




“Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Orientado a los medios de comunicación”

“Analysis phase for the implementation of an Information Security Management System (I.S.M.S.) based on ISO 27001. Oriented to the media”

- ¹ Esteban Fernando Castillo Durán  <https://orcid.org/0009-0007-4302-1708>
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
esfecasdu@gmail.com
- ² Fernando Illescas Peña  <https://orcid.org/0000-0001-9316-1118>
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
fernan.illescas@hotmail.com
- ³ Andrés Sebastián Quevedo Sacoto  <https://orcid.org/0000-0001-5585-0270>
Maestría en Ciberseguridad, Universidad Católica de Cuenca, Cuenca, Ecuador.
asquevedos@ucacue.edu.ec

Artículo de Investigación Científica y Tecnológica

Enviado: 16/07/2023

Revisado: 08/08/2023

Aceptado: 05/09/2023

Publicado: 13/10/2023

DOI: <https://doi.org/10.33262/concienciadigital.v6i4.1.2725>

Cítese:

Castillo Durán, E. F., Fernando Illescas Peña, F., & Quevedo Sacoto, A. S. (2023). Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Orientado a los medios de comunicación. *ConcienciaDigital*, 6(4.1), 6-25. <https://doi.org/10.33262/concienciadigital.v6i4.1.2725>



Ciencia Digital
Editorial



CONCIENCIA DIGITAL, es una revista multidisciplinar, **trimestral**, que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. <https://concienciadigital.org>

La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Esta revista está protegida bajo una licencia Creative Commons Attribution Non Commercial No Derivatives 4.0 International. Copia de la licencia: <http://creativecommons.org/licenses/by-nc-nd/4.0/>

**Palabras
claves:**

S.G.S.I. ISO
27001; Modelo
de madurez;
Activos de
información;
Análisis de
riesgos.

Resumen

Introducción: La falta de un plan de gestión de Seguridad de la Información S.I. en la mayoría de las empresas, sumado al desconocimiento de la importancia que tiene una adecuada gestión en seguridad de la información (S.I.) representa un problema para las organizaciones. **Objetivo:** A través de este estudio ofrecer una guía que permita a la directiva mejorar notablemente el nivel de seguridad que posee la empresa. **Metodología:** Se ha optado por la utilización de los controles propuestos por el estándar ISO 27001, adoptando el marco de trabajo propuesto por MAGERIT para el análisis y para los controles basado en MITRE. **Resultados:** El estudio inicial proporcionó los valores preliminares de la situación actual de la empresa y se pudo deducir que el nivel de madurez en S.I. es deficiente, se detalló en el informe dirigido a gerencia con las recomendaciones sugeridas para la mitigación de los riesgos derivados del análisis realizado. **Conclusión.** Quedó evidenciada la necesidad de contar con un plan de gestión de S.I. que comprenda todas las políticas necesarias para garantizar que el nivel de madurez de la empresa se ajuste a los estándares establecidos en la ISO 27001. **Área de estudio general:** Tecnologías de la información. **Área de estudio específica:** Ciberseguridad.

Keywords:

S.G.S.I. ISO
27001;
Maturity
Model
Information
assets Risk
assessment

Abstract

Introduction: The lack of an IS Information Security management plan. In the majority of companies, added to the lack of knowledge of the importance of adequate information security management (IS), it represents a problem for organizations. **Objective:** Through this study, offer a guide that allows management to significantly improve the level of security that the company has. **Methodology:** It has been decided to use the controls proposed by the ISO 27001 standard, adopting the framework proposed by MAGERIT for the analysis and controls based on MITER. **Results:** The initial study provided preliminary values of the current situation of the company with which, we can deduce that the level of maturity in I.S. is deficient, this was detailed in the report addressed to management along with the suggested recommendations for mitigating the risks. **Conclusion.** The need to have a I.S. management plan was evident. that understands all the necessary policies to ensure that the

company's maturity level conforms to the standards established in ISO 27001.

Introducción

El presente documento comprende el estudio realizado en la empresa “*Medio de comunicación de la ciudad de Cuenca*” (*El nombre de la empresa en la cual se realizó este estudio, ha sido omitido en este documento por razones de confidencialidad, y será referido de esta manera*), el cual abarca la fase inicial de planificación para la implementación de un sistema de gestión de seguridad de la información (S.G.S.I.), y sirve como base a la directiva de la empresa para su posterior implementación, este proceso se ha realizado bajo el estricto cumplimiento de las actividades comprendidas dentro de la norma ISO 27001 y sus familias derivadas.

La realidad latinoamericana en temas de ciberseguridad refleja un déficit muy alto en comparación con otras regiones a nivel global, concretamente en el caso del Ecuador, el tema de los ciberataques es constante, tal como se detalla en investigaciones previamente realizadas Agencia AFP (2019); Ortiz (2021), y de esta premisa nace la necesidad a nivel empresarial de protegerse contra este tipo de amenazas, otra investigación reveló que aproximadamente en el país se reportan un promedio de 10.000 denuncias de delitos informáticos anualmente Salcedo (2021).

Según manifiesta Moran Maldonado (2021) el sector empresarial en la ciudad de Cuenca, no es la excepción y es difícil poder estimar la cantidad de ataques diarios a las empresas ya que esto depende primero del ámbito, del tamaño de la misma, de su infraestructura entre otros parámetros que definen el riesgo potencial al cual se encuentran expuestas.

Metodología

En el artículo de Arévalo et al. (2017), detalla que existen varias metodologías que nos permiten realizar la evaluación de riesgos, las cuales pueden ser aplicables, dependiendo de las características que posee cada empresa, y a partir de esta poder realizar todo el proceso del análisis, la evaluación y posteriormente poder ofrecer los resultados deseados como producto final, la implementación de un Sistema de Gestión de Seguridad de la

Información (SGSI) posee su propio cronograma de actividades y requiere también definir un presupuesto basado en el cálculo de costos de los elementos necesarios (hardware, software, capacitación, etc) el mismo que forma parte de otro informe técnico.

Los pasos comprendidos en este estudio, fueron definidos mediante un cronograma desarrollado en un lapso de seis meses, iniciado en enero de 2023, con el fin de dar cumplimiento a todas las actividades que se están planificadas, se ha utilizado principalmente la metodología MAGERIT, ya que como lo señala en su documento Avila-Torres (2021) es apropiada para este tipo de estudios.

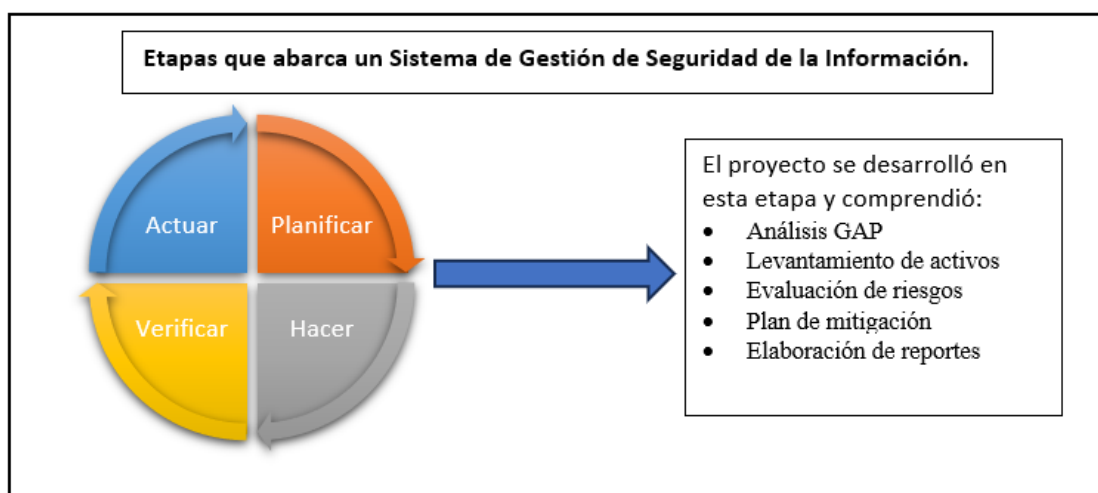
- **Primer paso.** El objetivo inicial fue recopilar la documentación necesaria y comprende los permisos requeridos por parte de la directiva de la compañía para la ejecución del proyecto, (realizado en enero 2023).
- **Segundo paso.** En la siguiente fase se procedió con la ejecución de un análisis GAP mediante el cual se define el punto de partida del proyecto, el mismo que constatará la situación actual de la empresa en materia de S.I. basado en la metodología MAGERIT v3 (realizado durante febrero 2023).
- **Tercer paso.** Posteriormente se evaluó el nivel conocimiento del personal de diferentes áreas de la empresa acerca de temas de seguridad de la información, se optó por un análisis cuantitativo, el cual permite obtener los resultados y posteriormente analizarlos, a través de un formulario de tipo cuestionario (proceso realizado en marzo 2023).
- **Cuarto paso.** Se realizó el levantamiento de activos de información, para identificar de entre todos, cuáles de ellos son considerados críticos, y clasificarlos según su importancia, basado también en la metodología MAGERIT v3 (realizado en marzo 2023).
- **Quinto paso.** A continuación, se realizó la evaluación de los riesgos, que es uno de los procesos medulares de este proyecto, ya que permitió identificar las amenazas y los riesgos a los cuales están expuestos los activos de información y el impacto dentro de la estructura de la empresa (realizado en abril 2023).
- **Sexto paso.** Se procedió a analizar las vulnerabilidades con la finalidad de identificar posibles puntos de ataque, se definió una matriz que clasifica los

resultados en función de su criticidad, y así se determinó la prioridad de cada uno (realizado en mayo 2023).

- **Séptimo paso.** Se revisaron los resultados de los procesos realizados, con lo cual se tendrá una idea clara de las posibles soluciones a implementarse (realizado durante junio 2023).
- **Octavo paso.** Se procedió a elaborar un plan de mitigación de riesgos, aplicando los controles indicados en la norma ISO 27001 sobre aquellos dominios que presentaron valores nulos durante la ejecución del análisis GAP (realizado durante junio 2023).
- **Noveno y último paso.** La etapa final consistió en la elaboración del documento final entregable para la directiva, consta de dos reportes: el primero es el informe ejecutivo, el cual contiene los resultados del estudio explicados de una manera fácil de entender para los directivos, detallando las conclusiones y recomendaciones a implementarse, el segundo documento es el informe técnico que contiene un registro detallado de todas las actividades desarrolladas, y resultados obtenidos de cada una de las mismas (realizado en julio 2023).

Figura 1

Delimitando el alcance del proyecto



Nota: Dentro del ciclo de vida de un S.G.S.I, el proyecto se enfoca en la primera etapa.

Resultados

Modelo de madurez inicial

Se planteó realizar un análisis de brechas (Análisis GAP) preliminar que sirvió como punto de partida para todo el proyecto y posteriormente de acuerdo con el cronograma de actividades definido previamente, se ejecutaron las tareas correspondientes a los siguientes pasos comprendidos en la fase de planificación de acuerdo a los parámetros establecidos en la norma ISO 27001.

Se utilizó la matriz planteada en la ISO 27002 conocida también como Anexo A de la ISO 27001, la cual presenta un formulario de preguntas que comprenden los dominios desde el A5 hasta el A18 y sus respectivos subdominios, comprende: el análisis diferencial, el cuestionario GAP, los controles, la matriz de responsabilidades; los resultados obtenidos indican un valor muy bajo, esto era predecible ya que, no existe un estudio previo, ni políticas o controles establecidos en la mayoría de los dominios analizados, la Figura siguiente refleja gráficamente los resultados obtenidos.

Figura 2

Resultados del modelo de madurez inicial



Nota: Representación gráfica de los valores obtenidos al aplicar los controles de la ISO27001.

En el siguiente paso se realizó una comparación en función del Modelo de Madurez de la Capacidad de Ciberseguridad (CMM), el cual según indica Revista Seguridad360 (2022) define las 5 etapas de madurez basándose en una escala de valores de 1 al 5 detallada de la siguiente forma:

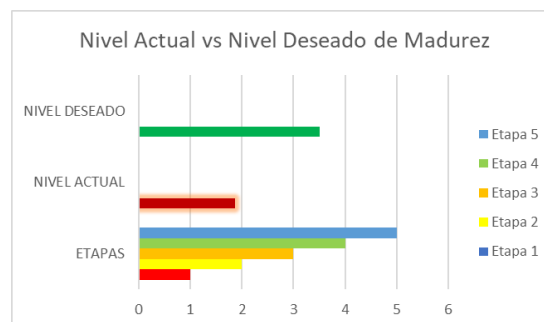
1. **Inicial.** En la cual no existen ni controles, ni políticas.
2. **Formativa.** Los controles o políticas son muy básicos o no se encuentran claramente detallados.
3. **Consolidada.** Los controles y las políticas se encuentran definidos e implementados.
4. **Estratégica.** Refleja la toma de decisiones de los indicadores considerados clave para la empresa y su evolución.
5. **Dinámica.** Existen políticas y procedimientos para alterar las estrategias a seguir dependiendo de las capacidades y los intereses de la empresa, la toma de decisiones y asignación de recursos son clave en esta etapa.

Escenario actual versus escenario deseado

De acuerdo a esta escala de valores, podemos determinar que la empresa se encuentra en un punto entre la etapa 1 y la etapa 2 (1.8), ya que, en algunos aspectos no posee madurez de manera generalizada, existen otros en los cuales hay controles y procesos con un nivel de cumplimiento, los resultados se muestran en la siguiente Figura.

Figura 3

Nivel de Madurez (actual vs. deseado)



Nota: Comparativa entre de los valores obtenidos del nivel de madurez actual y deseado.

Inventario de activos de información

La metodología empleada para la clasificación de los activos fue MAGERIT v3, ya que con ella se puede clasificar de una manera clara y simplificada los diferentes tipos de activos de tal manera que la información pueda tabularse ordenadamente dentro de una matriz, se procedió a llenar la matriz en Excel y se obtuvieron los siguientes resultados:

Tabla 1
Activos de información de la empresa

Total Activos:	32
Total Activos (ALTO):	13
Total Activos (MEDIO):	10
Total Activos (BAJO):	9

Nota: Total de los activos de información inventariados.

Selección de los activos críticos

Luego de obtener la matriz de los activos, procedemos a determinar de entre todos ellos cuales son considerados activos críticos, se los clasificó utilizando la metodología MAGERIT de la siguiente manera: valores de 0 a 1.9 son considerados como importancia “**BAJO**”, valores de 2 a 2.5 su importancia se etiquetó como “**MEDIO**”, y valores de 2.6 a 3 son considerados como “**ALTO**”, estos valores se encuentran en la columna denominada “**Importancia A.I.**” de la matriz general de activos, y se obtuvo una tabla con 13 activos y la podemos ver a continuación.

Tabla 2
Activos críticos

Activo	Tipo
Centro de Datos	Instalaciones
Servidor de aplicaciones	Equipos Informáticos
Servidor Web	Equipos Informáticos
Servidor de correo Institucional	Equipos Informáticos
Base de Datos Aplicaciones	Datos o Información
Base de Datos Suscriptores	Datos o Información
Firewall	Redes de Comunicación
Servidor para Pre Prensa	Equipos Informáticos
Equipo CTP (Copiado Directo a Plancha)	Equipos Informáticos

Sistema de gestión empresarial E.M.	Aplicaciones de Software
Agencia Centro	Instalaciones
Agencia El Vergel	Instalaciones
Agencia El Arenal	Instalaciones
Total Activos Críticos:	13
Activos tipo Instalaciones:	4
Activos tipo Equipos Informáticos:	5
Activos tipo Datos o Información:	2
Activos tipo Redes de Comunicación:	1
Activos tipo Aplicaciones de Software:	1

Nota: Detalle de activos críticos.

Riesgos y Amenazas

Partiendo del hecho que un riesgo es la exposición a una circunstancia adversa que debemos afrontar, en este caso enfocado a los activos de información de la empresa; es necesario para este caso de estudio, determinar el grado de exposición al cual están expuestos los activos analizados de tal manera que posteriormente se pueda elaborar un plan para su mitigación y de esta manera protegerlos de una manera más adecuada y se muestran a continuación.

Tabla 3

Matriz de identificación de riesgos

Causa	Riesgo o Amenaza
Desastres naturales y/o provocados	Terremotos, inundaciones, guerras, manifestaciones, pandemias,
Eventos externos a la empresa	Falla de proveedores de servicios (energía eléctrica, ISP, servicios básicos), falla de proveedores de suministros (materia prima, bobinas, tinta, planchas, etc.) ataques externos.
Eventos internos	Problemas técnicos en la infraestructura de la empresa, fallas en el proceso de producción, ataques internos, fallas de seguridad.
Acciones fortuitas y/o deliberadas	Errores humanos, fallos de hardware, fallos de software, fallos en los equipos de oficina, incendios,
Acciones humanas	Personal con problemas laborales pueden ocasionar accesos no autorizados, robo de información, fuga de datos.

Nota: Identificación de riesgos.

Matriz de probabilidad.

Según la propuesta de MAGERIT, a continuación, se debe realizar la matriz que permita identificar la probabilidad que los riesgos puedan ocurrir, para ello se han detallado 5 niveles que son:

- **Improbable:** indica una probabilidad casi nula que un riesgo pueda ocurrir.
- **Posible:** indica que es muy poco probable que un determinado riesgo pueda ocurrir.
- **Ocasional:** indica que el riesgo puede materializarse en cualquier momento.
- **Probable:** un riesgo tiene una probabilidad alta que pueda ocurrir.
- **Frecuente:** el riesgo se presenta con una frecuencia muy alta.

Tabla 4

Matriz de valores de probabilidad

Probabilidad	Valor Asignado
Improbable	1
Posible	2
Ocasional	3
Probable	4
Frecuente	5

Nota: Valores asignados en reuniones con la directiva de la empresa.

Matriz de impacto

De la misma manera que la anterior, esta matriz se encuentra elaborada en base a la misma metodología MAGERIT, y a diferencia de la anterior, ésta indica el impacto que representa para la empresa si un riesgo llegara a materializarse, afectando directamente a la continuidad del negocio, y los niveles especificados son los siguientes:

- **Insignificante:** El impacto de la materialización de un riesgo no representa problema para la empresa.
- **Menor:** La ocurrencia de un riesgo representa un impacto mínimo para la empresa.
- **Moderado:** Un riesgo materializado representa un impacto momentáneo pero considerable para la empresa.

- **Mayor:** La materialización de un riesgo representa un impacto alto tanto en la cadena de producción de la empresa, lo cual se deriva en pérdidas económicas importantes.
- **Catastrófico:** Un riesgo identificado en este nivel, representa un impacto del nivel más alto en términos de continuidad del negocio, y la cadena de producción del mismo, dejándolo parcial o completamente paralizado, y de la misma manera produciendo la mayor pérdida posible para la empresa.

Tabla 5*Matriz de valores de impacto*

Impacto	Valor asignado
Insignificante	1
Menor	2
Moderado	3
Mayor	4
Catastrófico	5

Nota: Valores asignados en reuniones con la directiva de la empresa.

Riesgo inherente

Este concepto hace referencia a todo riesgo que se encuentra intrínsecamente en los procesos y tareas, se encuentra presente cuando no se han tomado las medidas necesarias que permitan minimizar tanto la probabilidad como el impacto de los riesgos identificados, por tanto no puede ser eliminado, es necesario darle un valor numérico para poder tabular los resultados para el conjunto de valores definidos tanto para la probabilidad como para el impacto, así pues, para la probabilidad tenemos la siguiente distribución:

La matriz para este caso se representa en la siguiente tabla y sus respectivos valores fueron proporcionados por la directiva, la cual determinó dichos valores en función de su criterio de acuerdo con la realidad de la empresa:

Tabla 6

Matriz de riesgo inherente

Matriz de Riesgos		
Riesgo	Probabilidad	Impacto
1. Desastres Naturales y/o provocados.	Posible	Catastrófico
2. Eventos externos.	Ocasional	Mayor
3. Eventos internos.	Posible	Mayor
4. Acciones fortuitas	Ocasional	Moderado
5. Acciones humanas	Posible	Mayor

Nota: Valores asignados en reuniones con la directiva de la empresa.

Los valores del riesgo inherente son el resultado de la multiplicación del valor de la probabilidad por el impacto, y quedan definidos de la siguiente manera:

Tabla 7

Cálculo del riesgo inherente

Riesgo Inherente	
Riesgo 1	2x5=10
Riesgo 2	3x4=12
Riesgo 3	2x4=8
Riesgo 4	3x3=9
Riesgo 5	2x4=8

Nota: Los valores fueron expuestos a la directiva.

A partir de estos datos, se deriva la matriz comparativa que representa la relación entre probabilidad e impacto, quedando distribuida de la siguiente manera en el mapa de calor.

Mapa de calor

Derivado de los riesgos inherentes, se presenta a continuación la matriz de calor sobre la cual se analizan los riesgos y su ubicación dentro de la misma, a fin de comprender mejor cuáles son aquellos sobre los cuales se debe tomar mayor atención.

Tabla 8

Mapa de calor

FRECUENCIA		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Frecuente						
Probable						
Ocasional				Riesgo 4.	Riesgo 2.	
Posible					Riesgos 3. – 5.	Riesgo 1.
Improbable						

Nota: Representación gráfica del nivel de criticidad de los riesgos detectados.

Vulnerabilidades

Para el análisis realizado en este punto, se tomó como base los datos obtenidos de la encuesta realizada al personal de T.I. dentro de la empresa, perteneciente al departamento de Sistemas, mediante la cual permitió conocer entre otros datos la manera en que está implementada la red, las versiones de software instaladas en los activos, tales como servidores, equipos de los diferentes departamentos, etc. con la finalidad de determinar las vulnerabilidades a las cuales se encuentran expuestos.

Se procedió a realizar una encuesta al jefe del departamento de sistemas de la empresa, y con la información proporcionada, se llenó la siguiente matriz.

Tabla 9

Encuesta al jefe del departamento de sistemas

¿Existe un manual de procesos interno en el departamento?	SI	NO
¿existe distribución de funciones en el departamento?	SI	NO
¿se entregan reportes de actividades a la directiva?	SI	NO
¿existe documentación sobre los requerimientos realizados por los otros departamentos?	SI	NO
¿existe un inventario de activos de información?	SI	NO
¿existen procesos de control de acceso de los usuarios?	SI	NO
¿está actualizado? (si existe)	SI	NO
¿está documentado? (si existe)	SI	NO
¿existen políticas de mantenimiento y control de la infraestructura de red?	SI	NO
¿existen políticas de mantenimiento y control de los equipos informáticos?	SI	NO
¿existen revisiones periódicas sobre las versiones de los sistemas implementados en los distintos departamentos de la empresa?	SI	NO
¿se realizan copias de seguridad periódicamente de la información crítica del negocio?	SI	NO
¿existen políticas que detallen los procesos de desarrollo de aplicaciones?	SI	NO
El acceso externo (terceros) tanto a la red, como a los sistemas de la empresa, ¿es monitoreado?	SI	NO
¿considera que la infraestructura de la empresa está preparada en caso de que un incidente de ciberseguridad ocurra?	SI	NO
¿existe algún plan de contingencia en caso de que un ataque informático llegue a afectar la infraestructura de la empresa?	SI	NO

¿se encuentran los sistemas informáticos de la empresa preparados para implementar los requerimientos detallados en la ley de protección de datos personales?	SI	NO
---	----	----

Nota: Las preguntas realizadas, fueron revisadas y aprobadas por la directiva en reunión previa.

La información recopilada permitió determinar las vulnerabilidades, siguiendo con la metodología MAGERIT, pasan a ser catalogadas en tres niveles: Alto, Medio, Bajo en función de la relevancia que tiene su mitigación para que no afecte a la continuidad del negocio, la siguiente tabla muestra los valores de las vulnerabilidades detectadas.

Tabla 10

Vulnerabilidades encontradas

Vulnerabilidad	Categoría
Inventario de activos de información (A.I.) desactualizado.	Medio
No existe control de acceso a usuarios.	Alto
Mantenimiento de infraestructura de red tercerizado.	Medio
No hay monitoreo de actividad de usuarios ni de terceros.	Alto
No se cuenta con plan de contingencia en caso de incidentes	Alto
Servidores con sistemas operativos desactualizados	Medio
No contar con servicio de ISP de contingencia	Alto
No existen reportes a gerencia, de incidentes o actividades	Medio
Equipos de usuarios con sistemas operativos y software antiguos	Medio
No existen políticas de responsabilidad de usuario	Alto
Posible fuga de información	Alto
No existe segmentación de red	Alto
No hay un correcto manejo de credenciales por parte del personal	Medio

Nota: Matriz de valores otorgadas a las vulnerabilidades detectadas.

Plan de tratamiento de riesgos, orientado a un medio de comunicación

Es necesario que el proceso se complemente con un plan adecuado que permita el correcto tratamiento de los riesgos a fin de mitigar el impacto que éstos producen, de tal manera que el riesgo residual se reduzca drásticamente.

Esta propuesta de plan se encuentra fundamentada en los controles indicados por la ISO27001 en el Anexo A de la norma, que es sobre la cual se ha trabajado a lo largo de este proyecto, y por lo tanto el cumplimiento obligatorio de la misma va de la mano con los objetivos determinados inicialmente, definiendo claramente los responsables para garantizar el cumplimiento de los mismos, toda esta información se encuentra detallada en la tabla a continuación:

Tabla 11
Controles a aplicarse

Cláusula	Controles	Responsable
A.5.1.1	Establecer políticas para S.I. que regirán en la empresa.	Gerente General.
A.5.1.2	Revisar las políticas establecidas	Gerente General.
A.6.1.3	Establecer reglas de gestión de roles, tareas, comunicación con la directiva	Jefe Talento Humano.
A.7.2.2	Realizar programas de capacitación tanto a personal como contratistas sobre las políticas de S.I. implementadas por la empresa.	Jefe Talento Humano.
A.7.2.3	Socializar con el personal y contratistas los procesos disciplinarios establecidos por la empresa, con la finalidad que todos los conozcan perfectamente.	Gerente General.
A.8.1.1	Actualizar el inventario de A.I. periódicamente o cada vez que se realiza la adquisición de un nuevo activo.	Jefe Sistemas.
A.8.1.2	Documentar los propietarios de cada activo que conste en el inventario.	Gerente Financiero.
A.8.1.3	Establecer las reglas de uso para cada uno de los activos, de tal manera que se garantice que los usuarios no den un mal uso a los recursos disponibles en cada activo.	Gerente Financiero.
A.9.2	Definir un esquema de control de acceso a cada recurso por parte del personal, en el cual se incluya los permisos que tiene cada uno a los diferentes recursos con los cuales desarrollan sus actividades.	Jefe Sistemas.
A.9.3	Establecer una regla para la que los usuarios gestionen correctamente sus credenciales de acceso a los sistemas	Jefe Sistemas.
A.10.1	Definir un algoritmo de encriptación de datos que sea robusto, así como la custodia de las llaves públicas y privadas generadas para su uso.	Jefe Sistemas.
A.11.2.8	Establecer responsabilidades al personal, sobre la correcta protección de sus equipos al ausentarse o dejarlos desatendidos.	Jefe Talento Humano.
A.11.2.9	Adoptar políticas de escritorios y pantallas limpias y socializar su importancia con todo el personal.	Jefe Talento Humano.
A.12.4	Realizar un control y monitoreo sobre los logs de eventos generados por los sistemas de la empresa con la finalidad de establecer responsabilidades en caso de incidentes y poder entregar reportes a la directiva.	Jefe Sistemas.
A.12.6	Documentar las vulnerabilidades presentadas a partir de los incidentes suscitados, para tener una bitácora y poder a partir de estos datos, ejecutar acciones de mitigación.	Jefe Sistemas.
A.12.7	Definir un calendario para la ejecución de las auditorías, preferentemente fuera de horarios laborales a fin de evitar retrasos en la cadena de producción.	Jefe Sistemas.
A.13.1.3	Planificar y ejecutar un proceso de segregación de redes ya que es muy riesgoso que toda la infraestructura esté expuesta en una sola red global	Jefe Sistemas.
A.14.2	Definir una política que garantice el desarrollo seguro de aplicaciones ya sean elaboradas internamente o tercerizadas, acompañado de cláusulas en los contratos de adquisición que garanticen el cumplimiento de la gestión de S.I. en su desarrollo.	Jefe Sistemas.
A.16.1.1	Dentro de las políticas de S.I. definidas por la empresa, es necesario detallar el control de los incidentes, definiendo claramente, responsabilidades y acciones realizadas luego de ocurrido un incidente.	Gerente General.

A.17.1.2	Establecer procedimientos necesarios para garantizar la continuidad de los procesos en caso de presentarse un incidente de seguridad poder evaluarlos mediante simulaciones y verificar su utilidad.	Jefe Sistemas.
A.18.2	Realizar una verificación del cumplimiento de las políticas de S.I. establecidas por la empresa	Gerente General.

Nota: Controles y responsables de sus ejecuciones fueron revisados por la directiva.

Tiempos estipulados

En caso de la directiva apruebe la ejecución del plan propuesto, se debería tomar en cuenta las siguientes consideraciones:

- En materia de actualización de equipos, cambio de la arquitectura de red para adoptar la segregación, el tiempo estipulado entre la solicitud, aprobación, implementación de cambios, y pruebas, no debería superar los **tres meses** en total.
- En lo relacionado a la implementación de las políticas de seguridad de la información, sí es necesario que, entre la propuesta de las mismas, la aprobación por parte de la directiva, la socialización, la puesta en marcha, exista un período de al menos **seis meses**, luego de lo cual se pueda realizar una primera evaluación.

Riesgo residual proyectado.

Es aquel que persiste a pesar de haber elaborado un plan de mitigación de riesgos, sin lugar a duda los valores presentes en el mismo deben reflejar una disminución muy significativa o casi total en comparación a los identificados inicialmente en la matriz de riesgos, el peso inherente ha sido reducido tras la aplicación de los controles propuestos en un 25% de su valor original, por tanto, la matriz a continuación presenta los valores actualizados.

Tabla 12

Cálculo del riesgo residual proyectado

	Riesgo Residual
Riesgo 1	$1.75 \times 3.75 = 6.56$
Riesgo 2	$2.25 \times 3 = 6.75$
Riesgo 3	$1.75 \times 3 = 5.25$
Riesgo 4	$2.25 \times 2.25 = 5.06$
Riesgo 5	$1.75 \times 3 = 5.25$

Nota: Cálculo realizado en base a la aplicación de los controles sobre los valores nulos iniciales.

Conclusiones

- **Primera.** El nivel de madurez de la empresa se encuentra por debajo de lo deseado, hace falta mucho trabajo para colocarla en niveles apropiados que permitan ofrecer parámetros mínimos para garantizar un adecuado manejo en temas de S.I.
- **Segunda.** La infraestructura de la compañía se encuentra vulnerable a ataques e incidentes ya que presenta equipos y sistemas obsoletos en gran medida.
- **Tercera.** No existen políticas de control en múltiples aspectos de la compañía, esto sumado al desconocimiento del personal en temas de seguridad de la información, representan un reto muy grande para la gerencia de la empresa.
- **Cuarta.** Es necesario realizar una inversión en modernizar infraestructura, puede implicar el realizar un estudio económico preliminar para determinar un orden de prioridades para que el impacto económico sea manejable para la empresa.
- **Quinta.** La directiva debe elaborar, aprobar y revisar a detalle un “**plan de gestión de seguridad de la información**”, el mismo que debe contener:
 - Las políticas internas de la empresa.
 - Designar un oficial de seguridad de la información.
 - Establecer plan de respuesta a incidentes.
 - Agendar un ciclo de simulación y pruebas de ataques en un ambiente controlado.
 - Establecer un cronograma para revisión de cumplimiento, a través de auditorías.
- **Sexta.** Es necesario indicar que la transformación digital que están atravesando los medios de comunicación a nivel mundial, obliga a los directivos de estas empresas a poner especial énfasis en la capacitación de su personal periodístico, debido a que, al estar próxima una eventual desaparición casi total de los medios impresos, la cadena de producción cambiará su orientación, trasladando así la creación, y difusión de contenidos directamente a los canales digitales, siendo entonces tanto los periodistas, como los administradores de contenido (*community*

managers) quienes se consideren como blanco principal de los ataques informáticos.

Referencias Bibliográficas

Agencia AFP (2019). Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange. El Comercio. <https://www.elcomercio.com/actualidad/seguridad/ecuador-denuncia-millones-ciberataques-assange.html>

Arévalo, F. M., Cedillo, I. P., & Moscoso, S. A. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management. Revista Killkana Técnica, 1(2), 31–42. https://gc.scalahed.com/recursos/files/r161r/w25610w/O1TI307_S2_R1.pdf

Ortiz, D. (2021, julio 29). Ecuador está entre los países con más ciberataques en América Latina. El Comercio. <https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html>

Moran Maldonado, N. M. (2021). Estado de la ciberseguridad en las empresas del sector público del Ecuador: una revisión sistemática. Universidad Politécnica Salesiana, Guayaquil, Ecuador, 1–17. <https://n9.cl/gwnhsb>

Revista Seguridad360 (2022). El modelo de madurez de la capacidad de ciberseguridad. Revista Seguridad 360. <https://revistaseguridad360.com/noticias/capacidad-de-ciberseguridad/>

Salcedo, J. S. (2021). ¿Qué revela el ataque informático a la CNT sobre la seguridad de datos en Ecuador? - Canal News Ecuador. <https://canalnewsecuador.com/2021/09/21/que-revela-el-ataque-informatico-a-la-cnt-sobre-la-seguridad-de-datos-en-ecuador/>

MAGERIT V.3 : Metodología de análisis y Gestión de Riesgos de los sistemas de información. (2012).

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Avila Torres, R. A. (2021). Análisis y evaluación de riesgos: aplicado a EMAPAL-EP, basado en la metodología de MAGERIT versión 3.0. www.dominiodelasciencias.com. <https://doi.org/10.23857/dc.v7i4.2425>

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Conciencia Digital**.



El artículo queda en propiedad de la revista y, por tanto, su publicación parcial y/o total en otro medio tiene que ser autorizado por el director de la **Revista Conciencia Digital**.



Indexaciones

