando la certeza de la materialización de la amenaza está entre el 30% y 49%
IMPROBABLE	Cuando la certeza de la ocurrencia de la amenaza está entre el 6% y 29%
EXCEPCIONAL	Cuando la certeza de la materialización de la amenaza es menor al 5%

Niveles	ETIQUETADO
CATASTRÓFICO	CONFIDENCIAL
MAYOR	RESTRINGIDA
MODERADO	PRIVADA
MENOR	USO INTERNO
INSIGNIFICANTE	PÚBLICO

Niveles de Impacto	Descripción
CATASTRÓFICO	internos y externos por paralización total de las operaciones empresariales
MAYOR	interno y externos por paralización parcial de las operaciones de la gestión de cobranza
MODERADO	Implica malestar al interior de la organización por problemas por paralización de operaciones
MENOR	Implica malestar en un área específica dentro de la empresa por paralización de sus actividades
INSIGNIFICANTE	Implica malestar de una persona al interior de la empresa por paralización de sus actividades

Anexo 7 Activos de Información con su criticidad, dependencia y custodio

Código del activo	Nombre del Activo de información	Codificación del Tipo de información	Tipo de Información	Clasificación del tipo de información	Criticidad del activo	Dependencia	Custodio
1	Base de datos del CRM	BBDE-ACCP-001	Datos Personales del cliente	CATASTRÓFICO	CATASTRÓFICO	9	Coordinador de Estrategias de Carteras Propias (CECP) / Gerente de Operaciones (GO) /Gerente de TI
		BBDE-ACCP-002	Información de Contacto del cliente	CATASTRÓFICO			
		BBDE-ACCP-003	Datos de la deuda del cliente	CATASTRÓFICO			
		BBDE-ACCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	CATASTRÓFICO			
		BBDE-ACCS-001	Nombres y apellidos, Número de cédula o RUC, estado civil, ciudad	CATASTRÓFICO			Coordinador de Estrategias de Carteras de Servicios (CECS) / Gerente de Operaciones (GO) / Gerente de TI
		BBDE-ACCS-002	Correo electrónico personal, correo electrónico laboral, Numeros de teléfono móvil, Numeros de telefono convencional, Dirección de domicilio, Dirección de trabajo.	CATASTRÓFICO			
		BBDE-ACCS-003	Saldos de la deuda (Saldos Total, Saldo Ajustado)	CATASTRÓFICO			
		BBDE-ACCS-004	Promesas o Acuerdos donde se detalla el método de pago del cliente.	CATASTRÓFICO			
		BBDE-XCCP-001	Datos Personales del cliente	MENOR			Coordinador de Estrategias de Carteras Propias (CECP)
		BBDE-XCCP-002	Información de Contacto del cliente	MENOR			
		BBDE-XCCP-003	Datos de la deuda del cliente	MENOR			
		BBDE-XCCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	MENOR			
		BBDE-XCCS-001	Datos Personales del cliente	MODERADO			Coordinador de Estrategias de Carteras Propias (CECP)
		BBDE-XCCS-002	Información de Contacto del cliente	MODERADO			
		BBDE-XCCS-003	Datos de la deuda del cliente	MODERADO			
		BBDE-XCCS-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	MODERADO			

2	Base de datos Analítica	BBDA-CS-001	Datos de las proyecciones de estrategia de carteras de servicios	MAYOR	MAYOR	10	Gerente de Negocios y Analítica
		BBDA-CS-002	Datos de las proyecciones de estrategia de carteras propias	MAYOR			
3	Base de Datos - Cargas Automáticas	BBDCA-001	Datos de las compras de carteras propias y asignaciones de carteras de servicios	CATASTRÓFICO	CATASTRÓFICO	11	Gerente de TI
4	DOCSERVER	DS-001	Datos de actas y decisiones de juntas directivas o comités mantenidos	MODERADO	MODERADO		Gerente General
		DS-002	Datos del accionista	MODERADO			Gerente Financiero / Gerente General
		DS-003	Datos de la entidad reguladora	MODERADO			Gerente General
5	BPM	BPM - 001	Datos del proveedor	MODERADO	MODERADO	12	Gerente Financiero
		BPM - 002	Datos Personales del colaborador	MODERADO			Analista de Nómina / Gerente de Talento Humano
		BPM - 003	Datos personales del ex-colaborador	MENOR			Gerente de Talento Humano
6	CRM	APP-001	Archivos y librerías de la aplicación web del CRM, aplicación de cobranza domiciliaria	MAYOR	MAYOR	13	Gerente de Tecnología de la Información
7	APP - Domiciliarios	APP-001	Archivos y librerías de la aplicación web del CRM, aplicación de cobranza domiciliaria	MAYOR	MAYOR	14	Gerente de Tecnología de la Información
8	FIREWALL	FW-001	Equipo de las reglas de seguridad de la red empresarial	CATASTRÓFICO	CATASTRÓFICO		Jefe de Infraestructura

		BBDE-ACCP-001	Datos Personales del cliente	CATASTRÓFICO			
		BBDE-ACCP-002	Información de Contacto del cliente	CATASTRÓFICO			
		BBDE-ACCP-003	Datos de la deuda del cliente	CATASTRÓFICO			
		BBDE-ACCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	CATASTRÓFICO			
		BBDE-ACCS-001	Nombres y apellidos, Número de cédula o RUC, estado civil, ciudad	CATASTRÓFICO			
9	Servidor de la base de datos del CRM	BBDE-ACCS-002	Correo electrónico personal, correo electrónico laboral, Numeros de teléfono móvil, Numeros de telefono convencional, Dirección de domicilio, Dirección de trabajo.	CATASTRÓFICO	CATASTRÓFICO		Jefe de Infraestructura
		BBDE-ACCS-003	Saldos de la deuda (Saldos Total, Saldo Ajustado)	CATASTRÓFICO			
		BBDE-ACCS-004	Promesas o Acuerdos donde se detalla el método de pago del cliente.	CATASTRÓFICO			
		BBDE-XCCP-001	Datos Personales del cliente	MENOR			
		BBDE-XCCP-002	Información de Contacto del cliente	MENOR			
		BBDE-XCCP-003	Datos de la deuda del cliente	MENOR			
		BBDE-XCCP-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	MENOR			
		BBDE-XCCS-001	Datos Personales del cliente	MODERADO			
		BBDE-XCCS-002	Información de Contacto del cliente	MODERADO			
		BBDE-XCCS-003	Datos de la deuda del cliente	MODERADO			
		BBDE-XCCS-004	Datos de la negociación del cliente(Promesas, Acuerdos, Facilidades de Pago)	MODERADO			
10	Servidor de Base de datos de Analítica	BBDA-CS-001	Datos de las proyecciones de estrategia de carteras de servicios	MAYOR	MAYOR		Jefe de Infraestructura
		BBDA-CS-002	Datos de las proyecciones de estrategia de carteras propias	MAYOR			
11	Servidor de base de Datos de Cargas Automáticas	BBDCA-001	Datos de las compras de carteras propias y asignaciones de carteras de servicios	CATASTRÓFICO	CATASTRÓFICO		Jefe de Infraestructura

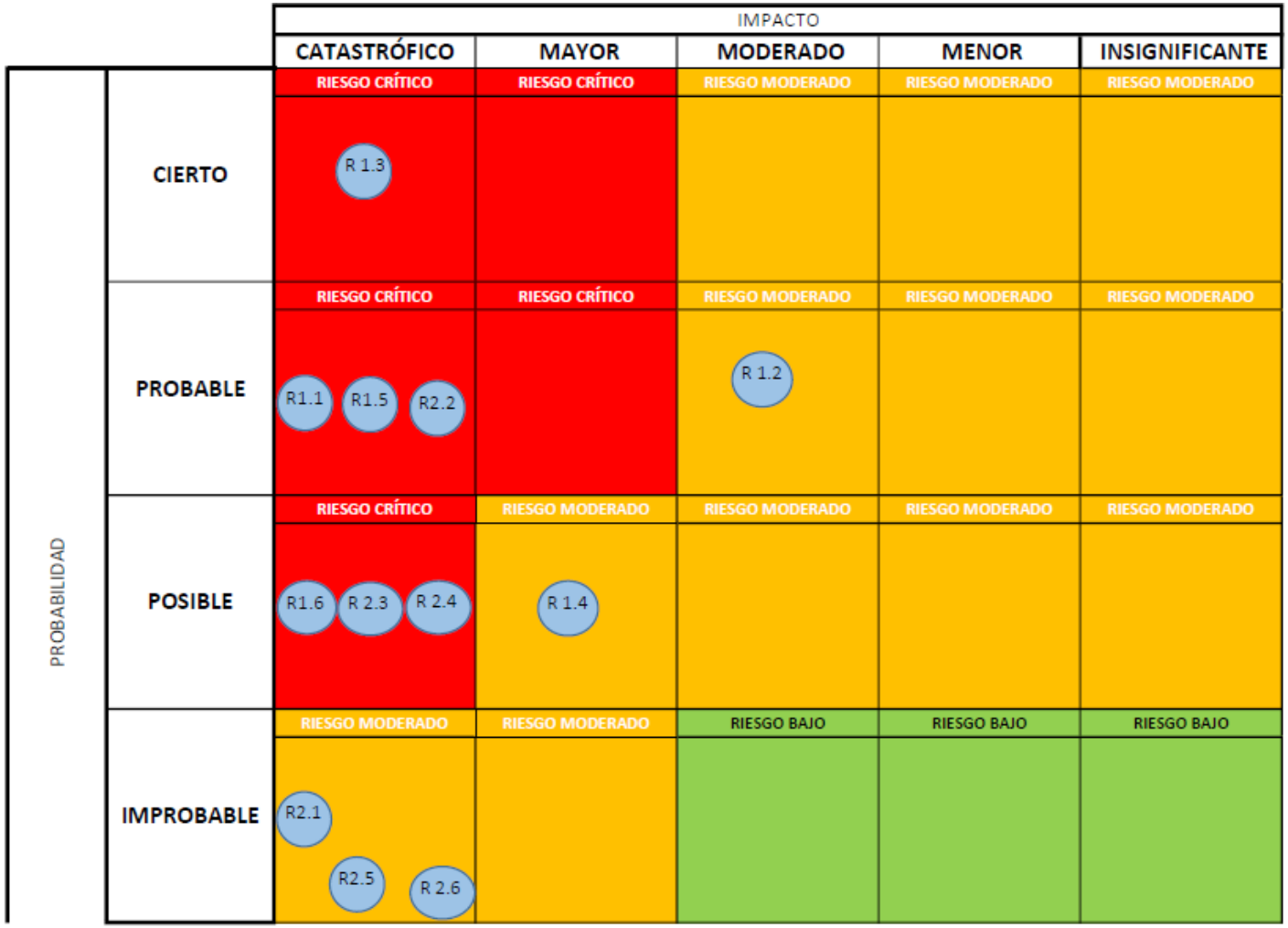
12	Servidor BPM	BPM - 001	Datos del proveedor	MODERADO	MODERADO		Jefe de Infraestructura
		BPM - 002	Datos Personales del colaborador	MODERADO			
		BPM - 003	Datos personales del ex-colaborador	MENOR			
13	Servidor web del CRM	APP-001	Archivos y librerías de la aplicación web del CRM, aplicación de cobranza domiciliaria	MAYOR	MAYOR		Jefe de Infraestructura
14	Servidor web de App - Domiciliarios	APP-002	Archivos y librerías de la aplicación web del CRM, aplicación de cobranza domiciliaria	MAYOR	MAYOR		Jefe de Infraestructura

Anexo 8 Matriz de riesgos de la empresa de cobranzas

									Identificación del riesgo	INHERENCIA			GRUPO DE CONTROLES		RESIDUAL		
Código del activo	Nombre del Activo de información	Tipo de Activo	Amenazas	Origen	Cod. Vulnerabilidad	Vulnerabilidades	Impacto en	Impacto Organizacional	ID Riesgo	IMPACTO RI	PROBABILIDAD RI	SEVERIDAD RI	Mitigación de Probabilidad	Mitigación de Impacto	IMPACTO RR	PROBABILIDAD RR	SEVERIDAD RR
1	Base de datos del CRM	[D] Datos / Información	Destrucción de información	D	V1.1.1	- Falta de concienciación en el personal que administra los datos (sobre integridad, disponibilidad, confidencialidad de la información)	Disponibilidad	Financiero, Operacional	R1.1	CATASTRÓFICO	PROBABLE	CRÍTICA	FUERTE	MODERADO	MAYOR	IMPROBABLE	MODERADA
					V1.1.2	- Falta de procedimientos para el manejo de información clasificada											
					V1.1.3	- Información sin encriptación											
			Divulgación de información	D,A	V1.1.1	- Falta de concienciación en el personal que administra los datos (sobre seguridad y privacidad de la información)	Confidencialidad	Financiero, Legal, Reputación	R1.2	MODERADO	PROBABLE	MODERADA	MODERADO	DÉBIL	MODERADO	POSIBLE	MODERADA
					V1.1.2	- Falta de procedimientos para el manejo de información clasificada											
					V1.2.1	- Falta de mecanismos de monitoreo establecidos para violaciones de seguridad lógica											
			Pérdida parcial o total de información	D, A, E	V1.3.1	- Administración inadecuada de los respaldos de información (backups)	Disponibilidad	Financiero, Operacional	R1.3	CATASTRÓFICO	CIERTO	CRÍTICA	MODERADO	MODERADO	MAYOR	PROBABLE	CRÍTICA
					V1.3.2	- Falta de mecanismos de identificación y autenticación de usuarios											
					V1.3.3	- Falta de un procedimiento formal para el alta y baja de usuarios											
			Alteración y/o modificación no autorizada de la información por parte del personal de la empresa	D,A	V1.4.1	- Falta de procedimientos formales para control de cambios	Integridad	Operacional, Legal, Reputación	R1.4	MAYOR	POSIBLE	MODERADA	FUERTE	MODERADO	MODERADO	EXCEPCIONAL	BAJA
					V1.4.2	- Falta de responsabilidades de seguridad de la información en las descripciones de puestos de trabajo											
					V1.4.3	- Mala gestión de contraseñas											
			Abuso de privilegios de acceso	D, A	V.1.5.1	- Mala Administración de los perfiles y permisos de usuario	Confidencialidad, Integridad, Disponibilidad	Reputación, Legal	R1.5	CATASTRÓFICO	PROBABLE	CRÍTICA	DÉBIL	DÉBIL	CATASTRÓFICO	PROBABLE	CRÍTICA
					V.1.5.2	- Falta de un proceso formal y periódico de revisión de los derechos de acceso											
					V.1.5.3	- Falta de revisiones periódicas a los logs de la base de datos											
			Errores del administrador	D, A	V1.6.1	- Falta de la aplicación de actualizaciones en el motor de base datos	Confidencialidad, Integridad, Disponibilidad	Operacional, Financiero	R1.6	CATASTRÓFICO	POSIBLE	CRÍTICA	MODERADO	MODERADO	MAYOR	IMPROBABLE	MODERADA
					V1.6.2	-Instalación incorrecta del software de base de datos											
					V1.6.3	- Configuración incorrecta de parámetros											
2	Firewall	[HW] Equipamiento informático (hardware)	Desastres naturales (Fuego, daños por agua)	E	V2.1.1	- Mal funcionamiento del sistema contraincendios	Disponibilidad	Financiero, Operacional	R2.1	CATASTRÓFICO	IMPROBABLE	MODERADA	DÉBIL	DÉBIL	CATASTRÓFICO	IMPROBABLE	MODERADA
					V2.1.2	- Ubicación del data center en una zona susceptible a inundaciones											
					V2.1.3	- Deterioro de instalaciones físicas del edificio											
			Avería de origen físico o lógico	D,A	V2.2.1	- Falta de mantenimientos preventivos al equipo	Disponibilidad	Financiero, Operacional	R2.2	CATASTRÓFICO	PROBABLE	CRÍTICA	DÉBIL	DÉBIL	CATASTRÓFICO	PROBABLE	CRÍTICA
					V.2.2.2	- Inestabilidad en la red de energía eléctrica.											
					V2.2.3	- Susceptible a variación de temperatura											
					V2.2.4	- Falta de recursos en el equipo.											
			Errores del administrador	D,A	V1.4.1	- Falta de procedimientos formales para control de cambios	Confidencialidad, Integridad, Disponibilidad	Financiero, Operacional	R2.3	CATASTRÓFICO	POSIBLE	CRÍTICA	MODERADO	MODERADO	MAYOR	IMPROBABLE	MODERADA
					V1.6.3	- Configuración incorrecta de parámetros											
					V2.3.1	- Falta de concienciación en el personal que administra el equipo											
			Errores de mantenimiento / actualización de equipos	D	V2.2.1	- Falta de mantenimientos preventivos al equipo	Disponibilidad	Financiero, Operacional	R2.4	CATASTRÓFICO	POSIBLE	CRÍTICA	MODERADO	DÉBIL	CATASTRÓFICO	IMPROBABLE	MODERADA
					V.2.4.1	- Incorrecta aplicación de actualizaciones de software en el equipo.											
					V.2.4.2	- Demora en la instalación de parches liberados por el fabricante											
			Abuso de privilegios de acceso	D,A	V.1.5.1	- Mala administración de los perfiles y permisos de usuario	Confidencialidad, Integridad, Disponibilidad	Financiero, Operacional	R2.5	CATASTRÓFICO	IMPROBABLE	MODERADA	DÉBIL	DÉBIL	CATASTRÓFICO	IMPROBABLE	MODERADA
					V.1.5.2	- Falta de un proceso formal y periódico de revisión de los derechos de acceso											
					V.2.5.1	- Falta de revisiones periódicas a los logs del equipo											
					V2.6.1	- Inadecuado control de los accesos físicos a las instalaciones											

			Robo	D	V2.6.2 V2.6.3	- Falta de protección física del edificio, puertas y ventanas. - Falta de mecanismos de monitoreo establecidos para violaciones de seguridad física	Disponibilidad, Confidencialidad	Financiero, Operacional	R2.6	CATASTRÓFICO	IMPROBABLE	MODERADA	MODERADO	DÉBIL	CATASTRÓFICO	EXCEPCIONAL	MODERADA

Anexo 9 Mapa de Calificación Riesgo Inherente



Anexo 10 Evaluación de controles existentes

			Tipo de Control				Otros Criterios de Evaluación de Controles													
Cód. Control	Controles (que existen ahorita relacionados con la vulnerabilidad)	Vulnerabilidades que Controla	Preventivo	Detectivo	Correctivo	Automatización	Segregación de Funciones	Cumplimiento Obligatorio?	Número de vulnerabilidades controladas	Mitiga	Calificación del Control por número de vulnerabilidades controladas	Calificación por Control Preventivo	Calificación por Control Detectivo	Calificación del Control por Correctivo	Calificación por Automatización o No	Calificación por Segregación de Funciones o No	Calificación del Control por Cumplimiento	Calificación por mitigación	Calificación del Control	Fortaleza del control
CON-001	Campañas de concientización sobre phishing.	V.1.1.1 V.1.1.3 V.1.2.1 V.1.4.3	X			Semi-Automático	N/A	NO	4	Probabilidad	2	3	0	0	0	0	0	2	7	DÉBIL
CON-002	Acuerdos de confidencialidad con el personal de la empresa	V.1.1.3 V.1.2.1 V.1.3.3 V.1.4.2	X			Manual	NO	SI	6	Probabilidad	3	3	0	0	1	0	2	2	11	MODERADO
CON-003	Monitoreo periódico de los respaldos de base de datos	V.1.1.3 V.1.3.1	X	X		Semi-Automático	NO	NO	2	Ambos	1	3	2	0	0	0	0	3	9	DÉBIL
CON-004	Definir procedimientos formales de gestión de cambios junto con responsables	V.1.1.1 V.1.1.2 V.1.3.2 V.1.3.3 V.1.4.1 V1.4.2 V.1.4.3 V.1.5.1 V.1.5.2 V.1.5.3 V.1.6.2 V.1.6.3 V.2.3.1 V.2.4.1 V.2.4.2	X	X		Manual	SI	NO	15	Ambos	4	3	2	0	1	2	0	3	15	FUERTE
CON-005	Revisión y actualización de los privilegos asignados conforme el rol en la empresa.	V.1.1.1 V.1.1.2 V.1.2.1 V1.3.2 V.1.3.3 V.1.4.1 V1.4.2 V.1.4.3 V.1.5.1 V.1.5.2 V.1.5.3 V.1.6.3 V.2.3.1 V.2.4.1	X	X	X	Manual	SI	NO	14	Ambos	4	3	2	1	1	2	0	3	16	FUERTE

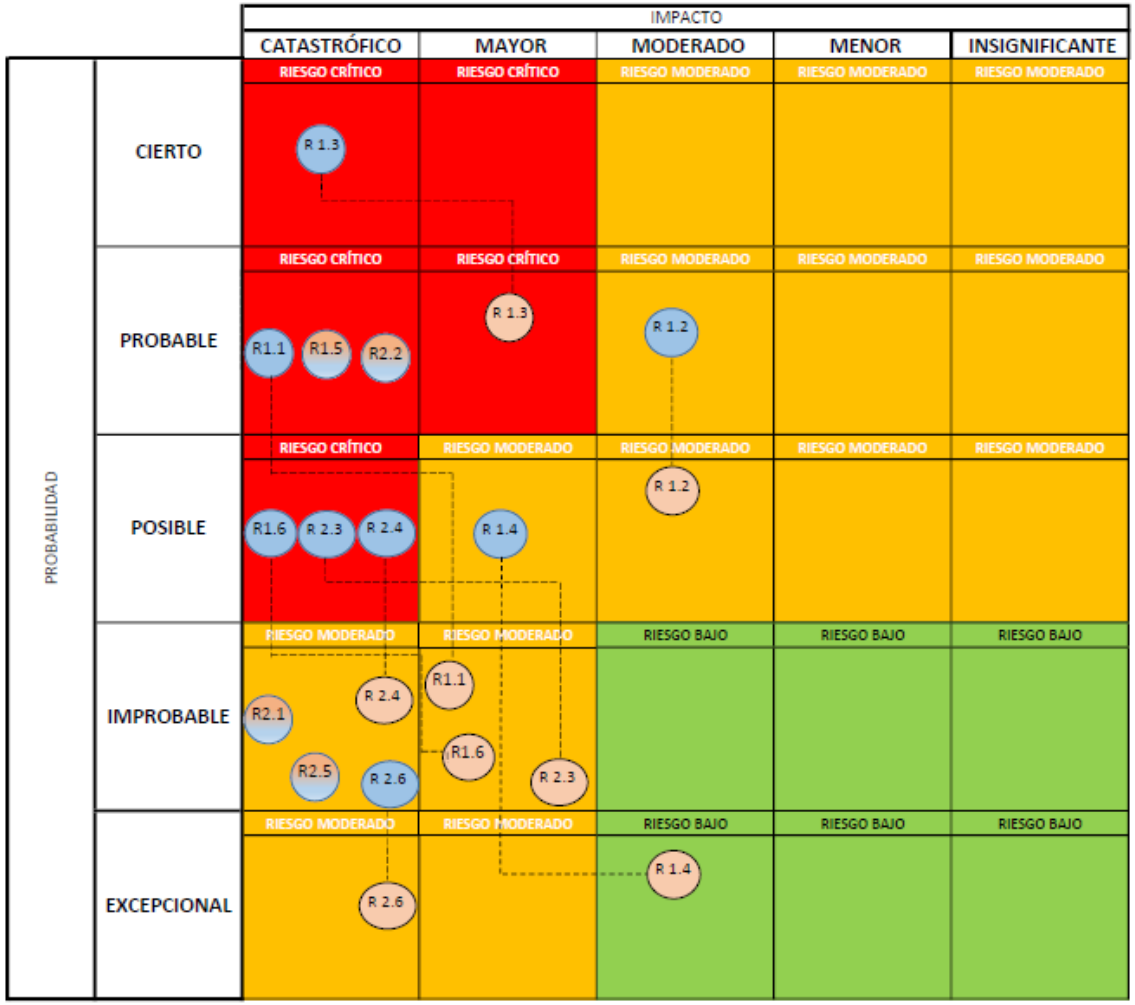
CON-006	Actualización semestral del motor de base de datos	V.1.4.1 V.1.6.1 V.1.6.2	X		X	Manual	NO	SI	3	Ambos	2	3	0	1	1	0	2	3	12	MODERADO
CON-007	Mantenimiento Anual del sistema contraincendios	V.2.1.1	X	X		Manual	N/A	SI	1	Probabilidad	1	3	2	0	1	0	2	2	11	MODERADO
CON-008	Mantenimiento Semestral a las instalaciones físicas de las oficinas	V.2.1.2 V.2.1.3 V.2.2.2 V.2.2.3 V.2.6.2	X	X	X	Manual	N/A	SI	5	Ambos	3	3	2	1	1	0	2	3	15	FUERTE
CON-009	Mantenimientos Semestrales a los equipos del Data Center	V.2.2.1 V.2.2.3 V.2.2.4	X	X		Manual	N/A	SI	3	Probabilidad	2	3	2	0	1	0	2	2	12	MODERADO
CON - 011	Bitácora de control de los accesos físicos a las instalaciones de personal interno y externo a la organización.	V.2.6.1 V.2.6.3	X	X	X	Manual	N/A	SI	2	Ambos	1	3	2	1	1	0	2	3	13	MODERADO
CON - 012	Controles de seguridad física tales como: Cámaras de circuito cerrado, biométrico, uso de credenciales institucionales, guardias de seguridad	V.2.6.1 V.2.6.3	X	X		Manual	N/A	SI	2	Probabilidad	1	3	2	0	1	0	2	2	11	MODERADO

Anexo 11 Calificación de los grupos de controles de la empresa de cobranzas

RIESGO	PROMEDIO CALIFICACION GC	CONTROLES SELECCIONADOS	Reduce	CANTIDAD IMPACTO	CANTIDAD PROBABILIDAD	CANTIDAD AMBOS	MITIGACION PROBABILIDAD	MITIGACION IMPACTO
R. 1.1	11,6	CON-001	Probabilidad	0	2	3	FUERTE	MODERADO
		CON-002	Probabilidad					
		CON-003	Ambos					
		CON-004	Ambos					
		CON-005	Ambos					
R. 1.2	12,25	CON-001	Probabilidad	0	2	2	MODERADO	DÉBIL
		CON-002	Probabilidad					
		CON-004	Ambos					
		CON-005	Ambos					
R. 1.3	13	CON-002	Probabilidad	0	1	3	MODERADO	MODERADO
		CON-003	Ambos					
		CON-004	Ambos					
		CON-005	Ambos					
R. 1.4	12,2	CON-001	Probabilidad	0	2	3	FUERTE	MODERADO
		CON-002	Probabilidad					
		CON-004	Ambos					
		CON-005	Ambos					
		CON-006	Ambos					
R. 1.5	15,5	CON-004	Ambos	0	0	2	DÉBIL	DÉBIL
		CON-005	Ambos					
R. 1.6	14,33	CON-004	Ambos	0	0	3	MODERADO	MODERADO
		CON-005	Ambos					
		CON-006	Ambos					
R. 2.1	13	CON-007	Probabilidad	0	1	1	DÉBIL	DÉBIL
		CON-008	Ambos					
R. 2.2	13,5	CON-008	Ambos	0	1	1	DÉBIL	DÉBIL
		CON-009	Probabilidad					
R. 2.3	14,33	CON-004	Ambos	0	0	3	MODERADO	MODERADO
		CON-005	Ambos					
		CON-006	Ambos					
R. 2.4	14,33	CON-004	Ambos	0	1	2	MODERADO	
		CON-005	Ambos					

		CON-009	Probabilidad					DÉBIL
R. 2.5	15,50	CON-004	Ambos	0	0	2	DÉBIL	DÉBIL
		CON-005	Ambos					
R. 2.6	9,75	CON-008	Ambos	0	1	2	MODERADO	DÉBIL
		CON-011	Ambos					
		CON-012	Probabilidad					

Anexo 12 Mapa de Calificación de Riesgo Residual



Anexo 13 Políticas planteadas a la empresa de cobranzas.

Política de Gestión de Activos

Responsable: El responsable de seguridad de la información

Debe mantener información organizada y actualizada con respecto a los activos y el ciclo de vida de la información que se transmite, procesa, almacena o distribuye en los mismos.

- El inventario de activos debe ser preciso, consistente y debe estar actualizado.
- Cada activo del inventario debe tener un propietario, quien tendrá autoridad sobre el mismo.

Política de Clasificación de la Información

Responsable: El responsable de seguridad de la información

Debe clasificar la información de acuerdo con su importancia y su relevancia con respecto a requisitos legales, valor, sensibilidad y criticidad, considerando riesgos que involucren su revelación o modificación no autorizada.

- Los controles de protección de cada tipo de información deben estar asociados a las necesidades y procesos del negocio, así como al cumplimiento de los requisitos legales.
- El procedimiento de etiquetado de información debe diseñarse conforme los niveles de clasificación planteados.
- La información debe ser manipulada de acuerdo con su nivel de clasificación.

Política de Control de Acceso

Responsable: El responsable de seguridad de la información

Debe proteger los recursos de tratamiento y la información de accesos no autorizados, basados en los requisitos de negocio y de seguridad de la información.

- En el proceso de alta de usuarios se debe considerar la identificación del usuario y las autorizaciones respectivas para sus tareas asegurando, de esta manera, la segregación de funciones.
- Los privilegios de usuarios administradores en los sistemas de la organización son restringidos para individuos específicos y están autorizados únicamente para realizar su trabajo de forma correcta.
- En todos los sistemas o plataformas de uso de la empresa se crearán usuarios asociados a una persona física y cuando se requiera de usuarios genéricos los mismos tendrán un responsable asociado.
- Si existe un cambio en las funciones de un usuario debe eliminarse los accesos relacionados con la función anterior y a su vez asignar los accesos necesarios para las nuevas funciones.
- La custodia de usuarios con privilegios especiales y usuarios genéricos debe permitir identificar al personal que la usa, la justificación o necesidad de su uso y el monitoreo de su utilización.
- Utilizar mecanismos de identificación y autenticación de usuarios de múltiple factor.
- El personal debe cumplir con los lineamientos de la organización para la gestión de contraseñas de acceso personal, las mismas no deben ser transferidas ni reutilizadas.
- Cuando un usuario se desvincula de la organización, se deben retirar los accesos otorgados y la eliminación o inhabilitación del usuario asociado.
- Anualmente se realizará una revisión de los derechos de acceso para verificar si existieron cambios en el perfil y asegurar la correcta asignación de usuarios.

Política de Seguridad Física y Ambiental

Responsable: El responsable de seguridad de la información

Debe prevenir a la organización sobre daños u obstrucciones en la información, considerando riesgos exclusivamente asociados al acceso físico no autorizado a las instalaciones; para ello, se plantean los siguientes lineamientos:

- Las áreas de trabajo deben estar delimitadas físicamente.
- Las áreas donde se encuentran activos de información que contienen información privada y secreta, deben contar con sistemas de bloqueo de acceso y se permite su ingreso únicamente con autorización y/o acompañamiento del ente responsable de su custodia.
- Las áreas de trabajo deben ser distribuidas dentro de la oficina de manera que, tanto el personal como público en general que accede a las mismas no tenga acceso físico o visual a información clasificada, privada o secreta de la organización.
- El personal debe estar capacitado para actuar de manera oportuna ante amenazas externas y ambientales.

Política de Copia de Seguridad

Responsable: El responsable de seguridad de la información

Debe asegurar la preservación de los datos para garantizar la continuidad de las operaciones.

- Los requisitos para la generación de copias de seguridad deben ser establecidos y socializados dentro de la organización.
- El inventario de los soportes de información debe estar actualizado e indicar su contenido, ubicación y responsables.
- Los responsables de los soportes de información son los encargados de mantener el inventario y una copia actualizada de ellos en una ubicación remota.
- Asegurar el buen funcionamiento del proceso de creación de respaldos y disponibilidad de la información con la ejecución de pruebas periódicas trimestrales de recuperación de la información desde los soportes almacenados.

- Encriptar todos los soportes de información existentes.

Política de gestión de vulnerabilidades técnicas

Responsable: El gerente de tecnología

Debe contar con información oportuna de las vulnerabilidades técnicas de los sistemas de información y equipos utilizados en la empresa para evaluar la exposición a las mismas y tomar medidas oportunas.

- El personal debe conocer sus responsabilidades y las funciones a realizar para dar soporte a las vulnerabilidades técnicas.
- Los tiempos de reacción ante vulnerabilidades deben ser evaluados y asignados para mantener la continuidad de la operación.
- Los procedimientos para la gestión de vulnerabilidades deben ser registrados, actualizados y contar con medidas de mitigación para reducir el impacto generado por una amenaza, conocida o no.
- Los activos y sus respectivos componentes físicos o lógicos deben mantenerse actualizados y probados previo a su paso a producción.

Política de Seguridad de las comunicaciones

Responsable: El responsable de seguridad de la información

Debe proteger la información tanto en las redes como en los recursos de tratamiento de la información. Para cumplirlo se necesita:

- Establecer responsabilidades y procedimientos en la gestión de red y sus equipos.
- Realizar un adecuado registro de los eventos y monitoreo que incluya revisiones mensuales de los logs de todos y cada uno de los equipos de red para permitir la detección de acciones relevantes para la seguridad de la información.
- Identificar disposiciones de seguridad para servicios particulares como son los niveles de servicio, requisitos y características de seguridad y

asegurarse que los proveedores del servicio de red cumplen con estas medidas.

- Garantizar la segregación de redes para los distintos servicios de información, usuarios y sistemas.
- Establecer procedimientos y controles que protejan el intercambio de información mediante recursos de comunicación.
- Establecer acuerdos para el intercambio seguro de información de la empresa y terceros.
- Proteger la mensajería electrónica.
- Actualizar y documentar oportunamente los acuerdos de confidencialidad

Política de Gestión del Control de Cambios

Responsable: El responsable de seguridad de la información

Debe garantizar que los cambios realizados en los activos o sistemas de información empresarial no afectan a los procesos y sistemas del negocio para lo cual se debe considerar:

- La creación de un procedimiento detallado y formal de control de cambios que involucre a diferentes responsables garantizando la seguridad de la información.
- La identificación y el registro de todos y cada uno de los cambios que se realicen.
- El proveedor de la solución o equipo en el cual se ejecutará el cambio es quien debe ejecutar el cambio para ello debe asegurarse de contar con la asesoría o de ser necesario el acompañamiento del fabricante.
- El impacto que pueden tener los cambios en la gestión del servicio.
- Todo procedimiento de gestión de cambios debe tener un proceso de rollback asociado que permita en el caso de algún problema poder reversar el cambio y continuar con la operación.
- Antes de la ejecución de un cambio se debe informar a todos los involucrados, quienes son los responsables de efectuar las pruebas pertinentes luego de la aplicación de los cambios.

- Previa a la ejecución de un cambio se debe realizar respaldos de los servidores o de las configuraciones de los equipos.

Política de Gestión de Contraseñas

Responsable: El responsable de seguridad de la información

Debe establecer sistemas para gestión de contraseñas que permitan al usuario crear contraseñas seguras.

- El personal debe mantener la confidencialidad de su clave de acceso, utilizando contraseñas individuales y asegurándose de no divulgarlas.
- Siempre que se sospeche o exista una exposición de contraseñas, las mismas deben ser cambiadas.

Anexo 14 Planes de Acción

Plan de acción											
Vulnerabilidad asociada	COD. CONTROL	Descripción del control	Fortaleza del control	Severidad RI	Severidad RR	Vulnerabilidad	Plan de acción	Capacidad de ejecución	Tipo	Alcance	Responsable
V.1.1.1 V.1.1.3 V.1.2.1 V.1.4.3	CON-001	Campañas de concientización sobre phishing.	DÉBIL	CRÍTICA	MODERADA	V.1.1.1	Adquirir un software para la automatización de campañas y entrenamientos sobre pishing.	Mediano Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área Financiera - Área de Tecnología
						V.1.1.1	Diseñar un plan semestral de capacitación sobre phishing que contemple campañas de simulacros.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología.
						V.1.1.1	Evaluar periódicamente mediante los resultados de las campañas de phishing para reforzar concientización en los usuarios vulnerables.	Mediano Plazo	Mejora del Control	Autónomo	Responsable de la seguridad de la información
V.1.1.2 V.1.1.3 V.1.2.1 V.1.3.3 V.1.4.2 V.2.3.1	CON-002	Acuerdos de confidencialidad con el personal de la empresa	MODERADO	MODERADA	MODERADA	v.1.1.2	Diseñar procedimientos de manejo de la información conforme su nivel de clasificación.	Mediano Plazo	Mejora del Control	Autónomo	Responsable de la seguridad de la información
						v.1.3.3	Crear y cumplir políticas para el alta y baja de usuarios.	Mediano Plazo	Mejora del Control	Organizacional	- Área de Recursos Humanos - Área de Tecnología
						v.1.4.2 v.1.5.2	Revisión anual de los derechos de acceso del personal de acuerdo a su cargo y función	Corto Plazo	Mejora del Control	Organizacional	- Área de Recursos Humanos - Área de Tecnología
V.1.1.3 V.1.3.1	CON-003	Monitoreo periódico de los respaldos de base de datos	DÉBIL	CRÍTICA	CRÍTICA	v.1.3.1	Definir y acatar las políticas de copia de seguridad respecto a la ejecución de pruebas periódicas trimestrales y contar con evidencias de dichas pruebas.	Corto Plazo	Mejora del Control	Autónomo	Área de Tecnología
						V.1.1.3	Establecer un proceso de encriptación de los respaldos de la base de datos.	Corto Plazo	Mejora del Control	Autónomo	Área de Tecnología

						V.1.4.1	Establecer políticas y procedimientos para la gestión de cambios.	Largo Plazo	Mejora del Control	Organizacional	- Area de Tecnología - Responsable de Seguridad de la información
V.1.1.1 V.1.1.2 V.1.3.2 V.1.3.3 V.1.4.1 V1.4.2 V.1.4.3 V.1.5.1 V.1.5.2 V.1.5.3 V.1.6.2 V.1.6.3 V.2.3.1 V.2.4.1 V.2.4.2	CON-004	Definir procedimientos formales de gestión de cambios junto con responsables	FUERTE	MODERADA	BAJA	V.1.6.2	Implementar una herramienta que permita tener un historial de los cambios realizados.	Largo Plazo	Mejora del Control	Organizacional	- Área Financiera - Área de Tecnología
						v.2.3.1	Establecer un proceso disciplinario para incumplimientos de los procesos de gestión de cambios.	Mediano Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Recursos Humanos
						v.1.3.2	Implementar doble factor de autenticación tanto para aplicativos como para correo electrónico empresarial.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología
						v.1.4.3	Definir y cumplir políticas para la gestión de contraseñas	Mediano Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área de Tecnología
						V.1.6.3 V.2.4.1	Incluir en el procedimiento de gestión de control de cambios la descripción detallada de las configuraciones que se deben realizar.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología
						V.2.4.2 V.1.6.1	Establecer procedimientos para la gestión de vulnerabilidades técnicas que consideren el tiempo de aplicación de actualizaciones dependiendo del activo.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología
						v.1.5.3	Revisión mensual de los logs de las bases de datos.	Mediano Plazo	Implementación del Control	Autónomo	Área de Tecnología
V.1.1.1 V.1.1.2 V.1.2.1						V.1.2.1	Establecer e implementar mecanismos de monitoreo para violaciones de seguridad como por ejemplo un SIEM (Security Information and Event Management)	Mediano Plazo	Mejora del Control	Organizacional	- Área Financiera. - Área de Tecnología.

V1.3.2 V.1.3.3 V.1.4.1 V1.4.2 V.1.4.3 V.1.5.1 V.1.5.2 V.1.5.3 V.1.6.3 V.2.3.1 V.2.4.1	CON-005	Revisión y actualización de los privilegos asignados conforme el rol en la empresa.	FUERTE	CRÍTICA	CRÍTICA	1.5.1	Establecer políticas de seguridad de la información donde se definan los responsables directos y socializarla con el personal de la organización.	Corto Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área de Tecnología
						1.5.1	Establecer procesos disciplinarios para el incumplimiento de las responsabilidades en seguridad de la información.	Mediano Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área de Tecnología
						V.1.5.2	Implementar y cumplir políticas de control de acceso	Corto Plazo	Mejora del Control	Organizacional	- Responsable de la seguridad de la información - Área de Tecnología
V.1.4.1 V.1.6.1 V.1.6.2	CON-006	Actualización semestral del motor de base de datos	MODERADO	CRÍTICA	MODERADA	-	Revisar cada tres meses si existen nuevas actualizaciones para el motor de base de datos, si existen aplicarlas.	Corto Plazo	Mejora del Control	Autónomo	- Área de Tecnología
V.2.1.1	CON-007	Mantenimiento Anual del sistema contraincendios	MODERADO	MODERADA	MODERADA	v2.1.1	Realizar revisiones y mantenimientos preventivos trimestrales del sistema contra incendios	Corto Plazo	Mejora del Control	Organizacional	- Área de Mantenimiento - Área Financiera
						v2.1.1	Mantener un registro histórico de fallas reales o posíbles, así como de los mantenimientos preventivos y correctivos.	Corto Plazo	Mejora del Control	Autónomo	Área de Mantenimiento
						v2.1.1 V.2.1.2	Implementar un Data Center Alterno que brinde las funcionalidades básicas para brindar continuidad al negocio	Largo Plazo	Mejora del Control	Organizacional	- Área de Mantenimiento - Área Financiera - Área de Tecnología

V.2.1.2 V.2.1.3 V.2.2.2 V.2.2.3 V.2.6.2	CON-008	Mantenimiento Semestral a las instalaciones físicas de las oficinas	FUERTE	CRÍTICA	CRÍTICA	V.2.1.3 V.2.6.2	Contratar equipos inmobiliarios especializados para efectuar revisiones, cambios por seguridad y mantenimientos trimestrales de las instalaciones físicas del edificio de la empresa.	Corto Plazo	Mejora del Control	Organizacional	- Área de Mantenimiento - Área Financiera - Área de Tecnología
						v.2.2.2	Mantener un registro histórico de fallas en las instalaciones físicas reales o posibles, así como de los mantenimientos preventivos y correctivos.	Corto Plazo	Mejora del Control	Autónomo	Área de Mantenimiento
V.2.2.1 V.2.2.3 V.2.2.4	CON-009	Mantenimientos Semestrales a los equipos del Data Center	MODERADO	CRÍTICA	MODERADA	v.2.2.3	Implementación de un nuevo UPS que cubra la totalidad del DataCenter de la empresa	Mediano Plazo	Mejora del Control	Organizacional	- Área de Mantenimiento - Área Financiera - Área de Tecnología
						v.2.2.1	Mantenimientos trimestrales a los equipos	Mediano Plazo	Mejora del Control	Organizacional	- Área Financiera - Área de Tecnología
						v.2.2.1	Mantener un registro de fallos y de mantenimientos realizados.	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología
						v.2.2.4	Supervisar la utilización de los recursos de los equipos y realizar proyecciones futuras de capacidad	Mediano Plazo	Mejora del Control	Autónomo	Área de Tecnología
V.2.5.1	CON -010	Revisión mensual de los logs del equipo.	NO EXISTE	CRÍTICA	MODERADA	v.2.5.1	Revisión mensual de los logs de los equipos y registrarlos.	Mediano Plazo	Implementación del Control	Autónomo	Área de Tecnología
V.2.6.1 V.2.6.3	CON - 011	Bitácora de control de los accesos físicos a las instalaciones de personal interno y	MODERADO	MODERADA	MODERADA	v2.6.1	Implementar un sistema para el registro automático de accesos físicos que incluya identificaciones individuales (Tarjeta Magnética) que deberán ser utilizadas únicamente por personal autorizado para el ingreso a las instalaciones físicas.	Mediano Plazo	Mejora del Control	Organizacional	- Área de Mantenimiento - Área Financiera - Área de Tecnología

		externo a la organización.				v2.6.3	El acceso del personal externo a las instalaciones debe ser con previa autorización y acompañamiento de personal autorizado.	Corto Plazo	Mejora del Control	Organizacional	- Área de Recursos Humanos -Área de Tecnología
V.2.6.1 V.2.6.3	CON - 012	Controles de seguridad física tales como: Cámaras de circuito cerrado, biométrico, uso de credenciales institucionales, guardias de seguridad	MODERADO	MODERADA	MODERADA	v2.6.1	Implantar políticas para el uso correcto de la credencial, tanto para el personal como para visitantes.	Corto Plazo	Mejora del Control	Autónomo	- Área de Recursos Humanos
						v.2.6.3	Realizar revisiones trimestrales de la efectividad de las políticas implantadas referentes al uso de credenciales.	Mediano Plazo	Mejora del Control	Autónomo	- Área de Recursos Humanos