FACULTAD DE POSTGRADOS

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN DEL CALL CENTER “NM”

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

Profesor Guía:

Juan López

Autores:

Fernando Jiménez

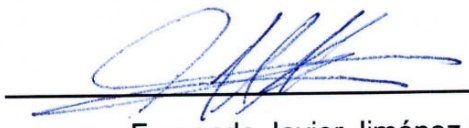
Juan Chávez

Año

2022

DECLARACIÓN DE AUTORÍA

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



Fernando Javier Jiménez Fuentes

DECLARACIÓN DE AUTORÍA

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

Juan Gabriel Chávez Borrallos

RESUMEN

“NM” es una empresa de call center que atiende llamadas entrantes y salientes de ciudadanos del Ecuador. Maneja información privada que debe ser protegida, tanto por requerimientos legislativos, como por intereses propios de la empresa.

El estudio presentado en este proyecto representa el desarrollo del programa del sistema de gestion de seguridad de la información del call center “NM” el cual fue ejecutado en 5 fases.

Cada fase cuenta con una estructura metodológica simple que permiten interactuar entre ellas, formado parte de un sistema de gestión de seguridad de la información.

Se inicia analizando la situación actual de la seguridad de información en la empresa, estudiando de la misma manera las debilidades que representan riesgos para la continuidad del negocio (desde un punto de vista de seguridad de la información).

Finalmente, se culmina proponiendo cambios que permitan cerrar brechas en el sistema de seguridad de la información de la empresa.

ABSTRACT

"NM" is a business dedicated to provide call center services which answer inbound and outbound calls from citizen in Ecuador. It handles private information that must be protected to comply with legislative requirements as well as to protect its own interests.

The study presented in this document represents the development of the program for the information security management system (ISMS) in the call center "NM", which was performed during 5 phases.

Each phase has a simple methodological structure that allows it to interact between them, while being a part of the information security management system.

We begin analyzing the current status in terms of information security in the enterprise, studying at the same time, the weaknesses that represent risks against business continuity.

Finally, the development is closed by proposing changes that will allow to close breaches in the ISMS.

INDICE

INTRODUCCIÓN

Desarrollar un SGSI es una actividad que debe ser desarrollada de una manera metodológica. En el mercado, existen muchas organizaciones que no tienen implementación de seguridad en su institución como el caso que se presenta en este trabajo.

La organización estudiada es una empresa de call center, orientada actualmente a fines comerciales, brindando soluciones de telemarketing a sus clientes. La ventaja competitiva consiste en el uso de los sistemas de información para automatizar la mayor cantidad de procesos que realizan los ejecutivos, proporcionando acceso inmediato a toda la información necesaria para la gestión de los clientes finales.

Uno de sus objetivos empresariales es expandir las operaciones, abordando una mayor cantidad de campañas, por lo que se espera hacer uso de una mayor cantidad de datos de lo que actualmente se utiliza, poniendo a la empresa en una situación de riesgo ante el manejo de la información.

La empresa “NM” no cuenta con un sistema de gestión de seguridad de la información y todos sus procesos se han implementado siguiendo un paradigma empírico.

El proceso seguido consiste en identificar de una manera general, los activos críticos de información, analizar sus debilidades y vulnerabilidades para luego establecer directrices que habilitará la implementación de un gobierno a nivel de seguridad de la información.

De esta manera, el presente trabajo propone la aplicación de un sistema de seguridad de la información estructurado, basado en la norma ISO27001:2013, el cual le permitirá a la empresa mantener procesos bien establecidos que pueden seguirse para asegurar la confidencialidad, integridad y disponibilidad de la información, alineándose al objetivo empresarial de crecimiento.

1. DESARROLLO DEL PROGRAMA

1.1. Objetivo General

Desarrollar el Sistema de Gestión de la Información que permita realizar un adecuado manejo de los datos y la mitigación del riesgo al que están expuestos, de manera que el CALL CENTER apoye la disponibilidad, confidencialidad e integridad de sus datos, elevando de esta manera su nivel de gestión empresarial.

1.2. Objetivos Específicos

1. Proteger la información del cliente directo
2. Proteger la información del cliente indirecto
3. Proteger la operatividad de la empresa
4. Establecer lineamientos bases que permitan la elaboración y evolución del SGSI de la empresa

1.2. Metodología

El proceso de diseño del Sistema de Gestión de Seguridad de la Información (SGSI) está conformado por 6 fases generales que permiten documentar la situación actual, así como un plan de acción para alcanzar el objetivo general de implementar el SGSI.

Las fases son ejecutadas y documentadas utilizando instrumentos de evaluación ajustadas a la realidad de la empresa, tomando como referencia la normativa ISO27001:2015, de manera que permita establecer la situación actual y se enfoque en cumplir en un porcentaje aceptable los controles del ANEXO A de la norma, orientándose de esta forma a mitigar ataques y controlar vulnerabilidades que afecten la integridad, disponibilidad y confidencialidad de la información.

Adicionalmente, se desarrolla un “caso de negocio” que describe un ataque sufrido por una empresa muy parecida al caso de estudio y explica el por qué de la importancia de aplicar un SGSI (Ver Anexo 1 – Caso de estudio).

1.2.1 Alcance

El programa es desarrollado en 5 fases:

Fase 1 – Diagnóstico

Se evalúa la situación actual de la empresa en términos de seguridad de la información

Fase 2 – Clasificación de los tipos de información

Consiste en clasificar la información con la que trabaja la empresa

Fase 3 – Inventarios de activos de información

Enumera los activos que dan soporte a la información utilizada por la empresa

Fase 4 – Análisis de amenazas y vulnerabilidades de activos de información críticos

Estudia las amenazas y vulnerabilidades que existen en los activos de información con la finalidad de protegerles

Fase 5 – Documentos claves del SGSI

Pretende entregar los documentos principales del SGSI que serán los lineamientos a seguir para la implementación del sistema

1.3. Fase 1-Diagnóstico

1.3.1. Metodología

Para iniciar con el proceso de levantamiento del SGSI, el primer paso ejecutado fue analizar cómo se encuentra actualmente la organización respecto a la implementación de la seguridad.

El instrumento de evaluación utilizado está basado en la norma ISO27001:2013 (International Organization for Standardization, 2013), la cual contiene generalidades útiles para empezar a levantar un sistema de gestión de seguridad de la información.

En vista de que la empresa “NM” ha implementado de forma empírica todos sus procesos, no cuenta con un SGSI establecido. Con esta característica en mente, se desarrolla un instrumento de evaluación basado en las generalidades de la norma, lo cual permitirá establecer lineamientos de alto nivel, respecto a lo que se debería contar como empresa, desde el punto de vista de seguridad.

El instrumento desarrollado designa 7 componentes generales, apoyados en cada una de las secciones globales de la norma (las cuales comienzan desde el ordinal 4). Específicamente:

4. **Contexto**

   Relacionado con el entendimiento general de la empresa. Su motivación es comprender las necesidades que existen en la organización, incluyendo su contexto pero tambien tomando en cuenta el bienestar de las partes interesadas (identificándolas en el proceso).

5. **Liderazgo**

   Este punto pretende designar la responsabilidad de compromiso a la alta gerencia, sobre el sistema de gestión de la seguridad de la información, ya que un compromiso deficiente de los directivos de la organización, dificulta considerablemente la implementación del programa; incluso hasta exponerlo al fracaso.

6. **Planificación**

   Evalúa el nivel de preparación que tiene la organización ante eventos esperados o inesperados de seguridad de la información. Incluye elementos orientados a asegurarse que el programa alcance los objetivos trazados; para ello define directrices orientados a identificar los elementos de información, sus vulnerabilidades, responsables e impacto en caso de compromiso. De la misma manera, considera la mejora contínua y el nivel de integración del SGSI con los procesos de la empresa y el tratamiento y mitigación de los riesgos mediante la aplicación de controles.

7. **Soporte**

   Este componente se centra en contar con los recursos necesarios para alcanzar los objetivos del sistema de gestión de la seguridad de la información. La empresa debe asegurarse de que las personas encargadas del desarrollo del programa sean competentes desde el punto de vista de entrenamiento y educación. Igualmente, evalúa la comunicación de la información con entidades internas y externas. Adicionalmente, establece directrices para garantizar que la información documentada se encuentre disponible, asegurada y versionada.

8. **Operación**

   Intervenir las operaciones de la empresa constituye un esfuerzo e inversión considerable para cualquier organización, sin embargo, para el éxito del sistema de gestión de seguridad de la información, tanto el programa como la operación deben estar coordinadas de manera que se mantenga una constante revisión y monitoreo de cambios tanto esperados como no esperados en los procesos. Mantiene también directrices de control de procesos subcontratados de manera que ningún procedimiento quede excluído de la cobertura del SGSI.

9. **Evaluación de Desempeño**

   Se asegura de que el SGSI se encuentre optimizado mientras se encuentre activo en la organización. Incluye directrices de monitoreo, medición, análisis y evaluación de elementos definidos por la organización, así como sus responsables. Adicionalmente, incluye la participación de la alta gerencia, quienes deben conocer las decisiones tomadas por los responsables del SGSI respecto a los elementos que serán constantemente evaluados en este punto, así como los resultados obtenidos de estas calificaciones. De igual manera, se incluye una subsección de auditoría interna para asegurarse que el programa cumple con los requerimientos de la organización y se alínea con los lineamientos de la norma.

10. **Mejoras**

    Se centra en tomar acciones correctivas ante las “no conformidades” halladas, incluyendo las actividades que se ejecutan al momento y durante la incidencia, la documentación generada luego de solventado el inconveniente, el manejo de las consecuencias desencadenadas por el evento, y las acciones ejecutadas para corregir el problema. Adicionalmente, contiene una directriz de mejora contínua del programa.

En el instrumento desarrollado, cada componente se evalúa en un rango del 0 al 100%. El promedio del conjunto representa el resultado total de la aplicación del instrumento; el objetivo es alcanzar en cada apartado 100% para su evaluación. En caso de que no se alcance, la diferencia es denominada “brecha”.

La escala de evaluación utilizada representa una apreciación del estado actual, desde la implementación más baja (0%) hasta una aplicación alta (100%). En Tabla 1 - Tabla de escala de valoración de SGSI se describe el criterio utilizado.

Calificación	Criterio
0	No existen controles ni procesos aplicados para el apartado. La organización no reconoce que existe un problema que debe ser tratado.
20	La organización reconoce la existencia del problema pero no tiene procesos establecidos ni estandarizados. El proceso se aplica de modo empírico.
40	Se han implementado de manera regular los controles y procesos; sin embargo, su aplicación depende de la voluntad y conocimiento individual de cada persona. No existe formación ni comunicación formal sobre los procedimientos.
60	Existen controles y procesos documentados y bien comunicados pero la aplicación de los mismos no son controladas ni se analiza desviaciones de los objetivos.
80	Existen controles y procesos bien documentados y comunicados. Se monitorean y miden para asegurar que los controles funcionan eficientemente. Las buenas prácticas son omitidas en ocasiones y en algunas oportunidades no se aplica procesos de mejora contínua.
100	La aplicación de controles y procesos, además de estar bien documentados, son monitoreados constantemente, incluso mediante herramientas automatizadas, orientándose a resultados de mejora contínua.

Tabla 1 - Tabla de escala de valoración de SGSI

1.3.2. Resultados

Durante la evaluación se puede apreciar en primera instancia que el contexto de la empresa y requerimientos de la seguridad de la información no son conocidos claramente ni están establecidos de manera formal. Algunas necesidades son identificadas mediante conocimiento empírico de las personas que administran o ejecutan los procesos. Durante la evaluación se obtiene un 13% de avance para este punto.

El componente de liderazgo es uno de los más altos ya que la alta gerencia sí reconoce la necesidad de aplicación de la seguridad en todas sus áreas de desempeño. Los directivos entienden que la información que se maneja en sus procesos son importantes para el correcto funcionamiento de los servicios que se prestan en la organización y de alta importancia para los titulares, por lo tanto se encuentran comprometidos con implementación del SGSI. Algunas políticas de seguridad son aplicadas de forma empírica las cuales son responsabilidad del área de TI; este componente cuenta con un 50% de avance en su evaluación.

En cuanto a la planificación, no existe en la empresa ningún tipo de acciones que permitan tratar o identificar los riesgos y las oportunidades para mitigarlos. Salvo aquellas actividades que se ejecutan diariamente durante el desempeño normal de las operaciones y no cuentan con un marco de trabajo establecido. Este componente es el más bajo, con 0% de avance obtenido en la evaluación.

En vista de que la alta gerencia sí reconoce las necesidades de un sistema de gestión de la seguridad de información, se aplican ciertos procesos para garantizar que se cuenta con los recursos necesarios para implementarlo. La dirección evalúa al personal según sus cualidades y preparación académica con la finalidad de mantener cierto control en los recursos de información que se manejan. Existe una comunicación no metódica de la importancia de la seguridad de información a los integrantes de la empresa; este componente obtiene 50% de avance en su evaluación.

El componente “Operación” tiene 0% de avance ya que todas las operaciones se realizan de una forma reactiva según las necesidades de las campañas del momento. Ninguna de las actividades toman en cuenta la seguridad de la información durante sus flujos.

La evaluación de desempeño del sistema de gestión de seguridad de la información obtiene también una baja calificación en la evaluación (5%) ya que no existe un SGSI implementado en la empresa. El único ítem que aporta a este componente es el compromiso de la alta gerencia con la seguridad de la información ya que la dirección es informada de forma verbal sobre eventos y acciones tomadas respecto a elementos de la seguridad de la información.

Finalmente, el componente de mejoras obtiene un 20% de avance respecto a la evaluación pues las no conformidades y acciones tomadas se mantienen documentadas de una manera informal, vía correo electrónico.

En Figura 1 - Estado actual y brecha del SGSI ISO27001:2013, puede observarse la evaluación generalizada de cada uno de los puntos.

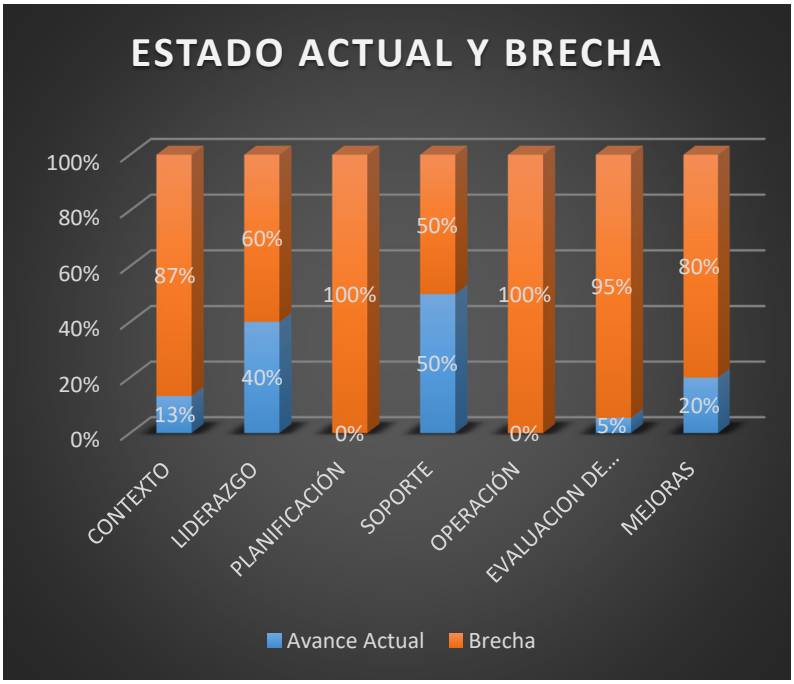


Figura 1 - Estado actual y brecha del SGSI ISO27001:2013

En Tabla 2 - Roadmap de implementación, se establecen los tiempos de duración aproximado para la implementación de los artefactos necesarios para cerrar las brechas encontradas.

Artefacto	Duración
Desarrollar el documento de contexto que incluye los objetivos de la empresa, misión,visión y factores externos e internos	2 meses
Elaboración de documentación de partes interesadas y requisitos de seguridad	1 mes
Elaboración del alcance del SGSI	1 semana
Elaboración de la documentación SGSI * Desarrollo de documentación formal de asignación de roles y responsabilidades en el SGSI * Desarrollo de la documentación de la política y objetivos de seguridad de la información * Elaboración de documento formal respecto a los presupuestos asignados al SGSI	6 meses
Creación de plan de comunicación a la dirección respecto a temas del SGSI Creación de plan para seguimiento de comunicación a la dirección respecto a temas del SGSI	1 mes
Desarrollo del inventario de información Desarrollo del documento de declaración de aplicabilidad Implementar el análisis de riesgo e impacto Desarrollo de la metodología para el tratamiento de riesgos	6 meses
Desarrollo de documentación resumen del SGSI	1 semana
Apertura de archivo de contrataciones Selección y aplicación de un framework para la evaluación de capacidades del personal del SGSI	2 meses
Creación de metodología para control de documentación	2 meses
Desarrollo del análisis y documentación de procesos	1 año
Desarrollo e implementación del plan de tratamientos de riesgos Documentación del plan de tratamiento de riesgos	6 meses
Creación de plan de comunicación para el personal	1 mes
Creación de un plan de comunicación para el SGSI	1 mes
Desarrollo de plan de auditoría * Elaboración de un plan de auditoría * Creación de comités de auditoría interna	2 meses

Tabla 2 - Roadmap de implementación

1.3.3. Anexos

- Anexo 1 – Caso de negocio (Att001 - Caso de Negocio.pptx)
- Anexo 2 – Evaluación de la situación actual del SGSI (Att002 - Analisis Situacion Actual ISO27001.xlsx)
- Anexo 3 – Roadmap de implementación (Att003 - Roadmap de implementacion.xlsx)

1.4. Fase 2 – Clasificación de los tipos de información

1.4.1. Metodología

Cliente directo y secundario

La empresa estudiada es un call center que maneja información principalmente de dos fuentes diferentes: los clientes directos y los clientes secundarios.

Los clientes directos son aquellas entidades, organizaciones o empresas que contratan directamente los servicios de call center para lograr un objetivo, bien sea de atención al cliente o de marketing; usualmente, el cliente directo proporciona información sobre sus consumidores directos.

Los clientes secundarios están conformado por los clientes directos de las empresas que contratan los servicios de call center. Para ilustrar el escenario, se plantea el siguiente ejemplo:

> *La empresa (ficticia) de telecomunicaciones "TELECOMEC" proporciona servicios de telefonía celular a sus clientes. Tiene una cartera de más de un millón de clientes; "TELECOMEC" desea realizar a sus subscriptores una encuesta de satisfacción de servicio y para ello contrata al call center "NM".*
>
> *"TELECOMEC" proporciona a "NM" la información de contacto de sus subscriptores de manera que pueda realizar la encuesta.*

En este escenario, el cliente directo es "TELECOMEC" mientras que los clientes secundarios están conformados por los subscriptores de "TELECOMEC".

La información manejada por la organización está compuesta por diversos tipos de elementos que en su totalidad conforman un cuerpo amplio de datos. Enumerarlos de una manera no estructurada podría ocasionar que se omitan ciertos componentes lo cual debilitaría la robustez del programa.

Por este motivo, se aplica un estudio metódico de clasificación de la información dentro de la empresa “NM”.

La metodología consiste primero en identificar los dominios a los cuales pertenece la información, determinando a la vez la persona que es responsable de la misma (el “dueño”) . Posteriormente se desagregan los dominios, detallando los tipos de información que lo conforman y describiendo de manera general lo que contienen. Finalmente, se designa un nivel de criticidad tanto para el tipo de información como para el dominio, lo cual permitirá comprender cuál es la información que representa un mayor valor para la empresa.

Un call center tiene la peculiaridad de que la información que administra es altamente dinámica, variando con cada campaña que ingresa bajo su gestión. Es por ello que identificar dominios se convierte en una tarea complicada para implementar el SGSI. Para este estudio se aplicó una técnica de “*top-down processing*” la cual consiste en “...utilizar nuestro conocimiento previo sobre el mundo para poder otorgarle sentido a la entrada (sensorial).” (Rookes & Willson, 2005).

Para la designación de niveles de criticidad, se aplica un instrumento general desarrollado para la empresa, el cual toma en cuenta el nivel de afectación (alto riesgo, riesgo moderado, bajo riesgo y ningún riesgo) de los siguientes criterios de impacto:

1. Ventaja Competitiva: Representada por la afectación a los elementos que la empresa considera su ventaja competitiva respecto a la competencia.
2. Nivel Operativo: Representada por la cantidad de horas de afectación a las actividades misionales de la empresa.
3. Ingresos: Representado por la disminución del rédito obtenido por la empresa.
4. Cumplimiento de normativas: Representado por el cumplimiento de leyes, normativas y directrices de cliente directo.

Las ventajas competitivas determinadas en el instrumento representan aquellos elementos que la dirección, en conjunto con el área operativa de la empresa,

consideran de mayor relevancia para la diferenciación del negocio. (Ver Tabla 3 - Ventajas competitivas de la empresa "NM").

Ventajas Competitivas
La empresa cuenta con un sistema de marcación automatizado ajustable a la necesidad de la campaña
Se mantiene un repositorio de datos proveniente de fuentes públicas, que cuenta con información de clientes, incluso si no han sido aun contactados
El proceso de toda llamada es almacenado y alimenta al repositorio de datos de manera continua
La mayoría de los procesos administrativos de operaciones a nivel de telefonía toman menos de 2 minutos
Todas las operaciones se encuentran integradas de manera que el agente cuente con todos los datos en una sola pantalla

Tabla 3 - Ventajas competitivas de la empresa "NM"

El instrumento toma en cuenta la confidencialidad, disponibilidad e integridad. Esta tríada “ayuda al personal de soporte y administrativo del gobierno de IT obtener un buen entendimiento desde cero, sobre el nivel de seguridad en el que debe enfocarse y su importancia para la organización.” (John R., 2017)

Un elemento de información es ubicado en el riesgo correspondiente, cuando cualquiera de los ítems de la tríada alcanza el criterio de impacto. Por ejemplo, si para la “información de campaña”, la afectación de confidencialidad e integridad no pone en riesgo o tiene un bajo riesgo de los criterios de impacto, pero su disponibilidad podría dejar inoperativa a la empresa por más de 24 horas, entonces el item es ubicado en la sección de “alto riesgo”.

Cada tipo de información puede tener una calificación de máximo 300 puntos. “Ningún riesgo” representa 0 puntos, mientras que el resto de las clasificaciones de riesgo suma 100 puntos a la escala cada uno; Adicionalmente, se utiliza un criterio cualitativo denominado “Criticidad Operativa”, basado exclusivamente en el papel que juega el item para mantener activa las operaciones; La criticidad operativa se evalúa según la siguiente escala:

1. Ninguno: La operación no se ve afectada por la ausencia de este elemento

2. Bajo: La operación se afecta levemente sin este elemento
3. Medio: La operación se afecta considerablemente sin este elemento
4. Alto: La operación no puede continuar sin este elemento

Cada elemento de información es etiquetado con la letra “I” seguido de un número de 3 dígitos.

Tabla 4 - Criterios de evaluación de criticidad de la información (parte 1) y Tabla 5 - Criterios de evaluación de criticidad de la información (parte 2) resume el criterio utilizado en el instrumento.

	Bajo Riesgo				Ningún riesgo			
Afectación de ->	**Ventaja Competitiva**	**Nivel Operativo**	**Ingresos**	**Cumplimiento de normativas**	**Ventaja Competitiva**	**Nivel Operativo**	**Ingresos**	**Cumplimiento de normativas**
Confidencialidad (Accesos no autorizados a la información)	< 25 % hasta 15%	< 16 horas hasta 1 hora	< 15% hasta 5%	Incumplimiento de reglas internas	< 15%	< 1hora	< 5%	No aplica
Integridad (Alteración de la información por eventos maliciosos o inesperados)	< 25 % hasta 15%	< 16 horas hasta 1 hora	< 15% hasta 5%	Incumplimiento de reglas internas	< 15%	< 1hora	< 5%	No aplica
Disponibilidad (Inhabilidad para acceder a la información en el momento requerido)	< 25 % hasta 15%	< 16 horas hasta 1 hora	< 15% hasta 5%	Incumplimiento de reglas internas	< 15%	< 1hora	< 5%	No aplica

Tabla 4 - Criterios de evaluación de criticidad de la información (parte 1)

	Alto Riesgo				Riesgo Moderado			
Afectación de ->	**Ventaja Competitiva**	**Nivel Operativo**	**Ingresos**	**Cumplimiento de normativas**	**Ventaja Competitiva**	**Nivel Operativo**	**Ingresos**	**Cumplimiento de normativas**
Confidencialidad (Accesos no autorizados a la información)	> 70%	> 24 horas	> 50%	Incumplimiento de disposiciones gubernamentales	< 70% hasta 25%	< 24 horas hasta 16 horas	< 50% hasta 15%	Incumplimiento de reglas del cliente
Integridad (Alteración de la información por eventos maliciosos o inesperados)	> 70%	> 24 horas	> 50%	Incumplimiento de disposiciones gubernamentales	< 70% hasta 25%	< 24 horas hasta 16 horas	< 50% hasta 15%	Incumplimiento de reglas del cliente
Disponibilidad (Inhabilidad para acceder a la información en el momento requerido)	> 70%	> 24 horas	> 50%	Incumplimiento de disposiciones gubernamentales	< 70% hasta 25%	< 24 horas hasta 16 horas	< 50% hasta 15%	Incumplimiento de reglas del cliente

Tabla 5 - Criterios de evaluación de criticidad de la información (parte 2)

1.4.2. Resultados

Dominios

En el marco del estudio se identifican 9 dominios de información sobre los cuales reposa la funcionalidad de la empresa.

1. Cliente directo o primario

   Está conformada por datos de la entidad que contrata los servicios de callcenter. Incluye información general de la organización, detalles del contrato, condiciones, etc.
2. Cliente secundario

   Son los datos referente a las personas que serán contactadas por el callcenter. La información manejada depende de lo proporcionado por el contratante (cliente directo), sin embargo usualmente incluye, nombres y apellidos, identificación, contactos.
3. Campañas

   Cada contratante puede solicitar múltiples servicios al call center. Cada uno de ellos es catalogado como “campaña”. En este dominio se maneja la información directa del servicio que se está prestando al contratante. Incluye el nombre de la campaña, datos de configuración y administración de la plataforma omnicanal.
4. Cliente gestionado

   Este dominio está representado por la información que es recopilada durante el contacto que se logra con un cliente secundario. Estos datos varían según la naturaleza de cada campaña, pero representan un cuerpo de información diferenciado respecto a lo que es entregado por el contratante.
5. Proveedores

   Conformado por la información de los proveedores que permiten el funcionamiento de la empresa. Incluyen datos de contacto, definiciones contractuales, financieras y otros.
6. Minería de datos

Está conformado por los datos que se obtiene mediante la minería de información obtenida de fuentes públicas. Este dominio representa una ventaja competitiva para la empresa.

7. Histórico

   Conformado por la información histórica de interacciones, incluída grabaciones en formato de onda.

8. Organización

   Conformada por toda la información inherente a la organización como datos de talento humano, financieros, inventarios, knowledge base, etc.

9. Telefonía

   Representado por la información requerida para el acceso telefónico.

En Tabla 6 - Dominios, dueño y tipo de información (parte 1) y Tabla 7 - Dominios, dueño y tipo de información (parte 2), se presenta un consolidado de lo descrito.

Dominios	Dueño	Tipo de información	Definición	Criticidad del Dominio
Cliente directo	Empresa / Dirección Financiera y Comercial	Información de entidad	Identificación de la entidad, RUC, el nombre, el contacto comercial	33,33
		Información de contrato	Detalles del contrato, financieros, etc.	
Cliente a contactar	Cliente Directo ; Administrado por Jefe de TI	Informacion general	Nombres completos e identificacion	83,33
		Información de contacto	Teléfonos, correos	
		Información de ubicación	Dirección	
		Información de árbol genealógico	Parentescos	
		Información de posición financiera	Línea de crédito	
Campañas	Jefe de TI	Información general de campaña	Detalles de la campaña, condiciones, productos	175,00
Cliente gestionado	Jefe de Operaciones	Información de gestión	Datos levantados durante la gestión como producto vendido o atención prestada	100,00
Proveedores	Director Financiero	Información de contrato y servicios	Detalles de los servicios, información financiera y de configuración	8,33

Tabla 6 - Dominios, dueño y tipo de información (parte 1)

Dominios	Dueño	Tipo de información	Definición	Criticidad del Dominio
Minería de datos	Jefe de TI	Informacion general	Nombres completos e identificación	98,61
		Información de contacto	Teléfonos, correos	
		Información de ubicación	Dirección	
		Información de árbol genealógico	Parentescos	
		Información de posición financiera	Línea de crédito	
		Información de preferencias y costumbres	Sitios visitados o históricos de compras	
Histórico	Jefe de TI	Información de contactos previos	Como fecha, número de contacto, quien atiende, etc.	91,67
		Grabaciones	Grabaciones de onda de las conversaciones	
Organización	Direcciones	Financiera	Libros de contabilidad, datos bancarios, responsabilidades de sueldos, Incentivos, bonificacions y comisiones	21,67
		RRHH	Nómina de trabajadores	
		Inventarios	Detalles de los assets	
		Knowledge Base	Preguntas frecuentes, almacenadas en el sistema de base de conocimiento	
		Cámaras	Grabaciones de video de circuito cerrado	
Telefonia	Jefe de IT	Telefonía	Información de configuración	233,33

Tabla 7 - Dominios, dueño y tipo de información (parte 2)

1.4.3. Anexos

- Anexo 4 – Clasificación de la información y determinación del riesgo (Att004 - Instrumentos.xlsx ; hoja “2-AnalImpact-Dominios-TiposInfo”)

1.5. Fase 3 – Inventarios de activos de información

1.5.1. Metodología

Para esta fase, se efectúa un inventario de activos tecnológicos físicos (servidores, switches, firewalls, access points), con los que cuenta la empresa, la cual al ser bastante pequeña, solo utiliza pocos equipos.

Los activos de información se mapearon directamente con el hardware que los soporta, bien sea en su transmisión, hospedaje o tratamiento.

El nivel de criticidad de cada activo físico fue evaluado según el impacto que tendrá a la empresa en caso de que surja un evento que afecte la confidencialidad, integridad y/o disponibilidad de los recursos de información que soporta; se utiliza una escala del 0 al 100, siendo 100 el de mayor criticidad.

1.5.2. Resultados

Para la empresa se evidencia que toda su infraestructura tecnológica está centrada en un servidor que hospeda todos los activos de información con los que trabaja la organización.

Se cuenta con equipos de soporte para la transmisión de datos (2 switches de 24 puertos) y un firewall; adicionalmente un router perteneciente a la operadora telefónica provee el servicio de troncal SIP (Session Initiation Protocol).

Para el acceso inalámbrico, existen 3 access points conectados a la red que se utilizan como puente a un enlace dedicado de internet.

Los activos físicos seleccionados para este estudio son aquellos que representan la mayor criticidad para la empresa, constituídos por el único servidor de la organización y el router proveedor del servicio de telefonía.

1.5.3. Anexos

- Anexo 5 – Hoja de cálculo con el inventario de activos físicos de la empresa (Att004 - Instrumentos.xlsx ; hoja “2.1-InventarioDeActivos”)

1.6. Fase 4 – Análisis de amenazas y vulnerabilidades de activos de información críticos

1.6.1. Metodología

Teniendo el listado enumerado de los activos físicos, se procede a analizar las amenazas a las que se encuentran expuestos. Para ello, se utiliza la “Metodología de Análisis y Gestión de Riesgos de Sistemas de Información”, MAGERIT versión 3.0 (Ministerio de Hacienda y Administraciones Públicas, 2012), cuyo objetivo es facilitar la labor de las personas que ejecutan un proyecto de seguridad, ofreciendo ítems estandares de referencia, y homogeneizando los resultados de análisis.

Cada ítem de amenaza fue etiquetado con la letra “A” seguido de un número único. Adicionalmente, se asigna un valor de probabilidad de 0% a 100% y de impacto entre 1 y 4. Las magnitudes se determinaron mediante una apreciación cualitativa, elaborada en conjunto con la dirección de la organización; se determina el nivel de riesgo, relacionando la probabilidad con el impacto, mediante la usual fórmula (*probabilidad x impacto*).

Utilizando como referencia los controles en el anexo A de la norma ISO 27001:2013 (International Organization for Standardization, 2013), se determinan las vulnerabilidades que podrían materializar las amenazas; de la misma manera, se determina el control que será aplicado para mitigar el riesgo.

1.6.2. Resultados

Para efectos del servidor, se observa que las amenazas con mayor riesgo son:

1. Avería de origen físico o lógico (A2)
2. Corte del suministro eléctrico (A3)
3. Fallo de servicios de comunicaciones (A5)
4. Degradación de los soportes de almacenamiento de la información (A6)
5. Caída del sistema por agotamiento de recursos (A19)

Mientras que las amenazas que constituyen un riesgo importante para el router del servicio de telefonía son:

1. Avería de origen físico o lógico (A2)
2. Corte del suministro eléctrico (A3)
3. Fallo de servicios de comunicaciones (A5)

Las vulnerabilidades relacionadas con esta amenazas son las siguientes:

1. Mala instalación de equipos (V1)
2. Insuficiente mantenimiento de equipos (V3)
3. Falta de planes de mantenimiento (V4)
4. Espacio físico inadecuado para los equipos (V5)
5. Falta de seguimiento de condiciones ambientales (V6)
6. Falta de SLA's para servicios subcontratados (V7)

7. Ausencia de redundancia del servicio (V8)
8. Falta de seguimiento de salud de los dispositivos (V9)
9. Falta de restricciones en instalación de software (V18)

Tomando como referencia los controles hallados en el Anexo A de la norma ISO 27001:2013, se seleccionan aquellos más relevantes que se encuentran relacionados con las vulnerabilidades correspondientes, los cuales se resumen en Tabla 8 - Resumen de controles seleccionados.

Resumen de controles seleccionados

Control	Grupo	Descripción
A.11.2.2	Elementos de Soporte	Los equipos deben ser protegidos contra fallas eléctricas y otras interrupciones causadas por elementos de soporte.
A.11.2.4	Mantenimiento de equipos	Los equipos deben ser mantenidos correctamente para asegurar su disponibilidad contínua e integridad.
A.12.3.1	Copias de Seguridad	Copias de seguridad de datos, software e imágenes de sistemas deben ser capturadas y probadas regularmente de acuerdo a una política de copias de seguridad.
A.13.1.1	Controles de Red	Las redes deben ser administradas y controladas para proteger la información en los sistemas y aplicativos
A.13.1.2	Seguridad de servicios de red	Los requisitos de mecanismos de seguridad, niveles de servicio y administración, de todos los servicios de red, deben ser identificados e incluidos en los acuerdos de servicios, sean estos provistos in-house o outsourced.
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben ser implementadas con redundancia suficiente para cumplir con los requerimientos de disponibilidad.

Tabla 8 - Resumen de controles seleccionados

Estudio de controles existentes

En la empresa se lograron identificar algunos controles que ya se implementaban previamente. Para estudiarlas se generó un instrumento que permite medirles en función a su autonomía (Manual, SemiAutomático y Automático) y tipo (Preventivo, Detectivo, Correctivo).

Se asigna un valor numérico en el rango de 1 a 3, siendo este último el de mejor desempeño. La suma de ambas magnitudes representan la evaluación del control.

Valor	Autonomía
1	Manual
2	SemiAutomático
3	Automático

Valor	Tipo
1	Correctivo
2	Detectivo
3	Preventivo

Tabla 9 - Clasificación de controles

Resultado de controles existentes

En los resultados se observa que la mayoría de los controles son de autonomía manual y de tipo preventivo, otorgándoles una evaluación de magnitud 4.

El riesgo residual se determina en reunión con los directivos de la empresa, quienes en conjunto con el personal de sistemas, asignaron los valores determinantes del riesgo residual.

A pesar que el instrumento pone evidencia que los controles sí disminuyen considerablemente el riesgo (ver anexo 6 – instrumento analisis de riesgo y heatmap), se recomienda establecer controles que sean automáticos para incrementar la efectividad de los mismos.

Adicionalmente, se puede observar que algunas amenazas no cuenta con controles para mitigar su riesgo, por lo tanto se recomienda establecer nuevos controles que permitan cubrirlos.

1.6.3. Anexos

- Anexo 6 – Instrumento análisis de riesgo y heatmap (Att004 - Instrumentos.xlsx ; hojas “3-Amenazas(RiesgoInherente)-Srv” y “3-Amenazas(RiesgoInherente)-Tel”)

1.7. Fase 5 – Documentos claves del SGSI

1.7.1. Metodología

Política de alto nivel

Se desarrolla el documento de política de alto nivel para la empresa, el cual define los roles y responsabilidades. (Ver anexo 7 – Políticas de alto nivel).

Esta política está basada en el “Formato de Referencia de Políticas de Seguridad de la Información” del Esquema Gubernamental de Seguridad de la Información (Ministerio de Telecomunicaciones, 2020), el cual consiste de la siguiente estructura:

- Antecedentes
  Pretende definir el por qué de la creación de la política, indicando los riesgos de no contar con una definición de la misma.
- Descripción de la política
  Describe la política que será implementada, cuál es su intención en la regulación de la seguridad de la información.
- Objetivo
  Detalla los objetivos principales de la política, incluyendo las reglas que deben seguirse para cumplir con estos.
- Roles y responsabilidades
  Enumera los cargos que serán responsables del cumplimiento de la política y detalla los roles que ejecuta cada uno de ellos.
- Alcance y usuarios
  Describe los usuarios a los que se aplicará la política de seguridad, delimitando claramente el alcance que se tendrá.
- Comunicación de la política
  Establece los mecanismos que serán utilizados para comunicar la política de una manera efectiva a los componentes de la organización.

- Documentos de Referencia
  Compendio de documentos que han sido utilizados como referencia para la elaboración de la política
- Terminología
  Glosario de términos utilizados a lo largo de la política

Plan de acción para la aplicación de controles

Basados en el anexo A de la norma ISO 27001, se redacta el documento de aplicabilidad para los controles que en él figuran (ver Anexo 8 – Declaración de aplicabilidad, ISO 27001, Controles).

1.7.2. Resultados

Como resultado de esta fase, se elaboran los documentos “Políticas de alto nivel” (anexo 7) y “Declaración de aplicabilidad, ISO 27001, Controles” (anexo 8).

1.7.3. Anexos

- Anexo 7 – Políticas de alto nivel (Att005 - Politica Alto Nivel.docx)
- Anexo 8 – Declaración de aplicabilidad, ISO 27001, Controles. (Att006 - Iso27001 StatementOfApplicability.xlsx)

2. Conclusiones y Recomendaciones

La empresa NM empieza como una organización pequeña de emprendedores, con pocos recursos y negocios limitados. Sin embargo, ha crecido paulatinamente y en este momento maneja una gran cantidad de información.

Con el crecimiento se introducen cada vez más variables que juegan un papel importante en temas de seguridad, como mayor personal y su riesgo inherente, manejo de información con requerimientos legales más estrictos, mayor volumen operativo, etc.

Como la empresa no se ha desarrollado con cimientos sólidos en seguridad, toda la aplicación ha estado basada en conocimientos empíricos, sin estructura metodológica.

Aplicar este SGSI permitirá a la empresa tener un marco de trabajo que le habilitará la posibilidad de seguir desarrollándose sin dejar de lado la seguridad de la información.

El SGSI presentado en este trabajo está limitado a solo dos activos de información críticos para la empresa. No obstante, se espera que la organización siga incrementando sus actividades y por lo tanto incorporando mayor cantidad de activos.

Es recomendable mantener actualizado el SGSI para cubrir aquellos activos menos importantes que fueron omitidos en este estudio e incluir nuevos procedimientos o características funcionales de la organización.

De la misma manera, se recomienda establecer las políticas necesarias que se ajusten a la empresa, ya que durante la aplicación de este estudio, se pueden observar falencias que dejan sin atención otros puntos cruciales para la empresa.

Adicionalmente, es importante mantener actualizado los activos de información debido a la naturaleza cambiante del giro de negocio, manteniendo así al SGSI al día con la transformación de la organización.

3. Referencias

International Organization for Standardization. (2013). Information Security Management.

John R., V. (2017). *Computer and Information Security Handbook.* Morgan Kaufmann.

Ministerio de Hacienda y Administraciones Públicas. (2012, Octubre). MAGERIT - Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. *Libro II - Catálogo de Elementos*. Madrid, España.

Ministerio de Telecomunicaciones. (2020, 03). *Formato referencial para la elaboración de la política de seguridad de la información (EGSI)*. Tomado de Gobierno Electrónico: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/03/Formato-Referencial_Pol%C3%ADtica-de-Seguridad-de-la-Informaci%C3%B3n-EGSI.pdf

Rookes, P., & Willson, J. (2005). *Perception: Theory, Development and Organisation.* Routledge. doi:10.4324/9780203977408