UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

Modelo de seguridad de la información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTORES

Julio Edgar Molina Ruiz
Carlos Vega Valqui
Eder Jair Villacrez Davila

ASESOR

Ricardo David Iman Espinoza
https://orcid.org/0000-0003-0409-8773

Chiclayo, 2021

Modelo de seguridad de la información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque

PRESENTADA POR

Julio Edgar Molina Ruiz
Carlos Vega Valqui
Eder Jair Villacrez Davila

A la Escuela de Posgrado de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el grado académico de

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

APROBADA POR

Miguel Angel Diaz Espino
PRESIDENTE

Gregorio Manuel Leon Tenorio
SECRETARIO

Ricardo David Iman Espinoza
VOCAL

Dedicatoria

A Dios por brindarme fortaleza en mi camino y permitirme mejorar cada día como persona y profesional. A mis padres por representar la motivación y agradecimiento que han regido en cada etapa de mi vida. A mi esposa por su apoyo incondicional, cariño y sacrificios.

Julio Molina

A Dios por permitirme culminar mi maestría exitosamente. A mis padres José y Gloria que son mi motivación para ser mejor como persona y profesional cada día. A mis hermanos y seres queridos por apoyo incondicional.

Carlos Vega

A Dios ya que gracias a él he logrado concluir mi carrera. A mi esposa e hijos por ser un pilar fundamental en mi vida y formación profesional. A mis padres y seres queridos.

Eder Villacrez

Epígrafe

“La mejor herencia que puede dejar un padre a sus hijos es la Educación”

-Víctor Molina

Agradecimiento

A la Universidad por permitirnos formarnos y fortalecer nuestras capacidades profesionales, al Ing. Ricardo Imán por su orientación y apoyo y a la docente María Arangurí por su tenacidad en los viros necesarios en el proyecto y en beneficio de nuestra formación profesional.

Turnitin Informe de Originalidad

Procesado el: 24-oct.-2021 10:09 -05
Identificador: 1680286570
Número de palabras: 29837
Entregado: 3

Tesis Modelo de Seguridad de la Información Por Julio Edgar Molina Ruiz

Índice de similitud	Similitud según fuente	
20%	Internet Sources:	20%
	Publicaciones:	5%
	Trabajos del estudiante:	N/A

2% match (Internet desde 01-nov.-2019)
http://tesis.usat.edu.pe/bitstream/20.500.12423/1488/1/TM_GarciaSamameSilvia.pdf

2% match (Internet desde 01-nov.-2019)
http://tesis.usat.edu.pe/bitstream/20.500.12423/1373/1/TM_VasquezVelasquezFatima_AlvaZapataJuliana.pdf

2% match (Internet desde 17-abr.-2018)
http://repositorioacademico.upc.edu.pe/upc/bitstream/10757/623063/5/MOSCAIZA_MO.pdf

2% match (Internet desde 13-sept.-2021)
https://vbook.pub/documents/cobit-5-information-securityresspa1213pdf-r21dd974e723

1% match (Internet desde 04-oct.-2021)
https://1library.co/document/z3evxwmq-gestion-contribuye-operacion-procesos-gestion-comercial-empresas-saneamiento.html

1% match (Internet desde 13-feb.-2021)
http://primeconsultores.com.pe/wp-content/uploads/2020/10/NTP-ISO-IEC-27035.pdf

1% match (Internet desde 02-abr.-2015)
http://fr.slideshare.net/danger-leinad/iso-27005espanol-34883875

1% match (Internet desde 17-jul.-2020)
http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/9196/T005.8%20G216a.pdf?isAllowed=y&sequence=1

1% match (Internet desde 04-nov.-2017)
http://dspace.udla.edu.ec/bitstream/33000/7554/1/UDLA-EC-TMGSTI-2017-16.pdf

< 1% match (Internet desde 22-sept.-2021)
https://tesis.usat.edu.pe/bitstream/20.500.12423/3451/1/TM_TaboadaCorneteroLuis.pdf

< 1% match (Internet desde 21-mar.-2020)
https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625703/c%c3%a1ceres_cc.pdf

< 1% match (Internet desde 10-nov.-2020)
https://1library.co/document/9ynvr6jz-propuesta-viabilidad-implementacion-estandar-investigacion-desarrollo-empresa-tecnofaktory.html

< 1% match (Internet desde 05-jul.-2021)
https://1library.co/document/y8r0nm5q-metodologia-fundamentada-aprendizaje-morfofisiologia-competencia-resolucion-estudiantes-universidad.html

< 1% match (Internet desde 27-jul.-2020)
http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3331/BC-TES-TMP-2179.pdf?isAllowed=y&sequence=1

< 1% match (Internet desde 28-ago.-2019)
http://docplayer.es/5605405-Universidad-central-del-ecuador.html

< 1% match (Internet desde 18-jul.-2020)
https://docplayer.es/20093328-Norma-tecnica-ntp-iso-iec-27001-peruana-2014.html

< 1% match (Internet desde 07-ago.-2020)
http://dspace.ucuenca.edu.ec/bitstream/123456789/28655/1/Trabajo%20de%20titulaci%c3%b3n.pdf

< 1% match (Internet desde 27-sept.-2021)
https://cpl.thalesgroup.com/es/industry/retail-data-security

< 1% match (Internet desde 24-sept.-2020)
https://www.isotools.org/2018/10/15/resumen-nueva-norma-iso-31000-gestion-riesgos/

< 1% match (Internet desde 19-jul.-2013)
http://www.mific.gob.ni/LinkClick.aspx?fileticket=tuKkTWwKlyI%3d&tabid=351&language=en-US

< 1% match (Internet desde 05-jun.-2017)
http://documents.mx/documents/sgsi5571fb12497959916993dbc1.html

< 1% match (Internet desde 17-nov.-2006)
http://www.pcm.gob.pe/portal_ongei/publicaciones/IEncuestadeSeguridad.pdf

< 1% match (Internet desde 02-jul.-2019)

Índice

Lista de figuras

Lista de Tablas

Resumen

En la actualidad, las capacidades tecnológicas e industriales de las empresas se han desarrollado para alcanzar un alto nivel, ello en respuesta a los constantes retos que demanda el mercado y la industria; y es, en este entorno de alta incertidumbre y competitividad, que la información ha tomado mayor valor, convirtiéndose en un activo relevante y debiéndose adoptar métodos y buenas prácticas para protegerla. Es así, que la presente investigación plantea una propuesta de solución frente a riesgos de seguridad de la información que puedan causar potenciales impactos a empresas editoriales.

La investigación fue aplicada a una empresa editora del medio, donde se abordaron los procesos de Gestión Operativa de Planta y Gestión Editorial, por considerarse los procesos más sensibles y de alto impacto en el negocio. Se determinó que tres grupos empresariales de la región formen parte de la muestra de estudio, con el propósito de desarrollar un marco estratégico de seguridad de la información y que permita proteger los activos de información y facilitar el logro de los objetivos de negocio. En virtud de ello, se identificó que estas no dimensionaban adecuadamente los riesgos de seguridad de la información y las potenciales amenazas existentes en "Tecnologías de la Información – IT" y "Tecnologías de la Operación – OT", dado que podrían afectar la continuidad de las operaciones y generar impactos de carácter financiero, contractual, legal y reputacional.

En este sentido, se estableció como objetivo general, respaldar la disponibilidad de las operaciones estratégicas de las empresas editoras de la región Lambayeque, a través de un modelo de seguridad de la información, sustentada en la armonización de estándares, normas y buenas prácticas de IT/OT y enmarcadas en el ciclo de Deming para su mejora continua.

Finalmente, se concluye que la propuesta "Modelo de Seguridad de la Información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la Región Lambayeque" fue valorada por juicio de expertos, evaluándose su confiabilidad a través del método del alfa de Cronbach y contrastándose su hipótesis, permitiendo que una organización mejore sus capacidades de prevención, detección, respuesta y recuperación frente a riesgos de seguridad de la información y fortaleza la concienciación de las personas en seguridad de la información.

Palabras clave: activo de información, riesgos de seguridad de la información, tecnologías de la información, tecnologías de la operación, ciclo de Deming.

Abstract

Nowadays, the technological and industrial capacities of companies have developed to reach a high level, in response to the constant challenges demanded by the market and the industry; and it is in this environment of high uncertainty and competitiveness that information has taken on greater value, becoming a relevant asset and requiring the adoption of methods and good practices to protect it. Thus, this research proposes a solution to information security risks that may cause potential impacts to companies in the publishing sector.

The research was applied to a publishing company, where the processes of Plant Operational Management and Editorial Management were addressed, as they are considered the most sensitive processes and have a high impact on the business. Three business groups in the region were selected as part of the study sample in order to develop a strategic information security framework to protect information assets and facilitate the achievement of business objectives. By virtue of this, it was identified that these did not adequately dimension the information security risks and potential threats existing in "Information Technology - IT" and "Operation Technology - OT", since they could affect the continuity of operations and generate financial, contractual, legal and reputational impacts.

In this sense, the general objective was to support the availability of the strategic operations of the publishing companies of the Lambayeque region, through an information security model, based on the harmonization of standards, norms and good IT/OT practices and framed in the Deming cycle for its continuous improvement.

Finally, it is concluded that the proposal "Information Security Model to support the availability of strategic operations in publishing companies in the Lambayeque Region" was assessed by expert judgment, evaluating its reliability through the Cronbach's alpha method and contrasting its hypothesis, allowing an organization to improve its capabilities for prevention, detection, response and recovery from information security risks and strengthen people's awareness of information security.

Keywords: information assets, information security risks, information technologies, operation technologies, Deming cycle.

I. Introducción

El proyecto de investigación desarrolló un modelo de seguridad de la información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque; teniéndose en consideración los modelos de trabajo, normas, estándares y buenas prácticas de seguridad de la información para caracterizarla y disponerla a las empresas del sector editorial.

En la actualidad, las empresas editoras mantienen su vigencia a pesar del contexto disruptivo que ha generado la pandemia de la Covid-19, esto gracias a las estrategias de apalancamiento financiero, al mejorar su capacidad de incrementar sus ganancias y mejorar sus ratios de rentabilidad, traducidos en estrategias de publicidad, adquisiciones y/o fusiones con otras empresas de la competencia, adaptación de procesos, diversificación y aprovechamiento de una marcada tendencia a la transformación digital. [1]

En este sentido, es imperativo y de acuerdo con lo mencionado, fortalecer de manera continua las capacidades de la organización, ello sin descuidar los recursos más valiosos que toda organización posee: los Activos de Información. Dicha afirmación, lleva a las organizaciones a disponer de una adecuada gestión de riesgos, frente a amenazas emergentes, propias de un mundo interconectado y digital, como ataques cibernéticos, suplantación de identidad y secuestro y/o corrupción de datos, espionaje y sabotaje industrial, etc., los cuales configurarían escenarios de indisponibilidad de los recursos tecnológicos y de la información.

Los activos de información han cobrado mayor relevancia, pues permiten mejorar capacidades de productividad, optimización de recursos y toma de decisiones oportunas (para hacer frente a nuevos desafíos que demanda el mercado). Sin embargo, las condiciones de riesgo también han cambiado en el contexto actual, por lo que se hace necesario dimensionarlos adecuadamente. De ello, se desprende el valor que adquieren estos dos pilares, los activos de información y la tecnología que la soporta, los cuales permitirán respaldar la continuidad de operaciones críticas y desarrollo de capacidades de resiliencia en los procesos, ambos enmarcados en un modelo de gestión y mejora continua.

Estos escenarios de mejora de procesos y de las capacidades de producción de las empresas del sector editorial, se componen y soportan en dos tecnologías lideres: “Tecnología de la Información IT” y “Tecnología de la Operación OT” y comprender este esquema es importante para el entendimiento de los objetivos del modelo propuesto y su alcance. Hoy en día, ambas tecnologías han alcanzado altos niveles de convergencia, en beneficio del sector en estudio.

Ambas tecnologías están expuestas a riesgos, por lo que según la “Encuesta Global de Seguridad de la Información 2018-19” de Ernst and Young” (1400 encuestados: CIO, CISO y otros ejecutivos a nivel internacional) se determinó que en estos dos años se registraron pérdidas de 6,4 mil millones de dólares por correos falsos enviados alrededor del mundo cada día, también se estableció que 3,62 millones es el costo promedio de una filtración de datos y que el 50% de autoridades locales en Inglaterra dependen de un software en un servidor sin soporte. De igual manera, el estudio evidencia que un 77% de organizaciones no tienen identificados sus principales activos de información y carecen de medidas de protección. Se aprecia que el 65% de las organizaciones no consideran a la seguridad de la información como parte de sus estrategias. En contraste, en el Perú esta cifra se eleva a un 90%, pues nuestro país ha registrado casos de vulneraciones tecnológicas debido a fallas en la seguridad de la información.
Asimismo, el diario El Comercio 2018 realizó una publicación el 21 de julio del 2018, referenciando que, en la ciudad de Arequipa, una empresa farmacéutica perdió 39 mil soles a causa de un virus informático. Se destaca que en una de las cuentas bancarias del BBVA para el pago de la nómina salarial de trabajadores se vio afectado debido a que un usuario accedió a un portal web clonado, simulando ser de la entidad bancaria mencionada. De esta manera los ciberdelincuentes lograron obtener los datos necesarios para realizar transacciones financieras. Paralelamente en la publicación de mayo del año 2017 se extrae que uno de cada cuatro casos de secuestros de datos (ransomware) en Latinoamérica ocurrió en territorio peruano, solicitándose monedas digitales Bitcoins por el rescate de la información.

Gelbstein (2011) expresa la importancia de los tres pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad, pues se torna necesario para respaldar una adecuada gestión de la seguridad de la información. Adicionalmente, según la Guía de Seguridad de Sistemas de Control Industrial – NIST SP 800-82 R2, enfatiza la importancia que las Tecnologías de la Operación brindan a uno de los pilares de la seguridad de la información: “la disponibilidad”, debido a que su estado determina la capacidad y grado de impacto al negocio al verse esta vulnerada o comprometida.

La exposición a los riesgos de la seguridad de la información en las empresas editoras, involucraría la consecución de impactos en las operaciones estratégicas y algunos de los factores que permitiría medir estos impactos son costos de carácter reputacional, costos por indisponibilidad de los sistemas industriales (pérdida de tiempo entre 15 % y 18 % en la producción editorial) ver anexo 1, costos por indisponibilidad de los sistemas informáticos, costos legales por información alterada y publicada, costos por brechas existentes en la concienciación de los empleados y grado de responsabilidad frente a la seguridad de la información (un 33% de los encuestados afirmó que conocía y comprendía la importancia de la seguridad y las pautas establecidas en sus organizaciones; además sólo un 27% manifestó adoptar medidas preventivas y acatar las buenas prácticas de seguridad de la información, asimismo el 67% de encuestados indica no haber recibido algún tipo de capacitación o charla sobre seguridad de la información o políticas orientadas a este fin) ver anexo 2.

Bajo la situación problemática descrita, se formula la siguiente interrogante: ¿De qué manera se puede contribuir a respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque? En virtud de la cuestión se planteó la siguiente hipótesis: es posible respaldar la disponibilidad de las operaciones estratégicas de las empresas editoras de la región Lambayeque con la implementación del modelo de seguridad de la información.

Para demostrar la validez del modelo -propuesto- en seguridad de la información, se establecieron como objetivos de la investigación fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a riesgos de seguridad de la información y riesgos tecnológicos (IT/OT), creando las condiciones necesarias para proteger los activos de información, a través de la armonización de metodologías, estándares y buenas prácticas de IT/OT, el incremento del grado de concienciación y capacitación al personal y finalmente la validación del mismo para medir su efectividad y usabilidad en la propuesta de valor.

Desde el punto de vista económico, el modelo contribuirá a reducir el impacto de los riesgos de negocio asociados a la vulneración de los activos de información e indisponibilidad de los recursos IT/OT; desde una perspectiva tecnológica creará las condiciones necesarias para la adopción de nuevas tecnologías, estos bajo requisitos de seguridad de la información; en lo social, propiciará la mejora de una cultura de seguridad de la información (sustentado en estrategias de concienciación y capacitación) y en el aspecto legal permitirá el cumplimiento regulatorio, propiciando la confianza de los stakeholders.

II. Marco teórico

2.1 Antecedentes

El actual tema de investigación que sustenta el presente proyecto toma como referencia las siguientes investigaciones dada su similitud y/o relación al abordar problemáticas semejantes en potenciales riesgos e impactos al negocio.

Mera Balseca, Sebastián [2] (2014) en su investigación denominada "Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo con la norma ISO/IEC 27002 y COBIT 5", aporta un modelo de gestión de riesgos de seguridad de la información asociado con el uso de las TI. De este antecedente se rescató la importancia de "La cascada de metas" definida por COBIT 5, como elemento útil para trasladar las metas corporativas en aspectos tecnológicos u organizacionales, caracterizando un modelo de gestión de seguridad de la información basado en políticas, procesos, estructura organizativa, cultura organizacional, información, servicios – infraestructura y personas con habilidades. Por otro lado, la norma ISO/IEC 27002 permitió establecer buenas prácticas para la gestión de seguridad de la información, garantizando la continuidad y mantenimiento de los procesos de seguridad de la información. Los resultados de la aplicación del modelo propuesto fueron satisfactorios, logrando el cumplimiento de requerimientos normativos, regulatorios y el reconocimiento y protección de información crítica de los procesos identificados en su alcance; facilitando de esta manera posteriores actividades de auditoría.

Córdova Oblitas, César [3] (2015) en su investigación denominada "Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio: Colegio de Ingenieros" , frente a la importancia de la información que se gestiona en los procesos departamentales de los colegios profesionales como: Contadores, Médicos, Ingenieros y Abogados; y ante la carencia de documentación, aplicación de normas internas para el resguardo de la información, el autor propone la implementación de la norma ISO 27001, la cual propone la adopción del ciclo de Deming PDCA (Planificar, Hacer, Verificar y Actuar), y la aplicación de gestión de riesgos con MAGERIT. El autor concluye que la implementación del SGSI con la norma ISO 27001 permitió lograr objetivos estratégicos propuestos, como determinar la documentación para culturizar a la alta dirección en buenas prácticas de seguridad de la información, aplicación de gestión riesgos en seguridad de la información y que afectan a los principales activos en la institución. Asimismo, lleva a establecer las salvaguardas para

mitigar potenciales riesgos, y determinar indicadores para medir la efectividad de cada control declarado. Para generar visibilidad y trazabilidad sobre el sistema de gestión se elaboró un cuadro de mando integral (BSC) alineándose con la mejora continua que demanda el SGSI.

Según Mercado, Enrique Joel [4](2016) en su investigación "Modelo de gestión de seguridad de la información para el E-Gobierno", realizó una revisión de modelos de seguridad de la información, analizando problemáticas, aspectos comunes y relevantes en la seguridad, lo que permitió identificar elementos (fases, organización, funciones, niveles, controles, indicadores y métricas) y sobre ello proponer un modelo de gestión de seguridad de la información para el Gobierno Electrónico en las entidades públicas peruanas, basado en la norma técnica ISO 27001. Sobre ella se determina un plan para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. Adicionalmente se hace uso de una herramienta de evaluación de niveles de madurez para establecer un estado actual y estado objetivo, propiciando una adecuada gestión de los procesos de seguridad de la información.

Rincón López, Carolina [5] (2016) propone el "Diseño de un framework para el gobierno de información basado en COBIT", cuyo aporte fue la identificación de los activos críticos de información, la asignación de roles y responsabilidades y el establecimiento de directrices para el manejo adecuado de la información; de manera que la organización podrá cumplir con requisitos regulatorios colombianos, tomar decisiones acertadas y reducir costos al evitar potenciales impactos en la seguridad de la información.

Soares Souza, Jackson Gomes [6] (2017) realizó un análisis del tratamiento de la seguridad de la información en la gestión de riesgos de la gobernanza de la tecnología de la información de una Institución Federal de Educación Pública de Brasil, donde se verificó el nivel de tratamiento que se brinda a la seguridad de la información en el marco de la gestión de riesgos en el Gobierno de TI. En ella se revaloró la importancia y necesidad de contar con lineamientos y/o políticas rectoras en seguridad de la información, programas de capacitación y concienciación, y procedimientos formalizados para propiciar y reforzar una cultura de seguridad de la información.

Jara Pérez, Diana [7] (2017) describe en su proyecto de investigación la importancia de una adecuada identificación, análisis y valoración de los riesgos de seguridad de la información para así contar con un plan de tratamientos robusto y altamente efectivo para los procesos incluidos en el alcance del SGSI del cliente TGE de la Empresa Assurance ControlTech. Ello acorde a los principios y directrices de la norma ISO 31000, para el proceso de CallCenter. El autor concluye que el marco utilizado en la investigación permitió determinar los riesgos de seguridad de la información con capacidad de impacto relevante, donde se optaron por acciones de mitigación para así evitar vulneraciones a la confidencialidad, integridad y disponibilidad de la información.

Aguilar Araujo, Carlos y otros [8] (2017) expone una propuesta de "Implantación del Cyber Security Framework (CSF) del NIST, usando COBIT en el caso de estudio de la empresa Honda del Perú". El aporte de la investigación facilitó un modelo de armonización de los objetivos de negocio y de TI, generando valor a la organización a través del uso de los catalizadores y escenarios de COBIT 5 y el ciclo de vida de gestión de riesgos del framework CSF (Core, Tiers y Profiles) de NIST. El autor concluye que una adaptabilidad exitosa del Cyber Security Framework (CSF) debe considerar la alineación de los objetivos estratégicos con los objetivos de TI, además de una identificación correcta de los Tiers, el cual muestra el nivel de madurez actual y objetivo de la organización respecto a la ciberseguridad. Adicionalmente el uso de herramientas como la cascada de metas, criterios de evaluación PAM y escenarios de riesgos propias de COBIT 5 permitió reforzar el marco de trabajo descrito.

Cruz, Miguel Ángel [9] (2017) propone una alternativa de "Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica MEDCAM PERÚ SAC", utilizando el método Deming o PDCA (plan, do, check, act) sugerida por la norma ISO/IEC 27001 y los controles recomendados por la norma ISO/IEC 27002, como resultado, se implementó un sistema de gestión de seguridad de la información, el cual permitió establecer y/o diseñar un conjunto de actividades que permitan la identificación, valoración y protección de los principales activos de información frente a potenciales riesgos y amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información. De esta manera se establecieron objetivos de seguridad para respaldar la consecución de los objetivos estratégicos del negocio.

Beteta Lazarte, Juan Enrique [10] (2018) analiza la toma de acciones preventivas frente a potenciales riesgos de seguridad de la informacion en las organizaciones como Mapfre Perú Seguros y Kallpa Corredora de Seguros. Bajo este propósito se recomienda la aplicación de una guía de controles para reforzar la gestión de la seguridad de la información, tomando en cuenta tecnologías emergentes, la tendencia de la transformación digital e internet de las cosas (IoT). Es propicio resaltar que frente a las bondades que presentan estas tendencias se debe considerar los potenciales riesgos que generan para así convertirlos en elementos facilitadores del negocio, pero sin descuidar las brechas y oportunidades que traen consigo. La investigación analiza riesgos de ciberseguridad y/o estrategias de protección de activos en el ciberespacio.

2.2 Bases teóricas

En este apartado se hará referencia de los conceptos que son aplicados en el desarrollo de la presente investigación y que sustenta el modelo teórico de la propuesta.

2.2.1 Gobierno de Tecnologia de la Información.

De acuerdo con ISACA en el documento COBIT 5 para la seguridad de la información, se enfatiza y ponen relevancia a la información como un recurso clave para todas las organizaciones y en ella la tecnología juega un papel importante. COBIT 5 un marco de trabajo integral que permite alcanzar objetivos de gobierno y de gestión de las TI.

Dicho marco se implementa a través de prácticas que proporcionan retroalimentación con respecto a dos cuestiones fundamentales:

- La organización obtiene un valor diferencial proporcionado por TI.
- Gestión del riesgo de TI.

De manera específica la seguridad de la información es abordada por el marco de trabajo de COBIT 5, está es una guía que se orienta por las siguientes razones:

- La necesidad de incorporar a la seguridad de la información en el contexto de la organización.
- La necesidad de establecer los riesgos de seguridad de la información a niveles aceptables y/o tolerables.
- La necesidad de cumplimiento de las leyes y regulaciones relevantes, requisitos contractuales y políticas internas.
- La necesidad de alineamiento con otros marcos y estándares relevantes.

2.2.1.1 Principios de COBIT 5 para seguridad de la información.

COBIT 5 se basa en un marco de cinco principios para seguridad de la información.

a) Principio 1. Satisfacer las necesidades de las partes interesadas, para ellos las organizaciones establecen entre sus objetivos el logro de beneficios propuestos, gestión del riesgo y uso efectivo de recursos. En este marco se establecen metas específicas de seguridad de la información para los procesos de una organización y en conformidad a las expectativas de las partes interesadas.

Figura 1. Cascada de metas.

Fuente: COBIT 5 para seguridad de la información.

b) Principio 2. El principio integra el gobierno de TI y el gobierno de la empresa, determinando que la información y las tecnologías son uno de los principales activos, al mismo tiempo que las parte interesadas y los procesos que conformar las operaciones del negocio.

c) Principio 3. Aplicar un marco de referencia único integrado. Este principio proporciona una base para integrar otros marcos de referencia, estándares y prácticas utilizadas, de manera que permite a las organizaciones utilizarlo como referencia para el gobierno y gestión de TI.

d) Principio 4. Hacer posible un enfoque holístico. Define un enfoque que cuenta con varios componentes que interactúan entre sí. COBIT 5 define catalizadores que de

manera individual o colectiva influye a que estas interacciones funcionen. Las metas de alto nivel de TI definen lo que los catalizadores deberían lograr.

e) Principio 5. Separar el Gobierno de la Gestión.

- Gobierno. Asegura que se evalúen las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcancen las metas corporativas equilibradas y acordadadas. [11]
- Gestión. Planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. [11]

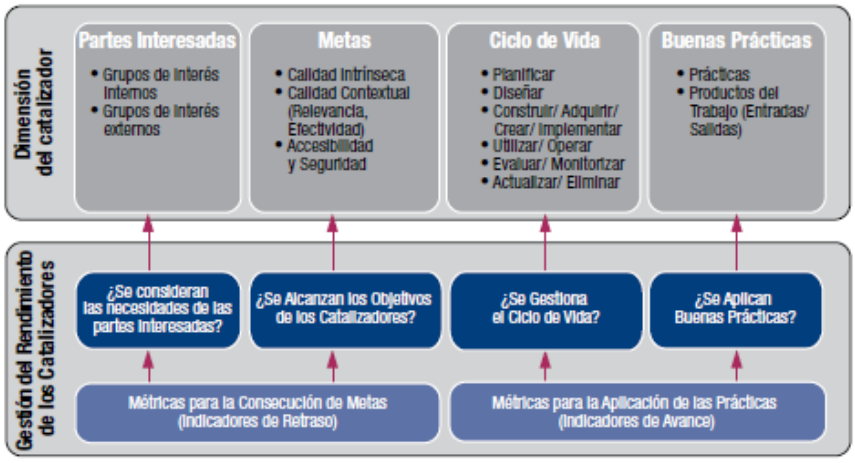
Figura 2. Modelo de referencia de procesos COBIT5

Fuente: COBIT 5 para seguridad de la información

Se establecen lineamientos a través de un conjunto de catalizadores, los cuales establecen las bases para el proceso de implementación de seguridad de la información como parte del gobierno de TI, estos definen:

- Una manera simple y estructurada.
- Manejar complejas interacciones.
- Facilitar resultados exitosos.

Figura 3. Catalizadores COBIT 5: Genéricos.



Fuente: COBIT 5 para seguridad de la informacion.

2.2.2 Seguridad de la Información.

De acuerdo con la norma ISO/IEC 27000:2018 la seguridad de la información permite preservar la confidencialidad, integridad y disponibilidad de la información. Esta consiste en la implementación y gestión de controles y/o salvaguardas apropiadas frente a una amplia gama de amenazas, con el objetivo de garantizar la consecución de estrategias y continuidad del negocio y reducir las potenciales consecuencias de incidentes de seguridad que puedan afectarla.

La seguridad de la información tiene como columna vertebral al proceso de gestión de riesgos, la cual lleva a establecer acciones, estrategias y un marco documentario para establecer lineamientos y directrices que permitan respaldar la seguridad de los principales activos de información de la organización.

2.2.3 Gestión de Seguridad de la Información.

Gestionar la seguridad de la información en una organización demanda la adopción de determinadas normas, estándares y buenas prácticas, las cuales permitirán establecer un marco de trabajo acorde a los objetivos del negocio, y expectativas de los stakeholders. En virtud de ello se detallan las siguientes normas:

a) ISO/IEC 27001:2013 Tecnología de la información Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requisitos.

La norma ISO/IEC 27001 proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Su implementación y/o adopción obedece a la necesidad de proteger los activos de información de una organización [12].

El sistema de gestión de seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información, aplicando para ello un proceso de gestión de riesgos; estos a su vez podrán ser gestionados a través de la identificación, análisis y valoración de riesgos, sustentándose así un conjunto de acciones que deberán ser desplegados para mitigar potenciales impactos.

Un sistema de gestión de seguridad de la información se implementa bajo un enfoque de procesos por lo que su alcance deberá considerar el grado de sensibilidad de estos procesos ante una eventual vulneración a la seguridad de la información.

b) ISO/IEC 27002 - Tecnología de la información- Técnicas de seguridad - Código de prácticas para la gestión de la seguridad de la información.

La norma ISO/IEC 27002 es un código de buenas prácticas para la implementación de controles de seguridad de la información, es un documento guía para que las organizaciones cumplan con requisitos de carácter tecnológico, regulatorio, de gestión y organizativos para preservar la confidencialidad, integridad y disponibilidad de la información.

Esta incluye la selección, implantación y gestión los controles, considerando el entorno de riesgos de seguridad de la información de la información, en este sentido, cada categoría principal de controles de seguridad contiene:

- Un objetivo de control que establece lo que se quiere conseguir.
- Controles técnicos de gestión y organizativos.

Está compuesta por 14 dominios, 35 objetivos de control y 114 controles:

- A.4. Políticas de seguridad de la información.
- A.5. Organización de la seguridad de la información.
- A.6. Gestión de activos
- A.7. Seguridad de los recursos humanos
- A.8. Gestión de activos.

- A.9. Control de accesos.
- A.10. Criptografía
- A.11. Seguridad Física y Ambiental.
- A.12. Seguridad de las operaciones.
- A.13. Seguridad en las telecomunicaciones.
- A.14. Adquisición, desarrollo y mantenimiento.
- A.15. Relaciones con los proveedores.
- A.16. Gestión de incidentes de seguridad de la información.
- A.17. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
- A.18. Cumplimiento.

c) ISO/IEC 27004 - Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Medición.

La norma ISO 27004 proporciona un conjunto de indicadores para la evaluación y/o medición de efectividad de seguridad de la información en una organización.

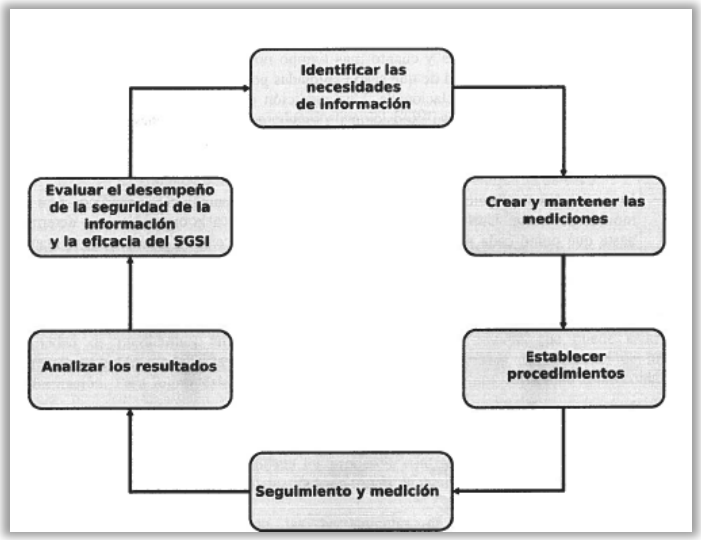
Permite medir el nivel de cumplimiento de controles y del sistema de gestión de seguridad de la información. Para ello, establece lo siguiente:

- El seguimiento y la medición del desempeño de la seguridad de la información.
- El seguimiento y medición de la eficacia de un sistema de gestión de la seguridad de la información (SGSI) incluidos sus procesos y controles; y
- El análisis y la evaluación de los resultados del seguimiento y la medición.

Es aplicable a organizaciones de todo tipo y tamaño. El documento ISO 27004 describe un modelo de medición para la seguridad de la información, incluyendo la relación entre los componentes del modelo de medición y las disposiciones de la norma ISO 27001.

El Anexo B de la norma ISO 27004 proporciona una guía práctica sobre cómo realizar el seguimiento, medición, análisis y evaluación de los procesos del alcance del SGSI.

Figura 4. Proceso de seguimiento, medición, análisis y evaluación



Fuente: ISO/IEC 27004

d) NIST SP 800-50 Creación de un programa de sensibilización y capacitación sobre seguridad de la tecnología de la información.

La norma proporciona pautas para construir y mantener una estrategia de concienciación y capacitación al personal en seguridad de la información. La guía presenta un enfoque, que va desde el diseño, desarrollo e implementación de un programa de concientización y capacitación.

La norma incluye orientación sobre cómo los profesionales de seguridad de TI pueden identificar las necesidades de concientización y capacitación, desarrollar un plan de capacitación y obtener la aceptación de la organización para la financiación del programa. También aborda los siguientes puntos:

- Selección de temas de concientización y capacitación.
- Fuentes y materiales de capacitación.
- Implementación del programa de concientización y capacitación, utilizando variedad de métodos.
- Evaluación de la efectividad del programa.
- Actualización y mejora del contenido del programa de acuerdo con los resultados obtenidos.

2.2.4 Gestión de la Ciberseguridad.

En la actualidad, el número de amenazas cibernéticas crece de manera exponencial y es necesario poder identificarlas, para ello es necesario un marco de gestión que permita medir los riesgos ante el uso de tecnologías cada vez más complejas y procesos cada vez más dependientes de las mismas, permitiendo identificar potenciales amenazas y vulnerabilidades.

a) ISO/IEC 27032:2012 - Lineamientos para Ciberseguridad.

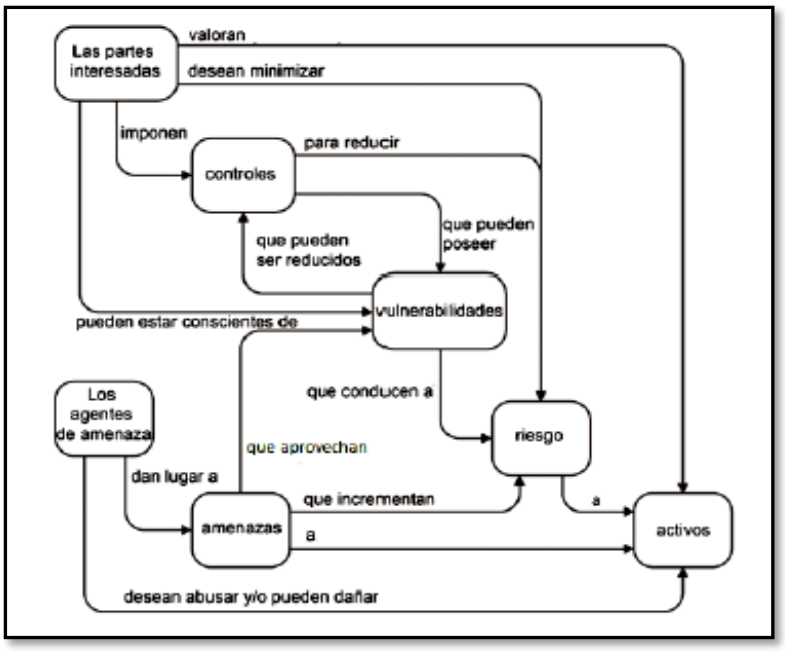
La norma ISO 27032 proporciona una guía para mejorar el estado de la Ciberseguridad en una organización o institución, poniendo en relevancia aspectos de seguridad como:

- Seguridad de la información.
- Seguridad de las redes.
- Seguridad en internet.

La norma de Ciberseguridad proporciona las mejores prácticas de la industria, se sustenta y armoniza con el resto de las normas ISO encaminadas en salvaguardar la seguridad de los principales de información y ciber activos de una organización. Esta se compone de un conjunto de lineamientos o guías que incluyen:

- Roles.
- Políticas.
- Métodos.
- Procesos y controles técnicos aplicables.

Figura 5. Conceptos de seguridad y sus relaciones.



Fuente: Norma ISO/IEC 27032

b) CYBERSECURITY FRAMEWORK NIST.

Como resultado del aumento de ciberataques a sistemas de infraestructuras críticas y al impacto que estos pudieran ocasionar en su disponibilidad, Estados Unidos, el 12 de febrero de 2013 a través de la Orden Ejecutiva (EO) 13636 del presidente Barack Obama, se emitió el propósito de "Mejora de la Ciberseguridad en Infraestructuras Críticas", delegándose al NIST (National Institute of Standards and Technology) el desarrollo de un marco de trabajo para la reducción de riesgos cibernéticos asociados con este tipo de entornos, contando con el apoyo y respaldo del Gobierno, la industria y profesionales especializados.

Para dicho propósito se desarrolló el Framework del NIST, siendo un enfoque basado en el riesgo para gestionar la ciberseguridad, y está compuesto por tres partes: el núcleo del marco, los niveles de implementación del marco y perfiles. En ella, cada componente del Framework refuerza la conexión entre los impulsores del negocio y las actividades de ciberseguridad.

El Framework lleva a establecer un conjunto de fases, actividades y acciones para desarrollar una estrategia ante potenciales amenazas y riesgos que puedan afectar la infraestructura critica de un país, sector industrial o de servicio, todos ellos basados en la operación de tecnologia IT/OT.

Al abordar aspectos de ciberseguridad es conveniente diferenciar las dimensiones de tecnologías de la información y tecnologías de la operación, pues su entendimiento permitirá caracterizar los riesgos, amenazas y/o vulnerabilidades sobre el tipo de tecnologia aplicada en la organización, ello de acuerdo con los atributos implícitos que poseen las dimensiones de IT/OT. Si bien ambos tipos de tecnologías poseen marcadas diferencias debido al tipo de operación que soporta y controla, es importante resaltar la actual convergencia que viene desarrollándose, todo ello como parte de la cuarta revolución: industria 4.0.

c) Tecnologia de la Informacion.

De acuerdo con el glosario de términos de seguridad de la NIST (NIST-7298). Tecnología de la Información representa a cualquier equipo o sistema interconectado que se utilice en la adquisición, almacenamiento, manipulación, gestión, control, visualización, intercambio, transmisión o recepción automática de datos o información. El termino incluye y determina el uso de computadoras, equipos auxiliares, software, u otros servicios similares y recursos relacionados en el tratamiento de la información. Su uso es masivo y cotidiano en instituciones y organizaciones no industriales. Para ello se recurre y toma como guía el documento NIST SP 800-53.

- **NIST SP 800-53. Controles de seguridad y privacidad para sistemas de información federales y organizaciones.**

  El documento NIST 800-53 proporciona un catálogo de controles de seguridad, especialmente orientados para los sistemas y organizaciones federales de EE. UU. El documento aporta un conjunto de controles para gestionar los riesgos de tipo IT, es decir riesgos de Tecnología de la Información.

  El documento permite establecer las siguientes categorías de controles:

  - ✓ **Cifrado de datos y administración de claves.** Cifrado de archivos, volúmenes y aplicaciones sólido y administrado a nivel central, combinado con una administración de claves simple y centralizada que es transparente para los procesos, las aplicaciones y los usuarios.

- ✓ **Políticas de accesos y controles de usuarios.** Políticas de acceso y controles de usuario que permiten que los datos se descifren solo para usuarios y aplicaciones autorizadas
- ✓ **Inteligencia de seguridad.** Aborda los registros que se capturan ante intentos de acceso a datos protegidos y que proporcionan información de inteligencia de seguridad de alto valor, pudiéndose utilizar soluciones de gestión de eventos tipo SIEM (información sobre seguridad y gestión de eventos).

El objetivo del documento es proporcionar directrices y/o controles para reforzar la seguridad de los de información y evitar que estos sean vulnerados, tanto en sistemas físicos, como sistemas basados en la nube, dispositivos móviles, y dispositivos de Internet de las cosas (IoT),

d) Tecnología de la Operación.

La tecnología de la operación es el uso de hardware y software para monitorear y controlar procesos físicos, químicos, equipos y /o dispositivos para infraestructuras críticas. Aborda un conjunto de tecnologías utilizadas en el sector industrial, la cual permite supervisar controlar y gestionar datos operativos a través de sistemas de control para ejercer acción sobre motores, variadores, sensores u otros mecanismos adoptados en dicho sector (plantas nucleares, plantas de tratamientos de agua, plantas eléctricas, sistemas financieros, sistemas militares, etc.). La implementación de controles de ciberseguridad para proteger este tipo de infraestructuras lleva a considerar el documento NIST 800-82.

- **NIST 800-82. Guía de seguridad de sistemas de control industrial (ICS).**

  El documento proporciona orientación sobre cómo asegurar los sistemas de control industrial (ICS) incluidos sistemas de control de supervisión y adquisición de datos (SCADA), sistemas de control distribuido (DCS), controladores lógicos programables (PLC), y otros. La guía proporciona una visión general de ICS y sus topologías, así mismo permite identificar amenazas y/o vulnerabilidades en este tipo de tecnología (OT) y establecer salvaguardas de seguridad para mitigar los riesgos asociados. [15]

Los objetivos de control que aborda el documento son:

- ✓ Restringir el acceso lógico a la red ICS y la actividad de la red.
- ✓ Restricción del acceso físico a la red y dispositivos ICS.
- ✓ Protección de componentes individuales de ICS de la explotación.
- ✓ Restringir modificaciones no autorizadas de datos,
- ✓ Detectar eventos e incidentes de seguridad.
- ✓ Mantenimiento de la funcionalidad en condiciones adversas.
- ✓ Restaurar el sistema después de incidente.

2.2.5 Gestión de Riesgos.

De acuerdo con la norma NTP ISO 73:2011 Gestión del riesgo. Vocabulario, riesgo es la consecuencia de la incertidumbre sobre el logro de los objetivos, y en este sentido la necesidad de gestionarla lleva a establecer acciones sistematizadas que permitan la dirección y el control en una organización respecto a sus riesgos identificados. Existen marcos de trabajo que llevan a operacionalizar la gestión de riesgos, documentos tales como ISO 31000 e ISO 27005.

a) ISO 31000 Gestión del Riesgo - Directrices.

El documento proporciona fundamentos y directrices para evaluar los riesgos en los distintos niveles de una organización, sean estos de niveles operativos o de gobierno, al mismo que propicia y/o genera confianza en los stakeholders.

La norma destaca la importancia del liderazgo de la alta dirección, debido a su capacidad asignar recursos y establecer responsabilidades en la consecución de objetivos establecidos, desplegándose así actividades de trabajo que permitan la identificación, análisis, valoración y tratamiento de los riesgos.

La gestión de riesgos se torna en una herramienta de soporte al proceso de toma de decisiones, permitiendo disminuir la incertidumbre frente al logro de objetivos establecidos.

Los principios que la sustentan son los siguientes:

- La gestión de riesgos debe ser integrado, y no aislado del resto de procesos de la organización.
- Debe ser estructurado, con resultados comparables entre periodos, y tangibles, que permita la medición de su desempeño.

- Debe ser adaptado, es decir, ajustarse al contexto de la organización y estar directamente relacionado con los objetivos.
- Debe ser inclusivo e involucrar a cada una de las partes interesadas, permitiendo diferentes puntos de vista o percepciones que puedan tener.
- Debe ser dinámico, con capacidad para responder a los cambios.
- Debe incluir la mejora continua.

La norma ISO 3100 ofrece un conjunto de herramientas, técnicas y métodos para abordar una valoración y análisis consensuado de los riesgos de una organización.

b) ISO/IEC 31010 Gestión de riesgo. Técnicas para la apreciación del riesgo.

La norma proporciona un conjunto de herramientas o técnicas para la identificación y apreciación del riesgo, es decir suministra un proceso estructurado que identifica como pueden verse afectados los objetivos de la organización, y analiza el riesgo en términos de impactos y probabilidades.

Los beneficios proporcionados por el conjunto de técnicas para la apreciación del riesgo son:

- Entender el riesgo y su impacto potencial en los objetivos;
- Proporcionar información para la toma de decisiones oportunas.
- Contribuir a la comprensión de los riesgos con el fin de facilitar la selección de las opciones de tratamiento.
- Comparación de los riesgos en sistemas, tecnologías o enfoques alternativos.
- Comunicar riesgos e incertidumbre.
- Cumplir con los requisitos regulatorios.

c) ISO/IEC 27005 - Gestión de riesgos de la Seguridad la Información.

La norma suministra directrices para la gestión del riesgo en la seguridad de la información, brinda soporte a los conceptos generales que se especifican en la norma ISO 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

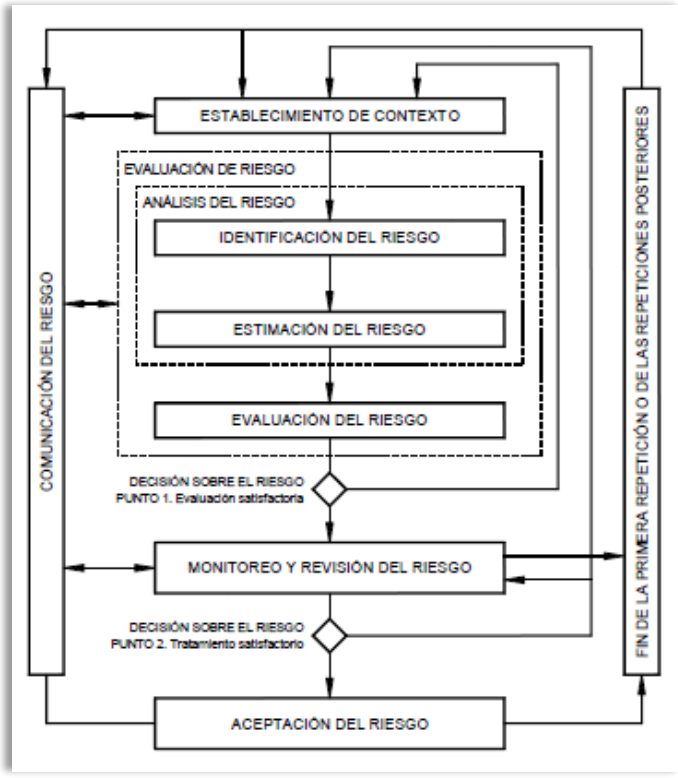
El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO 27001 y en ISO 27002 es importante para la comprensión de la ISO 27005. [13]

Es aplicable a todos los tipos de organizaciones que pretendan gestionar riesgos que podrían comprometer la seguridad de la información.

La norma de gestión de riesgos de seguridad de la informacion permite:

- La identificación de los riesgos.
- La evaluación de los riesgos en términos de impacto al negocio y la probabilidad de su materialización.
- Comunicar los resultados de la evaluación de riesgos.
- Priorizar las acciones de tratamientos de riesgos basados en los resultados de evaluación y análisis.
- Organizar las acciones para reducir la probabilidad de los riesgos.
- Informar a las partes interesadas sobre las decisiones tomadas en la gestión de los riesgos.
- Medir la efectividad y desempeño de la seguridad de la información.
- Monitorear y revisar periódicamente el grado de cumplimiento de las acciones y objetivos de la gestión de riesgos.

Figura 6. Proceso de gestión de riesgos de la seguridad de la información.



Fuente: Norma ISO/IEC 27005

2.2.6 Gestión de Incidentes de Seguridad de la Información.

La gestión de la seguridad de la información y la identificación y tratamiento de sus respectivos riesgos traen consigo la necesidad de gestionar determinados eventos e incidentes de seguridad identificados. El oportuno tratamiento de incidentes de seguridad de la información permitirá tratar potenciales vulnerabilidades o brechas de seguridad, y al mismo tiempo dotar a la organización de una fuente de aprendizaje y consulta para robustecer todo sistema, programa, o modelo de seguridad de la información y ciberseguridad. Se referencia a las normas NIST SP 800-61 e ISO 27035 como fuentes de consulta para abordar una correcta de gestión de incidentes de seguridad de la información.

a) NIST SP 800-61. Guía de manejo de incidentes de seguridad informática.

El marco NIST 800-61 indica las siguientes etapas para gestionar un incidente de seguridad informática:

- **Preparación.** Esta fase implica establecer y capacitar a un equipo de respuesta a incidentes, adquiriendo herramientas y recursos necesarios para ello. En esta etapa la organización debe limitar el número de incidentes, seleccionando e implementando un conjunto de controles, sustentados en los resultados de la evaluación de riesgos. En ella se proporcionan consejos para prepararse y gestionar incidentes, siendo necesario lo siguiente:
    - Información de contacto.
    - Mecanismos de notificación de incidentes.
    - Sistemas de seguimientos o plataforma de mesa de ayuda.
    - Ambiente seguro de almacenamiento.
    - Estaciones de trabajo forenses digitales y/o dispositivos de respaldo.
    - Equipos y/o dispositivos.
- **Detección y análisis.** En importante la detección de:
    - **Vectores de ataque.** Es factible desarrollar instrucciones por cada incidente, deberían estar preparadas para manejar incidentes que usan vectores de ataque comunes. Diferentes tipos de incidentes merecen diferentes estrategias de respuesta.

- **Señales de un incidente.** En esta etapa, se deben detectar y evaluar posibles incidentes, para ello se debe tener una combinación de tres factores:

  - ✓ Los incidentes pueden detectarse a través de muchos medios diferentes, con diferentes niveles de detalle y fidelidad.
  - ✓ El volumen de posibles signos de incidentes suele ser alto.
  - ✓ Conocimiento técnico especializado y una amplia experiencia, son necesarios para el análisis eficiente de datos relacionados con incidentes.

- **Fuentes de precursores e indicadores.** Se identifican utilizando muchas fuentes, como alertas de software de seguridad informática, registros, información disponible públicamente y personas.
  El equipo de respuesta a incidentes debe trabajar rápidamente para analizar y validar cada incidente, siguiendo un pre - proceso definido y documentando. El equipo debe realizar un análisis inicial para determinar el alcance del incidente. El análisis inicial deberá proporcionar suficiente información para priorizar actividades posteriores, tales como la contención del incidente y un análisis más profundo de los efectos de este.
- **Priorización de incidentes.** Esta priorización deberá hacerse en base al impacto funcional, impacto de la información y recuperación del incidente.

- **Contención, erradicación y recuperación.** En esta etapa se debe considerar lo siguiente:
  - ✓ La elección de una estrategia de contención es importante antes que un incidente impacte en los recursos o incremente el daño. La mayoría de los incidentes requieren contención, por lo que es una consideración importante al inicio del manejo de cada incidente. La contención proporciona tiempo para desarrollar una estrategia de remediación personalizada.
  - ✓ La recolección y manejo de evidencia.
  - ✓ La identificación de los host-atacantes.
- **Actividad posterior al incidente.** En esta etapa se considera las lecciones aprendidas, para ello el equipo de respuesta a incidentes debe analizar la causa raíz para establecer las lecciones aprendidas. Se deberá concertar con el

equipo y otros involucrados el tratamiento de las lecciones aprendidas, teniéndose en consideración el uso de datos de incidentes recopilados, la retención de evidencia, la lista de verificación de manejo de incidentes y respectivas recomendaciones.

Figura 7. Estrategias de NIST para enfrentar Ciberamenazas.

Fuente: NIST SP 800-61.

b) ISO/IEC 27035 - Gestión de incidentes de seguridad de la información.

La norma provee un enfoque estructurado y planificado para:

- Detectar, informar y evaluar incidentes de seguridad de la información.
- Responder a los incidentes de seguridad de la información y manejarlos.
- Detectar, evaluar y manejar las vulnerabilidades de seguridad de la información.
- Mejorar continuamente la gestión de incidentes y seguridad de la información como resultado de su gestión.

La norma ISO 27035 proporciona una guía para la gestión de incidentes de seguridad de la información en diferentes organizaciones. También respalda un marco de trabajo para que proveedores especializados brinden sus servicios de gestión de incidentes de seguridad de la información. La norma establece fases para gestionar los incidentes de seguridad de la información:

- **Planeamiento y reparación.** Política de gestión de incidencias de seguridad de la información y compromiso de la alta gerencia como a nivel de sistema, servicio y red. En esta etapa se establece el equipo de respuesta a incidentes de seguridad (CSIRT).
- **Detección e información.** En esta etapa se detecta e informa eventos de seguridad de la información.
- **Evaluación y decisión.** El evento de seguridad de la información se evalúa y decide si se trata de un incidente de seguridad de la información.
- **Respuestas.** En esta etapa se debe responder al incidente de seguridad de la información incluyendo un análisis forense y recuperación del incidente de seguridad de la información.
- **Lecciones aprendidas.** En esta etapa se identifican lecciones aprendidas, mejoras a la evaluación de riesgos de seguridad de la información y a los resultados de la revisión de la gerencia.

III. Metodología

3.1 Tipo de estudio y diseño de contrastación de hipótesis

El tipo de estudio es cuantitativo aplicado, descriptivo no experimental. Para el cumplimiento de los objetivos de la investigación, se identificó como diseño de contrastación del tipo pre test – pos test; el mismo que permitirá probar el planteamiento de la hipótesis. Se mide la variable dependiente a ser utilizada (pre test), posterior a la aplicación de lineamientos del modelo de seguridad de la información se efectúa una nueva medición (pos test).

A continuación, se detalla lo que se propone lograr en el resultado del método del diseño pre test - pos test.

G O1 X O2

Donde:

- G: Grupo Experimental
- O1: Respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque, antes de aplicar el Modelo de Seguridad de la Información.
- X: Modelo de Seguridad de la Información.
- O2: Respaldar la disponibilidad de las operaciones en las empresas editoras de la región Lambayeque, después de aplicar el Modelo de Seguridad de la Información.

3.2 Población, muestra de estudio y muestreo

Como parte inicial en el diagnóstico de esta investigación se consideró las empresas editoras con presencia en el norte del país listando a continuación:

- El Comercio con presencia en Ancash, La Libertad, Piura, San Martin, Loreto, Cajamarca, Lambayeque, Tumbes, Amazonas
- La Razón con presencia en Piura, Lambayeque, Anchas, Tumbes.
- Exitosa con presencia en Piura, Lambayeque, Anchas, Tumbes.
- La Primera con presencia Piura, Lambayeque, Anchas.
- El Ciclón con presencia en Lambayeque.
- Diario el Correo con presencia en Ancash, La Libertad, Piura, San Martin, Loreto, Cajamarca, Lambayeque, Tumbes, Amazonas.
- La Industria con presencia en Ancash, Libertar, Lambayeque

- Diarios La Hora con presencia en Piura, Tumbes.
- Diario Expresión con presencia en Lambayeque.
- Diario El Tiempo con presencia en Piura, Tumbes.

Del listado anterior se consideró sólo tres empresas editoras como muestra para el estudio con sede en la región Lambayeque. A continuación, se detalla información mínima:

a) Empresa editora 1.

La empresa editora1 empezó sus operaciones el 04 de mayo de 1839. Es un conglomerado de medios de comunicación, que administra varios periódicos y canales de televisión a nivel nacional. pertenece al sector ediciones e impresiones de periódicos y revistas. Tiene una antigüedad aproximada de 180 años, Cuenta con oficinas concesionarias en las ciudades más importantes del país. A continuación, detallamos brevemente puntos importantes de la organización.

Tiene como misión: “Orientar e informar, entretener y culturizar satisfaciendo así la cultura informativa de los lectores. Orientar a los ciudadanos dentro del marco de los principios democráticos, los derechos humanos y los valores cívicos, especialmente los que propugnan la libertad, la verdad, la honradez y la igualdad”.

Tiene como visión: “Nos proyectamos como el grupo informativo de referencia en el país, y el más importante y efectivo como vehículo publicitario”.

Sus valores: “Innovación, servicio, independencia y veracidad.”

b) Empresa editora 2.

La empresa editora 2, con más de 100 años de antigüedad tiene como fecha de fundación el 16 noviembre de 1981. Diario peruano de circulación nacional que se edita en Lima y tiene ediciones regionales en Chiclayo, Iquitos y Arequipa. Actualmente forma parte del Periódicos Asociados Latinoamericanos, al que pertenecen importantes editoras de Latinoamérica. Líneas abajo detallaremos puntos relevantes de la organización en referencia.

Su misión: “Editar publicaciones con una línea veraz y comprometida, agregando valor a la comunidad y a nuestros trabajadores, a través de un grupo institucionalizado”.

Su visión: “Ser el grupo editorial de mayor influencia en el país, transmitiendo nuestros valores, reafirmando nuestra vocación de servicio e incursionando en ámbitos empresariales innovadores”.

Sus valores: “Veracidad, integridad, respeto, dedicación”.

c) Empresa editora 3.

Forma parte de un grupo familiar conocido en la zona norte del país que pertenece al sector denominado: ediciones e impresiones de periódicos y revistas, cuya fecha de creación es el17 febrero de 1952,

Con más de 65 años de haber iniciado actividades, en la actualidad cuenta con oficinas en las ciudades de Chiclayo, Trujillo y Chimbote.

Tiene como misión: “Difundir y publicar noticias de la realidad local, nacional e internacional, de manera plural, objetiva, oportuna y confiable”.

Tiene como visión: “Ser una empresa periodística de referencia en la región aplicando un modelo de gestión comprometido con la excelencia”.

Tiene como valores: “Compromiso nacional, ético y patriótico, objetividad, pluralidad y veracidad”.

3.3 Métodos, técnicas e instrumentos de recolección de datos

Las diferentes técnicas o instrumentos para recolección de datos se describen en forma de resumen en la siguiente tabla.

Tabla 1. Técnicas para recolección de datos.

MÉTODOS	TÉCNICAS E INSTRUMENTOS
Entrevistas	Grabación de voz, y comunicación abierta
Cuestionarios	Encuestas
Observación	Registro de incidencias o de atenciones

Fuente: Elaboración propia

3.4 Plan de procesamiento para análisis de datos

El procesamiento para el análisis de datos es de tipo estadístico, en el que se utiliza la hoja de cálculo de Microsoft Excel, para hallar los porcentajes de variación en la implementación del modelo de seguridad, que conlleve a mejorar la gestión y la satisfacción de los Directivos de la Organización y de los usuarios, así como los diferentes cálculos que se realizan para analizar la problemática que existe en la institución.

Los resultados obtenidos se reflejarán en cuadros y gráficos estadísticos los cuales se publican en los anexos.

IV. Resultados

4.1 Análisis de situación actual de las empresas editoras

El diagnóstico de las empresas que son parte de la muestra de estudio se soportó a través de la elaboración y aplicación de cuestionarios, estos se aplicaron a los Gerentes de TI de cada organización, con el fin de diagnosticar si estas cumplen con las mínimas clausulas señaladas por la norma ISO 27001 en su anexo A (ver Anexo 2). La misma fue sometida al juicio y análisis de un especialista para cumplir con la estructura que este tipo de herramienta requiere para su efectividad (ver Anexo 3).

En la encuesta se ha evaluado cada una de las cláusulas establecidas en la ISO 27001 Anexo A, para el cumplimiento de los objetivos de control de seguridad de la información. De esta manera, pudo determinar el nivel de cumplimiento de los objetivos de control que serán parte del tratamiento de los riesgos del Modelo de Seguridad de la Información en el sector de las empresas editoras de la región Lambayeque, mostrándose así el siguiente gráfico:

Figura 8. Diagnóstico de Seguridad de la Información.

Fuente: Elaboración propia

A continuación, se detalla el análisis del diagnóstico del sector de las empresas editoras de la región Lambayeque respecto a las cláusulas del anexo A de la norma ISO 27001.

De acuerdo con la cláusula **políticas de seguridad** sólo el 40% de los encuestados, cuenta con políticas de seguridad de la información, algunas de las cuales vienen siendo aplicadas, sin embargo, un amplio sector del personal de estas organizaciones desconoce los objetivos, alcance e importancia de estas, carecen de buenas prácticas en cuanto a evaluaciones y actualizaciones periódicas.

En cuanto al **aspecto organizativo de la seguridad de la información** en su totalidad las empresas editoras, ninguna tiene claro los lineamientos a seguir, esto denota un nivel de cumplimiento bajo del 0%, evidenciando la falta procedimientos y controles que permitan gestionar desde el aspecto organizativo la seguridad de la información, es importante el establecimiento de mecanismos que tengan como base algún estándar o modelo de seguridad de la información, permitiendo a todo nivel una gestión de seguridad de la información adecuada.

Con respecto a la **Seguridad Ligada a los Recursos Humanos y la Gestión de Activos** se obtuvo como resultado un 33% respectivamente, donde editora 1 y editora2 mostraron un grado de madurez respecto a los dos objetivos de control, poniéndose en énfasis la importancia de la clasificación, trazabilidad y visibilidad de los activos de información e informática.

El Control de los Accesos y Cifrado denotan un bajo de nivel de cumplimiento donde se obtuvo un 12% y 0% respectivamente, por lo que esta situación genera brechas de seguridad de la información que deberán ser cubiertas por políticas de controles de acceso, registros y mecanismos de autenticación de usuarios establecidos, por lo que la implementación de mecanismos de monitoreo y seguimiento, permitirán el cumplimiento de determinados requisitos de la cláusula. Así mismo la confidencialidad de información sensible deberá ser protegida con mecanismo de encriptación.

Contrario a los resultados anteriores la cláusula **Seguridad Física y Ambiental** obtuvo un 43% la cual evidencia un nivel de cumplimiento medio bajo respecto al aseguramiento e identificación de áreas que deberán ser cubiertas con controles de acceso, infraestructura preparada ante eventuales fallos e incidente de seguridad y planes de mantenimiento regulares; en estos aspectos editora 1denotó un mejor equipamiento de cumplimiento de las exigencias a la cláusula. Editora 3 sin embargo denota un amplio margen de oportunidad de mejora respecto a las buenas prácticas de la cláusula.

Se ha evidenciado que la **Seguridad en las Operaciones** sólo cuenta con un nivel de cumplimiento del 3% siendo la empresa editora 1 la que resaltó en cuanto al establecimiento de controles de seguridad contra código malicioso en la red LAN mediante una solución EndPoint (antivirus, antispam, antispyware, etc.). Ello no implica que esté segura, ya que al igual que editora 2 y editora 3 se ha evidenciado que la falta de procedimientos y responsabilidades del uso y acceso a los sistemas informáticos, la documentación de los procedimientos operativos de uso y acceso, los procedimientos para afrontar incidentes en las comunicaciones, los registros de accesos y uso de las aplicaciones y servicios de la red de datos del personal operativo, el registro de las fallas en comunicaciones, el control documentado de toda la información referida a la red, los mecanismos y controles de seguridad de los medios de almacenamiento de información en tránsito, y los controles de seguridad para el sistema de correo electrónico, las vuelve vulnerables y las expone a amenazas existentes.

La Seguridad de las Telecomunicaciones al igual que la Adquisición, Desarrollo y Mantenimiento de Sistemas, y Relación con los proveedores denotan un bajo nivel de cumplimiento del 0% debido a que ninguna de las editoras tiene claro los lineamientos que permitan gestionar la seguridad en las telecomunicaciones, estableciendo controles en las redes para proteger la información de los sistemas y aplicaciones, así como definir los requerimientos de seguridad para servicios de redes internas y externas incluidos en los acuerdos y estos a su vez regulados en **las** políticas y procedimientos de protección de transferencia de información. Así mismo la protección de los mensajes que se intercambian a través de las redes, manteniendo cláusulas de confidencialidad que deben ser incorporados en los acuerdos de terceros. Así mismo la falta de controles necesarios para regular que los proveedores cumplan los requerimientos de seguridad y que estos se auditen necesariamente. Resaltar que la existencia de controles y procedimientos que definan y marquen la pauta en estas cláusulas es de vital importancia, a fin de establecer criterios necesarios para una gestión segura.

Con respecto a la **Gestión de Incidentes de Seguridad de la Información** se obtuvo como resultado un 65%, siendo editora 1 y editora 2 las que cuentan con procedimientos que permiten una gestión adecuada de incidentes de seguridad de la información. Lo opuesto a ello se ha evidenciado en editora 3, con la falta de controles y el establecimiento de mecanismos de gestión. teniendo como base la elaboración de procedimientos que permitan reportar, clasificar, evaluar y responder a los incidentes de seguridad de la información.

Los **Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio** cuenta con nivel de cumplimiento del 22%, siendo las que resaltan editora 1 y editora 2 al contar con un plan elaborado de continuidad del negocio, así mismo el contar con dicho plan y no ejecutarlo hace que se encuentren expuestas a la materialización de alguna vulnerabilidad o amenaza dejando fuera de línea los procesos estratégicos. Es evidente contar con un modelo o lineamientos que permitan las pautas en la elaboración de planes de contingencia robustos, estos sean implementados, y posterior a ello se realicen pruebas, mantenimientos y evaluaciones constantes, definido evidentemente en una gestión de continuidad del negocio en aspectos de seguridad de la información.

Se ha evidenciado respecto al **Cumplimiento** un resultado del 53% de cumplimiento, resaltando sobre todo editora 1 y editora 2 en cuanto a la definición de políticas y mecanismos de protección de datos y privacidad de la información del personal, estableciendo controles de prevención del uso inadecuado de los recursos de procesamiento de información, realizando auditorias permanentes. Contrario a ello editora 3 resalta con 0% de cumplimiento por la falta en definición de procedimientos y controles de acuerdo con normativa vigente. Importante considerar minimizar el riesgo de interrupciones de los procesos de negocio de la Organización, se deben planificar y acordar detalladamente los requisitos y las actividades de auditoría lo cual implica verificaciones recurrentes.

4.2 Análisis comparativo de las normas y estándares

En relación con la propuesta de un Modelo de Seguridad de la Información, se detalla una colección de normas, estándares, marcos de trabajo, guías y buenas prácticas como referencias líderes en la gestión de la seguridad de la información, las cuales serán las bases en que se fundamenta el Modelo propuesto.

Se ha tomado en cuenta los puntos más relevantes para analizar el enfoque, el cual se aborda desde su descripción, objetivos hasta su estructura, estas a su vez son vertidas en una matriz que permite establecer el grado de armonización entre ellas y su alineamiento hacia objetivos similares. Se realizó dos matrices con el objetivo de referenciar las fases de un modelo de gestión de seguridad de la información y los controles que se utilizan para ejecutar un plan de securización que finalmente es el producto en el cual se soporta la gestión de la seguridad de la información en una organización.

El proyecto también aborda dos aspectos tecnológicos implantados en este tipo de sector (empresas editoriales) como es la Tecnología de Información (IT) y la Tecnología de la Operación (OT), ambas convergiendo bajo una misma plataforma operativa, por lo que las matrices de armonización se sustentan en las normas o estándares más representativos de ambos aspectos tecnológicos.

a) Normas, estándares y marcos de trabajo base referenciados:

Tabla 2. Matriz de Normas, Estándares y Marcos de Trabajo de Seguridad de la Información.

	NIST Cybersecurity Framework	**ISO/IEC 27001:2013**	**COBIT 5 para Seguridad de la Información**	**ISO/IEC 27032:2012**
SIGLAS	NIST CSF - Marco de Seguridad Cibernética del Instituto Nacional de Normas y Tecnología de EE. UU	ISO - International Organization for Standardization IEC - International Electrotechnical Commission	COBIT corresponde por sus siglas en inglés para Objetivos de control para la información y tecnologías relacionadas	ISO - International Organization for Standardization IEC - International Electrotechnical Commission
¿QUÉ ES?	Marco de referencia que se centra en el uso de los impulsores del negocio para direccionar las actividades en ciberseguridad, considerando los riesgos de la ciberseguridad como parte de los procesos de gestión de riesgo de la infraestructura critica de un país u organización.	Norma internacional que define la forma de implementar y operar un Sistema de Gestión de Seguridad de la Información. Solo esta norma es certificable	Marco de trabajo basado en el marco integral de COBIT 5. Se centra en abordar la gestión de la seguridad de la información desde los procesos especializados en proporcionar una guía para definir, operar y monitorizar sistemas para la gestión general de la seguridad de la información.	Norma internacional que presenta una guía para la implementación de ciberseguridad en una organización.
ENFOQUE	Se enfoca en acciones de gestión de riesgos de ciberseguridad en infraestructuras críticas de un país e industria	Proveer requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI.	Proporcionar una guía más detallada y práctica para los profesionales de seguridad de la información y otras partes interesadas a todos los niveles de la empresa	No es un estándar que describe un sistema de gestión, sin embargo, respalda a la ISO 27001 al proveer de guías prácticas de seguridad para partes interesadas en el ciberespacio.

Fuente: Elaboración propia basada en documentos oficiales de las Normas, Estándares y Marcos de Trabajo.

La armonización y despliegue de los estándares seleccionados en la Tabla 2, se desarrolló en el Anexo 5 de la investigación, donde se considera el ciclo de Deming (PDCA) como base para referenciar el alineamiento y propósitos coincidentes con la seguridad de la información de los documentos citados.

De acuerdo con lo expuesto inicialmente, el modelo propuesto de seguridad de la información aborda dos aspectos tecnológicos que actualmente son parte de las operaciones del sector en estudio, donde la integración de los sistemas de tecnología de la información (IT) , utilizados para computación centrada en datos, con sistemas de tecnología operacional (OT), utilizados para supervisar eventos, procesos, dispositivos y realizar ajustes en las operaciones industriales, se presentan como potenciales retos y oportunidades de negocio que pretendemos sean atendidas bajo una convergencia tecnológica provechosa para las operaciones criticas identificadas en el estudio.

Dada esta idea de abordar conceptos diferentes, pero no excluyentes en cuanto a las funciones y características de estas tecnologías para trabajar en conjunto, se analizó y diseñó una matriz basada en normas y marcos de trabajo que respaldan a la seguridad de la información en IT (ISO 27001 y COBIT 5 para seguridad de la información) y seguridad de la información en OT (NIST Cybersecurity Framework e ISO 27032), denotándose su alineamiento bajo la dinámica del ciclo de Deming y cuyas fases o etapas de desarrollo para adoptar un sistema de gestión de seguridad de la información, evidencian coherencia entre sí, haciéndose factible formular un modelo de seguridad de la información .

b) Controles, Guías, Estándares y Buenas Prácticas de Seguridad de la Información referenciados:

Tabla 3. Matriz de controles, guías, estándares y buenas prácticas de Seguridad de la Información.

	SANS Y CIS – Critical Security Controls	**ISO/IEC 27002:2013**	**NIST Cybersecurity Framework.**	**NIST SP 800-53 rev.4**	**PCI-DSS 3.2**
SIGLAS	SANS - SysAdmin Audit, Networking and Security Institute	ISO - International Organization for Standardization	NIST - National Institute of Standards and Technology	NIST SP (Special Publication)	Payment Card Industry Data Security Standard
¿QUÉ ES?	Guía de buenas practicas	Código de buenas prácticas para la gestión de seguridad de la información	Marco de referencia	Compendio de controles para las agencias estadounidenses	Normas de seguridad de éxitos de la industria de tarjetas de pago
ENFOQUE	Acciones de ciberdefensa, orientados a mitigar los ataques comunes y dañinos	Controles que se integran dentro de todos los requisitos en la norma ISO 27001 en relación con el tratamiento de riesgos	Riesgos para la gestión de la ciberseguridad	Basado en experiencias de contención efectiva de ataques reales	Requisitos técnicos y operativos para proteger los datos de los titulares de las tarjetas

Fuente: Elaboración propia basada en documentos oficiales

Los detalles y despliegue de la Matriz de Controles, Guías, Estándares y Buenas Prácticas de Seguridad de la Información son abordados en el Anexo 4 y en ella se evidencia la armonización de cada control de seguridad de la información basada en la norma ISO/IEC 27002 (utilizada para tecnología IT) con los 20 controles de seguridad para infraestructuras criticas – Ciberseguridad (utilizada para tecnología OT principalmente) y como estas "conversan" con otras normas líderes en el mercado como la NIST SP 800-53 (Controles de seguridad de la información IT para instituciones federales norteamericanas), la PCI-DSS 3.2 (normas de seguridad de datos de la industria de tarjetas de pago) y se alinean complementariamente con el NIST Cybersecurity Framework.

A través de la matriz se evidencia que los objetivos de control y los controles mismos para tecnología IT se alinean con los de tecnología OT, demostrándose así una convergencia para el propósito de ejecutar e implementar planes de securización (producto del tratamiento de riesgos) en las operaciones estratégicas de las empresas editoriales.

4.3 Estructura del modelo propuesto.

El modelo propuesto de seguridad de la información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque contempla un ciclo de operación que consta de cinco (5) fases, las cuales permitirían que las empresas de este sector puedan gestionar adecuadamente la seguridad de sus activos de información y minimizar potenciales riesgos. El modelo armoniza con las principales normas y prácticas del mercado y se enmarca en el ciclo de Deming como parte de una gestión de mejora continua.

El proyecto no pretende abordar un Sistema de Gestión de Seguridad de la Información (SGSI) pero si crear las bases para subsiguientemente alcanzar su implementación, adopción y certificación, por lo que la propuesta insta a enmarcar los procesos al enfoque de seguridad de la información y al cambio cultural organizacional respecto a ella. En la tabla 4 se muestra en detalle el modelo de seguridad de la información, las fases, las sub-fases, los estándares considerados para el desarrollo de cada una de las fases y como consecuencia de ellos los documentos obligatorios generados.

Tabla 4. Modelo Propuesto de Seguridad de la Información.

MODELO PROPUESTO DE SEGURIDAD DE LA INFORMACIÓN			
PROCESO	**NORMAS/ESTÁNDARES A UTILIZAR**		**LISTA DOCUMENTOS OBLIGATORIOS**
FASE I - DEFINICIÓN DEL ALCANCE Y DIAGNÓSTICO	1.1 Análisis de Contextos y Partes Interesadas	ISO 27001	Análisis del contexto y partes interesadas
	1.2 Alcance del Modelo de Seguridad de la Información.	ISO 27001	Alcance del modelo de seguridad de la información
	1.3 Liderazgo y Compromiso.	ISO 27001	(1) Establecimiento del compromiso de la Alta Dirección. (2) Política del Modelo de Seguridad de la Información.
	1.4 Definición de Roles y Responsabilidades de Seguridad de la Información	COBIT 5 para Seguridad de la Información	Matriz de roles y responsabilidades.
	1.5 Definición del Perfil Actual	NIST SP 800-53/ NIST SP 800-82 /ISO 27002	Definición del estado actual OT (a través de Critical Security Controls Initial Assessment Tool v7) y estado actual IT (a través de análisis de brechas basado en la norma ISO 27002)
FASE II - PLANIFICACIÓN	2.1 Identificación, análisis y evaluación de Riesgos de Seguridad de la Información.	ISO 31000 e ISO 31010 anexo B	Identificación de activos (inventario de activos de información) Análisis de riesgos (Bow Tie)
	2.2 Tratamiento de riesgos de seguridad de la información.	ISO 31000 e ISO 31010 anexo B	(1) Matriz de Tratamiento de Riesgos de Seguridad de la Información (2) Diseño de documentos: políticas, procedimientos, instructivos, registros (estructura de una política y procedimiento).
	2.3 Identificación de aplicabilidad de controles.	ISO 27001	Declaración de Aplicabilidad del Modelo de Seguridad de la Información.
	2.4 Definición de los Objetivos de Seguridad de la Información	ISO 27001, ISO 27032, ISO 27003	Objetivos de Seguridad de la Información.
	2.5 Capacitación y Concienciación	NIST SP1 800-50	(1) Plan de capacitación y concienciación del modelo de seguridad de la información. (2) Registros de capacitación y concienciación. (3) evaluación y resultados de eficacia.
	2.6 Definición del Perfil Destino.	NIST SP 800-53/ NIST SP 800-82 / Framework Cybersecurity / ISO 27002	Perfil destino IT/OT
FASE III – IMPLEMENTACIÓN	3.1 Operacionalización de estrategias de Securización.	Framework Cybersecurity, ISO 27001	(1) Matriz Integral de Seguimiento de Acciones.
	3.2 Gestión de Incidentes	ISO 27002, ISO 27035, ISO 27005, NIST SP 800-61	(1) Procesos y procedimientos de gestión de incidentes. (2) Equipo de gestión de incidentes. (3) Cuadro de gestión de incidentes de seguridad de la información.
FASE IV - EVALUACIÓN DEL DESEMPEÑO	4.1 Monitoreo y medición.	ISO 27001, ISO 27004	Proceso Definición de Indicadores del Modelo de Seguridad de la Información. Cuadro de indicadores del modelo de seguridad de la información
FASE V – MEJORA CONTINUA	5. Mejora continua.	ISO 27001	(1) Cuadro de Control de Mejoras.

Fuente: Elaboración propia.

FASE I - Definición del alcance y diagnóstico

La fase se sustenta en los requisitos de cumplimiento de las normas (ISO 27001 y Framework Cybersecurity), donde se identifican los factores internos y externos con capacidad de influir en el modelo y las necesidades y/o expectativas de las partes interesadas. Asimismo, se establece el liderazgo y compromiso necesario de la Alta Dirección, para impulsar el modelo y asignar recursos; también se definen los roles y responsabilidades necesarios para el desempeño de las actividades, y se establece un perfil actual como base y recurso informativo del estado actual y nivel de madurez de la organización respecto a la seguridad de la información. La fase comprende 5 procesos:

1.1 Análisis del contexto y partes interesadas

Responde a los lineamientos de la norma ISO 27001 capítulo 4, cláusulas 4.1 y 4.2, donde requiere identificar los factores internos, externos y las necesidades y expectativas de las partes interesadas que son relevantes y que pueden afectar a la capacidad de lograr los resultados deseados del modelo de seguridad de la información en la organización.

a) Actividad: Se deberá prestar especial atención a la identificación y análisis de amenazas conocidas y los requisitos de seguridad relacionados con el sector de la organización, por lo que debe analizarse si su implementación va a generar una ventaja competitiva para la organización o permitir el cumplimiento de regulaciones para el negocio.

b) Elemento de salida: El proceso generará el siguiente documento:

Entregable	Proceso dependiente / norma/Anexo
Documento: Análisis del contexto y partes interesadas.	ISO 27001 Capitulo 4.

Tabla 5. Plantilla de análisis del contexto y partes interesadas.

ANALISIS DEL CONTEXTO Y PARTES INTERESADAS		**CÓDIGO: MSI-001**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción del objetivo del documento respecto al análisis del contexto y partes interesadas.
2	Alcance	Breve descripción del alcance del análisis del contexto y partes interesadas.
3	Referencia normativa	Descripción de las normativas que sustentan el documento en relación.
4	Análisis del Contexto	Se consideran los procesos del análisis del contexto que abordara el modelo de seguridad de la información.
5	Partes Interesadas	Se consideran las partes interesadas que abordara el modelo de seguridad de la información

Fuente: Elaboración propia.

La plantilla declarada en la tabla 5 es utilizada y desplegada en el anexo 6, tomando como referencia a la empresa editora consignada en la investigación.

1.2 Alcance del modelo de Seguridad de la Información

El proceso se sustenta en los lineamientos de la norma ISO 27001 capítulo 4, cláusula 4.3, donde se establecen los límites y la aplicabilidad del modelo respecto a los procesos que serán abordados y objeto de estudio, por lo que se considerará los resultados obtenidos respecto a:

- Los aspectos externos e internos referidos en las clausula 4.1.
- Los requisitos referidos en la cláusula 4.2.

a) Actividad: La definición preliminar del alcance es necesaria para crear un plan de proyecto, este debe recibir la aprobación de la Alta Dirección, el resultado es un documento que define el alcance del modelo de seguridad de la información, que incluye:

- Una descripción de como las áreas en el ámbito de aplicación interactúan con otros sistemas de gestión.
- El organigrama de la unidad de negocio y las capas organizaciones del Alcance.
- Los actores del modelo de seguridad (Directivos, procesos, sistemas de información, etc.)
- Ubicación geográfica.
- Tecnologías de información (sistemas y servicios e infraestructura tecnológica) que involucra el Alcance.
- Exclusión del Alcance.

b) Elementos de salida: El proceso generará el siguiente documento:

Entregable	Proceso dependiente / norma/Anexo
Documento: Alcance del Modelo de Seguridad de la Información.	ISO 27001 Capitulo 4 / Anexo 7 del presente documento

Tabla 6. Plantilla de Alcance del Modelo de Seguridad de la información.

ALCANCE DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN		**CÓDIGO: MSI-002**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción del objetivo del documento respecto al Alcance del modelo de seguridad de la información.
2	Alcance	Breve descripción del alcance del documento y su relevancia en el modelo de seguridad de la información.
3	Referencia normativa	Descripción de las normativas que sustentan el documento en relación.
4	Definición del alcance del modelo de seguridad de la información	Se consideran los procesos que abordara el modelo de seguridad de la información.

Fuente: Elaboración propia.

La plantilla declarada en la tabla 6 es utilizada y desplegada en el anexo 7, tomando como referencia a la empresa editora consignada en la investigación.

1.3 Liderazgo y Compromiso

Basado en la norma ISO 27001 capitulo 5, se establece contar con el liderazgo y compromiso de la alta dirección respecto al modelo de seguridad de la información, por lo que se deberá involucrar a estos para asegurar:

- Que el modelo de seguridad de la información logre los resultados previstos.
- Que se dirija y apoye a las personas para que contribuyan con la efectividad del modelo de seguridad de la información.
- Que se promuevan la mejora continua.

a) Actividad: El éxito del proyecto, nivel de involucramiento y compromiso del personal, dependerán del grado de respaldo de la alta dirección, por lo que obtener su aprobación para iniciar con el proyecto de implementación del modelo, es fundamental. Esta deberá evidenciarse a través de actas y registros.

También se define la política de seguridad de la información, la cual deberá ser consistente con los objetivos estratégicos del negocio. Se diseñará un documento de alto nivel que enmarcará el propósito del modelo propuesto. El lineamiento está basado en la norma ISO 27001, capitulo 5, clausula 5.2 donde se define la necesidad de establecer una política de seguridad de la información.

b) Elementos de salida: El proceso generará los siguientes documentos:

Entregable	Proceso dependiente / norma/Anexo
Documento: Política de seguridad de la información	ISO 27001 Capitulo 5 / Anexo 8 del presente documento
Documento de compromiso de la alta dirección	

Tabla 7. Plantilla de Política de Seguridad de la Información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		**CÓDIGO: MSI-003**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción del objetivo del documento
2	Alcance	Breve descripción del alcance de la política de seguridad de la información.
3	Referencia normativa	Descripción de las normativas que sustentan el documento en relación.
4	Definiciones	Se consideran la descripción de los términos que abordará el modelo de seguridad de la información en la presente política
5	Política de Seguridad de la Información	Se describe las políticas que abordará el modelo de seguridad de la información y que enmarcan los lineamientos que la organización deberá seguir.

Fuente: Elaboración propia.

La plantilla declarada en la tabla 7 es utilizada y desplegada en el anexo 8, tomando como referencia a la empresa editora consignada en la investigación.

Tabla 8. Plantilla de registro del compromiso de la alta dirección.

COMPROMISO DE LA ALTA DIRECCIÓN		**CÓDIGO: MSI-004**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Titulo	Describe el título del acta de compromiso
2	Lugar y Fecha	Breve descripción del lugar y fecha
3	Alta Dirección	Breve descripción del o los miembros que conforman la Alta Dirección.
4	Asunto	Descripción el asunto o motivo del compromiso
5	Cuerpo o contenido	Se detalla el contenido del compromiso de la Alta Dirección, dando detalles y sustentando de porque se realiza dicho documento.
6	Firmas	Firman los participantes del compromiso.

Fuente: Elaboración propia.

1.4 Definición de Roles y Responsabilidades.

Se basa en la estructura propuesta por COBIT 5 para Seguridad de la Información, capitulo 4, catalizador: estructuras organizativas; donde se incluye tres elementos claves en la toma de decisiones de una empresa, las cuales son:

- Modelo de estructuras organizativas.
- Ejemplos de roles y estructuras de seguridad de la información.
- Responsabilidad sore la seguridad de la información dentro de la empresa.

a) Actividad: En esta etapa se asignan responsabilidades y la autoridad necesaria para asegurar que el modelo propuesto de seguridad de la información desarrolle sus lineamientos y capacidades a través de la participación y control de desempeño del personal seleccionado, los cuales generarán inputs al modelo de seguridad de información.

b) Elementos de salida: El proceso generará los siguientes documentos:

Entregable	Proceso dependiente / norma/Anexo
Documento: Matriz de roles y responsabilidades de seguridad de la información	COBIT 5 para Seguridad de la Información, capitulo 4, catalizador: estructuras organizativas, anexo 9

Tabla 9. Plantilla de Matriz de roles y responsabilidades de seguridad de la información.

MATRIZ DE ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN		**CÓDIGO: MSI-005**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción del objetivo del documento
2	Alcance	Breve descripción del alcance del documento respecto a los roles y responsabilidades.
3	Roles y responsabilidades	Descripción de las normativas que sustentan el documento en relación.
4	Identificación de los responsables	Se consideran la descripción de los roles y responsabilidades y los cargos que se ejercerá en el modelo de seguridad de la información.

Fuente: Elaboración propia

La plantilla declarada en la tabla 9 es utilizada y desplegada en el anexo 9, tomando como referencia a la empresa editora consignada en la investigación.

1.5 Definición del Perfil Actual.

Tiene el propósito de definir el estado actual de los procesos que estarán dentro del Alcance (1.2 Alcance del Modelo de Seguridad de la Información) del proyecto, en el cual se establecerán dos aspectos de valoración:

- Nivel de cumplimiento.
- Nivel de madurez.

a) Actividad: Se utilizarán herramientas elaboradas en base a los objetivos de control de las normas de seguridad, los cuales son:

- Critical Security Controls Initial Assessment Tool v7. (basada en los 20 controles críticos de seguridad, difundida por el Centro de Seguridad de Internet CIS) para tecnología OT.
- Herramienta de análisis de brechas ISO 27002 para tecnología IT.

El resultado obtenido en esta etapa permitirá comprender el estado actual de la organización respecto a los niveles de cumplimiento y madurez en seguridad de la información, al igual que identificar las brechas de seguridad, permitiendo sincerar a las partes involucradas y establecer compromisos y acciones para mejorar la seguridad y minimizar los niveles de riesgo. Su definición respalda una posterior comparación entre un antes y un después de la implementación, el cual refleja una evidencia del desempeño y efectividad del modelo propuesto.

b) Elementos de salida: Se generan los siguientes entregables:

Entregables	Proceso dependiente / norma/Anexo
Análisis de brechas en tecnología de la operación - OT.	Anexo 10
Análisis de brechas basado en la norma ISO 27002	Anexo 11

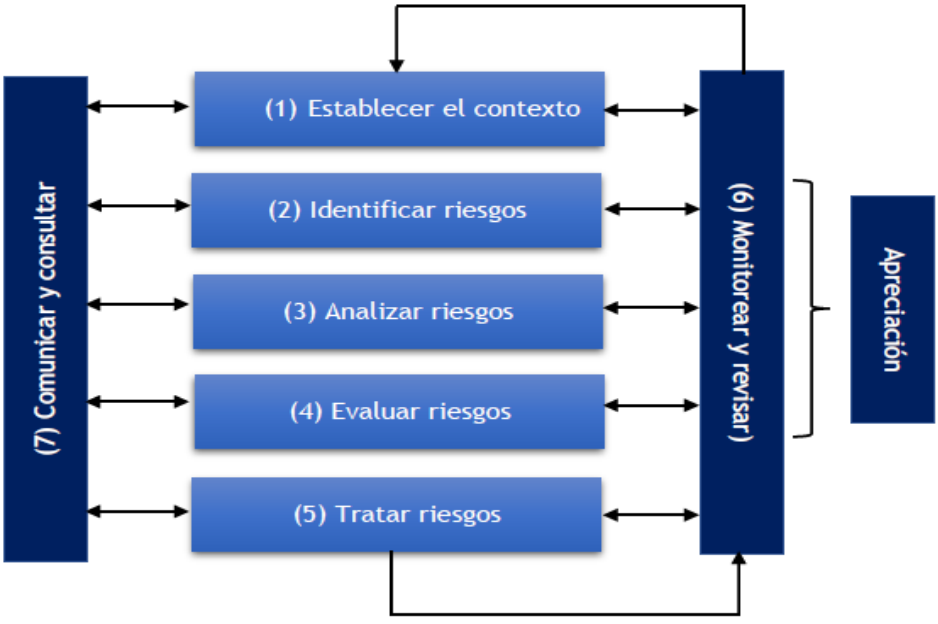
FASE II - Planificación

La fase tiene como objetivo establecer las bases que permitirán la identificación, análisis y evaluación de los potenciales riesgos, tomándose como referencia las directrices de la norma ISO 31000 e ISO 31010. A su vez permitirá establecer un conjunto de estrategias para la selección y/o implementación de controles de seguridad y determinar los objetivos de seguridad de la información, acorde con el nivel de madurez que se pretende alcanzar en el presente modelo.

2.1 Identificación, Análisis y Evaluación de Riesgos de Seguridad de la Información.

El proceso describe cada acción que se deberá realizar para abordar una gestión de riesgo eficiente, enmarcada desde el riesgo de la seguridad y el negocio. En ella se deberá identificar los principales activos de información, someterlos a una valoración y posteriormente abordar un análisis y evaluación de riesgos de seguridad de la información.

Figura 9. Esquema General de Gestión de Riesgos de Seguridad de la información.



Fuente: Norma ISO 31000 Gestión del Riesgo

Se cuenta con las siguientes actividades**:**

a) **Identificación de activos de información.** Se identifican los activos de información los cuales están categorizados en dos dimensiones, activos primarios y activos de soporte:
   - **Activos Primarios:** Estos se conforman de información digital o física, proceso o actividades del negocio, consideradas relevantes o críticas.
   - **Activos de Soporte:** Estos permiten respaldar y operacionalizar los activos primarios y se componen de servicios de TI, enlaces de comunicación y redes, equipos de procesamiento, proveedores, personal, espacios físicos, hardware y software.
   - **Valoración de activos.** Los activos de información se evalúan respecto de su importancia CID (Confidencialidad, Integridad y Disponibilidad) para los procesos y sistemas de información del alcance del Modelo de Seguridad de la Información y respecto a aspectos de legalidad y negocio, en ella se definirán los valores de importancia de los activos primarios y estos valores a su vez serán heredados a los activos de soporte que las respaldan.

   En los activos de soporte se centra la gestión de riesgos debido a que sobre estos se establecen los controles de seguridad de la información en el tratamiento de riesgos y que a la par llevan comprendidos a los activos primarios. Aquellos activos de soporte cuya importancia de valoración sea igual o mayor a cuatro (4) se catalogan como críticos y pasan a la fase de análisis de riesgos.

b) **Análisis del riesgo de Seguridad de la Información.**

   Todos los riesgos de seguridad de la información sin excepción serán registrados en la Matriz Bow Tie, en la cual se tipificarán los riesgos de seguridad de la información y seguirán el proceso que establece la herramienta (Matriz Bow Tie de la norma ISO 31010).

- **Paso 1. Identificación del riesgo.** La identificación de riesgos debe ser liderada por los gerentes de las áreas operativas, jefes de unidades o supervisores de área. Sin embargo, la participación en el ejercicio de identificación abarca a un grupo mayor, pudiendo comprender personal de diferente nivel en la organización y de diferentes áreas e incluso representantes de terceros.
- **Paso 2. Análisis de Riesgos.** En esta etapa se determina el nivel de exposición al riesgo, mediante la definición de la probabilidad de ocurrencia y el impacto esperado, tomando en cuenta la efectividad razonable de los controles implementados. Para ello, la metodología comprende la identificación de las causas, los controles existentes y las posibles consecuencias de un riesgo.

  Una vez determinado el nivel de exposición a un riesgo, se procede a compararlo con los criterios de criticidad y tolerancia establecidos por la organización, con la finalidad de tomar decisiones relativas a su tratamiento. Ello requiere de la estimación del Nivel de Riesgo Residual y la Máxima Pérdida Estimada.

- **Paso 3. Causas, impactos y controles.** Deben identificarse las principales o más probables causas, controlables o no, que puedan ocasionar que el riesgo ocurra. Cada una de ellas debe ser independiente de las demás. Igualmente, deben identificarse los impactos más relevantes, siendo necesario que el análisis abarque todos los posibles tipos de consecuencias (Sociales, ambientales, financieras, reputacionales, legales y de salud y seguridad).
  Los controles están dirigidos a tratar las principales causas e impactos del riesgo, de acuerdo con esto, los controles pueden clasificarse en:

  - **Controles Preventivos**: Estos son usados para gestionar las causas y, por ende, reducen la probabilidad de ocurrencia de un evento no deseado.

- **Controles Mitigantes:** Son aquellos que reducen los impactos en caso de que el evento de riesgo efectivamente se materialice. Se establecen cuando se ha decidido transferir o tolerar un riesgo y normalmente toman la forma de pólizas de seguro y “plan de contingencias”.
- **Controles Críticos:** El control crítico está definido como aquel control destinado a prevenir o mitigar un riesgo crítico y que previene la principal causa o más de una causa o mitiga el principal impacto o más de un impacto.

Nivel de Riesgo Residual: Es un índice que representa el nivel de riesgo residual asociado al evento de riesgo considerando que los controles ya están implementados y que han sido probados en su efectividad.

Nivel de Riesgo Residual = Factor de Severidad X Factor de Probabilidad

Factor de severidad: El factor de severidad se define como "el grado esperado de daño, lesiones o pérdidas, suponiendo una efectividad razonable de los controles mitigantes existentes y probados”.

La metodología considera una amplia gama de posibles "impactos" en la organización, ya sea de naturaleza financiera, de salud y seguridad, ambiental, social, reputacional y/o legal y utiliza la tabla guía del anexo 17 para estandarizar la evaluación de la gravedad y la mayor coherencia en el proceso.

En el Anexo 17 se muestra la tabla de severidad empleada para seleccionar el factor de severidad a emplear en el análisis de riesgos, comparando los impactos esperados con la descripción referencial establecida para cada tipo y nivel de impacto.

Factor de probabilidad: El factor de probabilidad se define como "la probabilidad de que Editora 1 experimente el impacto considerado, suponiendo una eficacia razonable de los controles preventivos existentes y probados". La metodología evalúa la probabilidad de que el evento de riesgo o situación ocurra en un marco de tiempo específico y utiliza la tabla guía que se muestra en el Anexo 13 para estandarizar la definición de la probabilidad y promover la coherencia en el proceso.

Máxima Pérdida Estimada: El MPE corresponde a una estimación de la peor pérdida creíble a través de la ocurrencia de un evento o situación de riesgo especial. Se define como la pérdida total (financiera, ambiental, social, legal, reputacional y/o en salud y seguridad) ocurrida en el peor de los casos creíbles para un escenario de riesgo particular, asumiendo que todos o la mayoría de los controles existentes son ineficaces. Las estimaciones de Máxima Pérdida Estimada a veces son calculadas para coberturar seguros de propiedad, proyectos y operaciones.

- **Paso 4. Manejo de la herramienta de Análisis – Bow Tie (ISO 31010 anexo B)**

  En el anexo 14 se muestra la herramienta Bow Tie con sus respectivas dimensiones para abordar los pasos anteriores mencionados. En ella se debe registrar los sustentos que permitan determinar los niveles de Probabilidad, Severidad y MPE, lo cual implica la descripción de un probable escenario ante la falla de los controles mitigantes existentes y otro, para la Severidad, considerando un funcionamiento razonable de los mismos, incluyendo en ambos el detalle de las consecuencias esperadas para cada tipo de impacto. Por otro lado, en el caso de la Probabilidad deben registrarse los argumentos que sustentan el factor seleccionado, considerando la operatividad de los controles

preventivos, aspectos coyunturales relevantes y estadísticas relativas al riesgo en la organización y la industria.

- **Criticidad:** Se refiere a la importancia relativa de un riesgo individual, es decir son aquellos que tienen un significativo impacto en el logro de los objetivos estratégicos, resultados esperados y los planes de desarrollo de la organización.
  Un riesgo es definido como crítico si cumple con uno de los siguientes criterios:

Nivel de Riesgo Residual (NRR)	**≥ 90**
Nivel de Severidad en Salud y Seguridad	**≥ 4**
Máxima Pérdida Estimada (MPE) Financiera	**≥ S/. 1 M**
Nivel de MPE No Financiera	**≥ 5**

  La criticidad determina el alcance para todas las actividades de gestión de riesgos: análisis, control, monitoreo y comunicación. Se establece que los riesgos críticos identificados:

  - ✓ Ser reportados a los responsables del modelo de seguridad de la información.
  - ✓ Verificación y/o periódica de los controles críticos y del riesgo.

- **Tolerancia al Riesgo**: La clasificación del riesgo residual sirve de base para definir las medidas adicionales de control de riesgo y establecer sus respectivas prioridades de aplicación.

  En general, un nivel de riesgo residual es tolerable si la gerencia está de acuerdo con que el costo de reducir el grado de

incertidumbre excedería el beneficio de hacerlo. Es decir, acepta continuar la operación con un determinado nivel de riesgo.

Sin embargo, se debe enfatizar que esta tolerancia o aceptación del riesgo se basa en la efectividad de los controles existentes, los cuales deberán ser verificados continuamente.

A continuación, se muestran los criterios de tolerancia definidos en función al Nivel de Riesgo Residual y su evaluación, estableciéndose cómo proceder en cada caso.

Tabla 10. Criterios de Tolerancia.

<table>
<tr><td rowspan="2">NRR</td><td colspan="4">EVALUACIÓN</td></tr>
<tr><td>Bien Controlado</td><td>Requiere Cierta Mejora</td><td>Requiere Mejora Significativa</td><td>Sin Control</td></tr>
<tr><td>>=300</td><td rowspan="2">RIESGO ALTO TOLERABLE
Se debe verificar que no es viable, técnica o económicamente, reducir el riesgo residual.</td><td rowspan="2">TOLERABLE CON PLAN DE ACCIÓN
Se implementará y monitoreará un Plan de Acción para llevar el riesgo a "Bien Controlado"
Requiere conocimiento del gerente general para continuar con la actividad o proyecto</td><td rowspan="2">NO TOLERABLE
Se debe detener las actividades y comunicar al Comité de Riesgos de manera inmediata
Se implementará y monitoreará un Plan de Acción para llevar el riesgo a "Bien Controlado"
Requiere autorización expresa del gerente general para continuar con la actividad o proyecto</td><td rowspan="2"></td></tr>
<tr><td>90-100</td></tr>
<tr><td>30</td><td rowspan="2">RIESGO TOLERABLE</td><td colspan="2" rowspan="2">TOLERABLE CON PLAN DE ACCIÓN
Se implementará y monitoreará un Plan de Acción para llevar el riesgo a "Bien Controlado"
Requiere conocimiento del gerente de planta para continuar con la actividad o proyecto</td></tr>
<tr><td><=10</td></tr>
</table>

Fuente: Determinación de acuerdos con integrantes del modelo de seguridad de la información.

- **Tratamiento de Riesgos:** Culminado el análisis y habiendo contrastado el nivel de exposición al riesgo con los criterios de tolerancia, debe definirse si el riesgo es tolerable o requiere de acciones adicionales que reduzcan dicho nivel, sea mejorando los controles existentes o implementando nuevos.

En términos generales, el tratamiento de los riesgos puede responder a una de las siguientes posibles estrategias o a una combinación de ellas:

- ✓ Eliminar la causa del riesgo, ya sea terminando o sustituyendo la actividad que la genera.
- ✓ Reducir la probabilidad de ocurrencia del evento mediante la implementación de controles preventivos (basados en ingeniería, basados en sistemas y basados en personas).

Como regla general se debe evaluar la aplicación de cada tipo de control desde el de mayor nivel de confianza (ingeniería) al de menor nivel de confianza (personas). A esto se denomina jerarquía de controles y su aplicación debe ir acorde con el nivel de exposición y con una valoración costo/beneficio de su implementación.

a) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Matriz de Identificación de Activos de la Información	Ver anexo N° 11
Matriz de Análisis de Riesgo de Seguridad de la Información: Bow Tie	Ver anexo N° 14

Tabla 11. Plantilla de Matriz de Inventario de activos primarios y soporte.

MATRIZ DE INVENTARIO DE ACTIVOS PRIMARIOS Y SOPORTE		**CÓDIGO: MSI-006**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	ID	Describa la identificación del activo
2	Proceso	. Describa el nombre del proceso que se identifica con el activo
3	Nombre del activo	Describa el nombre del activo
4	Categoría del Activo	. Describa la categoría del activo al que pertenece
5	Subcategoría del Activo	Describa la subcategoría del activo al que pertenece
6	Activo de Soporte Principal	Describa el nombre de los activos de soporte que pertenece
7	Ubicación Física	Describa la ubicación física del activo al que pertenece
8	Usuario del Activo	Describa el nombre del usuario al que pertenece o está encargado el activo.

Fuente: Elaboración propia.

2.2 Tratamiento de Riesgos de Seguridad de la Información.

Para el proceso de tratamiento de riesgos de seguridad de la información, se tienen las siguientes consideraciones:

- El nivel de seguimiento de los riesgos y su tratamiento estarán a cargo de las instancias organizacionales (gerente, jefes operacionales).

- Los integrantes de la Matriz de Roles y Responsabilidades, según corresponda, definirán las acciones para el tratamiento y determinarán el NRR (nivel de riesgo residual) después del Tratamiento.

- Se utilizará para el registro de las acciones de tratamiento la Matriz de Tratamiento de Riesgos de seguridad de la información.

- El coordinador general del modelo de seguridad de la Información realizará el seguimiento de todas las acciones determinadas en los procesos del modelo propuesto.

- Para los casos que sean necesarios, en la gestión de riesgos de seguridad de la información, se realizará la estimación monetaria de la severidad (sustento para la estimación de la severidad) y de la MPE - máxima pérdida estimada (sustento para la estimación de la MPE) exigida por las matrices Bow Tie.

a) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Matriz de Plan de tratamiento de riesgos de seguridad de la información.	Ver anexo 18

Tabla 12. Planilla de Matriz de Operaciones de Tratamiento de Riesgo de Seguridad de la Información.

MATRIZ DE OPCIONES DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION		**CÓDIGO: MSI-007**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Proceso / Sistema de información	Es el nombre del proceso o sistema de información al que le corresponde el riesgo a tratar
2	Subproceso	Es el subproceso de negocio al que corresponde el riesgo a tratar.
3	Código de riesgo	Es un identificador único correlativo del riesgo.
4	Categoría	Describa el nombre de la categoría al que pertenece el riesgo
5	NRR	Nivel de riesgo residual.
6	Opción de tratamiento	Esta descripción que empieza con un verbo en infinitivo
7	Acciones de tratamiento	Es la acción que se plantea en concordancia con la opción de tratamiento que propone la metodología de riesgos.
8	NRR después de tratamiento	Es el Nuevo Nivel de Riesgo Residual que se logrará luego de ejecutada la acción de tratamiento.

Fuente: Elaboración propia.

Tabla 13. Plantilla de Matriz de Plan de Tratamiento de Riesgo de Seguridad de la Información.

MATRIZ DE PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACION		**CÓDIGO: MSI-008**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Proceso/ Sistema de información	Es la descripción del proceso o sistema de información al que le corresponde el riesgo a tratar.
2	Subproceso	Es la descripción del subproceso de negocio al que corresponde el riesgo a tratar.
3	Código de riesgo	Es un identificador único correlativo del riesgo.
4	Riesgo	Es la descripción de escenario de riesgo, se extrae del Bow Tie.
5	NRR	Es el Nivel de Riesgo Residual, se extrae del Bow Tie.
6	Dimensión CID afectada	Puede ser: Confidencialidad, Integridad o Disponibilidad, se determina según el Bow Tie del riesgo.
7	Acciones de tratamiento	Es la descripción de la acción que se plantea en concordancia con la opción de tratamiento elegida.
8	Tipo de acción	Empieza con un verbo, Puede ser: Preventiva o Mitigante.
9	Estado	
10	Fecha	Es la descripción del día, mes y hora que de establecimiento de los parámetros de tratamiento.
11	Responsable	Es el nombre de la persona que es responsable de que se lleve a cabo la acción de tratamiento.

Fuente: Elaboración propia

2.3 Identificación de Aplicabilidad de Controles.

La norma ISO 27000 en su cláusula 2.75 define a la Declaración de Aplicabilidad como un documento que describe los objetivos de control y los controles que son pertinentes y aplicables a un sistema de gestión de seguridad de la información, en virtud de ello el modelo considero su pertinencia como parte de su documentación debido a la relevancia.

Consideraciones: El documento se sustenta capítulo 6.1.3 de la norma ISO 27001, inciso d), donde se determina producir una declaración de aplicabilidad, que contendrá los controles necesarios y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A de la misma norma.

Propósito: producir un documento que será una referencia ante una futura auditoria y eventual implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la organización. Se considera que será uno de los primeros documentos que se analizará, su validación deberá realizarse desde la gerencia antes de pasar a la Fase de Implementación.

a) **Elementos de entrada:**

Entregables	Proceso dependiente / norma/Anexo
Alcance del Modelo de Seguridad de la Información.	Clausula 1.2 de la fase I
Política del Modelo de Seguridad de la Información.	Clausula 1.3 de la fase I
Resultados del Análisis de Riesgos.	Clausula 2.1 de la fase II
Plan de Tratamiento de Riesgos.	Clausula 2.3 de la fase II

a) **Actividades**: se hará uso de la norma ISO/IEC 27002 y de los Controles Críticos de Seguridad de la Información (Cybersecurity), donde se considerará los objetivos de control y controles de seguridad. Al disponer de ambos listados se contrastará cada control definido en la matriz de Tratamiento de Riesgos, al ser congruentes dicho contraste o comparación se entiende que el control será parte de una lista seleccionada que conformarán el documento: Declaración de Aplicabilidad.

   En ella se deberá justificar la aplicación de cada control, así como los controles excluidos. Dicho documento deberá ser sometido a una aprobación por parte de la gerencia.

b) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Declaración de Aplicabilidad	Ver Anexo 19

Tabla 14. Plantilla de declaración de aplicabilidad.

MATRIZ DE DECLARACION DE APLICABILIDAD		CÓDIGO: MSI-009
Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción del objetivo del documento.
2	Alcance	Breve descripción del alcance del documento.
3	Usuarios	Son los usuarios que participan del documento.
4	Tipo de control	Es la descripción del tipo de control que pertenece
5	Aplicable	Considere usted si es aplicable
Cn	Justificación	Considere usted si es justificable
7	Responsable	Considere usted si es responsable

Fuente: Elaboración propia.

2.4 Definición de los Objetivos de Seguridad de la Información.

Los objetivos del Modelo de Seguridad de la Información son la expresión de la intención de la organización para tratar los riesgos identificados y para cumplir con los requisitos de seguridad de la organización. El proceso se sustenta en las normas ISO 27001, ISO 27003 e ISO 27032, donde se establecen la necesidad de definir dichos objetivos y su congruencia con los objetivos estratégicos del negocio y la política de seguridad de la información.

Es pertinente que la determinación de los objetivos debería tomar en consideración los siguientes puntos:

- Eventos de riesgo históricos dentro de la organización.

- Actuales y nuevas exposiciones al riesgo.
- Tendencias de problemas operativos e incidentes anteriores.
- Costos del financiamiento del riesgo.

El éxito y fracaso de otros proyectos y programas de seguridad de la información.

b) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Documento: Objetivos de Seguridad de la Información	Ver Anexo 20

Tabla 15. Plantilla de Objetivos de Seguridad de la Información.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN		**CÓDIGO: MSI-00X**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Objetivo	Breve descripción de los objetivos de seguridad de la información alineados a sus objetivos estratégicos.
2	Marco Estratégico	Breve descripción de la misión, visión y objetivos estratégicos.
3	Pilar Estratégico	Describe los objetivos estratégicos del negocio.
4	Objetivos de seguridad de la información.	Son los objetivos establecidos para el modelo de seguridad de la información.

Fuente: Elaboración propia.

2.5 Capacitación y Concienciación del Modelo de Seguridad de la Información.

El objetivo de este proceso es asegurar que todo el personal al que se le haya asignado responsabilidades definidas en el Modelo de Seguridad de la Información sea competente para llevar a cabo las tareas requeridas. Se debe interiorizar conceptos cuya postura se alineen con los objetivos de seguridad de la información. También se busca que los usuarios y personal externo (proveedores) que brinda servicios en la organización sea concientizado en las buenas prácticas de seguridad de la información.

La etapa utiliza los lineamientos de la norma NIST SP 800-50para construir un programa de entrenamiento y concienciación, a través de estrategias de difusión y contenido se estaría ejecutando un Plan diseñado para desplegarse durante todo el año.

El proceso de capacitación y concienciación mantienen diferencias de enfoque:

Tabla 16. Capacitación y Concienciación.

DIFERENCIAS	
CAPACITACIÓN	**CONCIENCIACIÓN**
Adquisición de habilidades	Cambio de hábitos
Dirigida al intelecto	Dirigida principalmente a las emociones y el comportamiento
¿Qué habilidades tienen que adquirir?	¿Qué comportamiento queremos reforzar o cambiar?

Fuente: Elaboración propia.

a) Actividades:

- Identificar las competencias necesarias para garantizar el correcto funcionamiento del Modelo de Seguridad de la Información.
- Implementar un programa de capacitación para el personal que realiza trabajos que afecten al Modelo de Seguridad de la Información.
- Implementar un programa de concienciación sobre seguridad de la información adecuado a personal tercero (proveedores). En el anexo

21 se muestra una plantilla que nos permite desarrollar un plan de capacitación y concienciación.

- Evaluar la eficacia de las medidas adoptadas y mantener registros.

b) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Plan de capacitación y concienciación del Modelo de Seguridad de la Información.	Anexo 21
Registros de capacitación y concienciación.	Tabla 18

Tabla 17. Plantilla de Plan de capacitación y concienciación del Modelo de Seguridad de la Información.

PLAN DE CAPACITACION Y CONCIENCIACION DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: MSI-00X
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Introducción	Breve descripción de la introducción del documento en referencia.
2	Objetivo	Breve descripción de los objetivos del plan de capacitación y concienciación.
3	Alcance	Describe el alcance del plan de capacitación y concienciación.
4	Plan de capacitación	Describe detalles del plan de capacitación.
5	Plan de concienciación	Describe detalles del plan de concienciación.

Fuente: Elaboración propia.

Tabla 18. Plantilla de Registros de Capacitación y Concienciación.

REGISTROS DE CAPACITACION Y CONCIENCIACION		**CÓDIGO: MSI-00X**
Elaborado por: _____ Revisado por: _____ Aprobado por: _____		
Cambios en el presente documento:		
N°	**ASPECTO**	**DESCRIPCIÓN**
1	Datos del empleador	Breve descripción de la información del empleador.
2	Temas tratados	Breve descripción de los temas a tratarse.
3	Capacitador	Descripción del nombre de la(s) persona(s) a brindar la capacitación.
4	Relación de participantes	Descripción de la lista detallada con información de los participantes.

Fuente: Elaboración propia.

2.6 Definición del perfil destino.

Es el estado "objetivo" al que se desea llegar. Estos se basan en los resultados del Perfil Actual del modelo, donde se definen estrategias y se priorizan acciones que conducirán hacia un perfil deseado. El proceso se sustenta en los requisitos del NIST Framework Cybersecurity y se basa en los objetivos de control de la norma ISO/IEC 27002, NIST SP 800-53 y NIST SP 800-82.

El valor objetivo deberá ser establecido por los responsables y/o lideres del modelo de seguridad de la información y se sustentará en la implementación y ejecución de la "Matriz Integral de Seguimiento de Acciones", cuyos resultados, elevarían el nivel de cumplimiento respecto a los controles definidos en la matriz, como la adopción de mejores prácticas en tecnología IT/OT.

a) Elemento de entrada:

Entregables	**Proceso dependiente / norma/Anexo**
Definición del estado actual IT/OT	Clausula 1.5 de la fase I

b) Elemento de salida:

Entregables	Proceso dependiente / norma/Anexo
Establecimiento del perfil destino IT/OT	Ver anexo 10, anexo 11

FASE III – Implementación

La fase de implementación aborda la operacionalización del modelo de seguridad de la información, en ella se establece un plan de securización que deberá desplegarse y monitorear su ejecución y cumplimiento. A su vez se ejecuta un plan de gestión de incidentes, cuyos eventos alimentaran al modelo de seguridad para lograr resiliencia organizacional. Esta comprende 2 procesos:

3.1 Operacionalización de Estrategias de Securización

El objetivo del proceso es garantizar la protección efectiva de los activos de la organización a través de la implementación de los controles IT/OT obtenidos en la Matriz de Tratamiento de Riesgos de Seguridad de la Información. Esta se basa en el requisito de la norma ISO 27001capitulo 8 y del Framework Cybersecurity del NIST.

En ella se realizarán acciones de priorización basada en el nivel de riesgo residual y evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se producen cambios importantes, teniendo en cuenta los criterios establecidos en la ISO 27001 capítulo 6.1.2 a) por lo que se deberá retener información documentada de los resultados de las evaluaciones y tratamiento de riesgos de seguridad de la información.

a) Elementos de entrada:

Entregables	Proceso dependiente / norma/Anexo
Matriz de Tratamiento de Riesgos de Seguridad de la Información	Clausula 2.2 de la fase II

b) Actividades:

- Revisión de la matriz de tratamiento de riesgos de seguridad de la información.
- Aplicación de los controles de seguridad técnicos, administrativos y de gestión.
- Seguimiento de aplicación de los controles y coordinación con responsables de riesgos, dueño de activos y responsables de los controles.

c) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Matriz Integral de Seguimiento de Acciones	Ver anexo 23

3.2 Gestión de Incidentes

El proceso se sustenta en los lineamientos de la norma ISO/IEC 27002, ISO 27005, ISO 27035 y la NIST SP 800-61, los cuales tienen por objetivo principal asegurar que los eventos de seguridad sean detectados, identificados y tratados.

La norma ISO 27005 define un escenario de incidente como una amenaza que aprovecha una vulnerabilidad o un grupo de vulnerabilidades durante un incidente de seguridad de la información.

La norma ISO 27035 nos brinda un enfoque estructurado y planificado para detectar, informar y evaluar incidentes de seguridad de la información, al mismo tiempo como responder y gestionarlos. Proporciona orientación sobre la gestión de incidentes de seguridad de la información y se complementa con la NIST SP 800-61, cuya guía brinda detalles sobre incidentes de seguridad informático.

La información del proceso de gestión de riesgos es un insumo importante para el proceso de mejora continua de la organización.

a) Elementos de entrada:

Entregables	Proceso dependiente / norma/Anexo
Políticas, procesos y procedimientos de seguridad de la organización.	Clausula 1.1, 1.2, 1.3 y 1.4 de la fase I
Análisis de riesgo	Clausula 2.2 de la fase II

b) Actividades: Aplicación de métodos para detectar y responder a los incidentes, la formación adecuada, la comunicación de incidentes.

c) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Procesos y procedimientos de gestión de incidentes.	ISO/IEC 27002, ISO/IEC 27035, ISO/IEC 27005, NIST SP 800-61
Equipo de gestión de incidentes.	ISO/IEC 27035
Cuadro de gestión de incidentes de seguridad de la información.	

FASE IV – Evaluación del desempeño

No se puede controlar aquello que no se puede medir y en virtud de dicha afirmación se hace necesario evaluar el desempeño del modelo de seguridad de la información propuesto, ello a través de indicadores. Esta actividad permite establecer el estado de salud del modelo respecto a la seguridad de la información. La fase consta de 1 proceso:

4.1 Monitoreo y Medición.

El proceso aborda el monitoreo del desempeño respecto a las acciones, el mantenimiento y la mejora del modelo de seguridad de la información y a su vez demanda medir el nivel de eficiencia como aporte del modelo en el propósito de salvaguardar la seguridad de la información.

La norma ISO 27004 brinda un catálogo y un conjunto de indicadores que permiten medir el desempeño y la eficiencia de la seguridad de la información en una organización, determinándose también la frecuencia, la responsabilidad del monitoreo, medición y evaluación.

a) Actividades:

- Se establecen tableros estratégicos u operacionales, así como informes para presentar los resultados a las partes interesadas.
- Se determina lo que se debe medir y controlar, por lo que se define los métodos de supervisión, medición, análisis y evaluación. Se recopilan los datos y se realiza el análisis y la evaluación de los resultados de supervisión y medición. Es una evaluación sistemática de los objetivos y metas de la organización contra sus logros efectivos, por lo que deben ser considerados en el contexto de la estrategia de la organización y sus objetivos.

b) Elementos de entrada:

Entregables	Proceso dependiente / norma/Anexo
Matriz tratamiento de riesgos de seguridad de la información implementados en el Modelo de Seguridad de la Información.	Clausula 2.2 de la fase II
Matriz Integral de Seguimiento de Acciones	Clausula 3.1 de la fase III

c) Elementos de salida:

Entregables	**Proceso dependiente / norma/Anexo**
Indicadores	Cuadro de indicadores del modelo de seguridad de la información

FASE V – Mejora continua

La fase se sustenta en el ciclo de Deming, el cual es un proceso cíclico y repetitivo que conlleva a una mejora continua, la periodicidad la determina los responsables o lideres del modelo de seguridad de la información.

5.1 Mejora continua

El proceso es un requisito de la norma ISO 27001, el cual tiene por objetivo principal mejorar continuamente la eficacia del Modelo de Seguridad de la Información, asegurarse de que los objetivos del Modelo se mantengan alineados con los objetivos del negocio. Esta etapa garantiza que los planes y procedimientos sean continuamente actualizados.

a) Elementos de entrada:

Entregables	Proceso dependiente / norma/Anexo
Modelo de Seguridad de la Información	Clausula 2.1, 2.2, 2.3, 2.4 de la fase II
Cuadro de indicadores del Modelo de Seguridad de la Información	Clausula 4.1 de fase IV

b) Actividades:

- Proceso continuo de seguimiento a la Matriz Integral de Seguimiento de Acciones.
- Mantenimiento y mejora del Modelo de Seguridad de la Información.
- Actualización continua de la documentación y registros.
- Documentar las mejoras.

c) Elementos de salida:

Entregables	Proceso dependiente / norma/Anexo
Cuadro de Control de Mejoras	ISO 27001

5.2 Objetivos del modelo de seguridad de la información y estrategias de cumplimiento

La presente investigación declara los objetivos que pretende alcanzar el modelo de seguridad de la información, para evidenciar acciones de cumplimiento y su efectividad, ellos enmarcados en el objeto de estudio: empresa editora 1.

a) Objetivo 1: Armonización de metodologías, estándares y buenas prácticas de IT/OT.

Para el desarrollo del modelo de seguridad de la información, se tomaron en cuenta los siguientes aspectos:

- **Normas, estándares y marcos de trabajo base referenciados:**
  NIST Cybersecurity Framework, norma ISO/IEC 27001:2013 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos, COBIT 5 para Seguridad de la Información, norma ISO/IEC 27032:2012 Tecnología de la Información. Técnicas de Seguridad. Directrices para Ciberseguridad.

- **Controles, guías, estándares y buenas prácticas de Seguridad de la Información referenciados:**
  Controles Críticos de Seguridad – Infraestructuras Críticas 20 Controles de Ciberseguridad para tecnología IT/OT, norma ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de Seguridad. Código de prácticas para seguridad de la información, NIST SP 800-53 rev.4 Controles de seguridad y privacidad para los sistemas de información federal y organizaciones – EE. UU.

  De acuerdo con las normas y estándares descritos, se realizó una revisión, análisis y alineamiento conforme el grado de relación y congruencia entre ellas, permitiendo el soporte necesario para el desarrollo del modelo de seguridad de la información.

  En el anexo 4 se muestra la estructura resultante del proceso de armonización, así mismo el detalle de la estructura con las normas, estándares, controles, guías y buenas prácticas de seguridad de la información.

b) Objetivo 2: Fortalecer las capacidades de prevención, detección, respuesta y recuperación frente a riesgos tecnológicos.

De acuerdo con el análisis de riesgo, se identificaron potenciales amenazas y riesgos de seguridad de la información en los procesos del Alcance del modelo (Gestión Operativa de Planta y Gestión Editorial) es así, que estos fueron dimensionados en riesgos a la Confidencialidad, riesgos a la Integridad

y riesgos a la Disponibilidad en dichos procesos. Esta actividad permitió establecer acciones preventivas, mitigantes y de mejora con el propósito de dotar y tomar acción de manera proactiva en los escenarios de riesgos identificados.

Es así como, en el proceso de Gestión Operativa de Planta, se identificaron nueve causas, siete controles preventivos y cuatro acciones de mejora en la dimensión de Disponibilidad; paralelamente en la dimensión de Integridad se identificaron seis potenciales causas que afectarían a los activos de información, cinco controles preventivos y tres acciones de mejora para minimizar el impacto en determinados escenarios adversos. En contraste en la dimensión de Confidencialidad se identificaron una acción de mejora y seis controles preventivos, sumándose cinco potenciales causas adversas.

De igual manera, en el proceso de Gestión Editorial, se identificaron diez causas, nueve controles preventivos y tres acciones de mejora para la dimensión de Disponibilidad, en la dimensión de Integridad se obtuvieron cinco causas, seis controles preventivos y una acción de mejora, en Confidencialidad cuatro causas, cuatro controles preventivos, una acción de mejora.

Como segunda etapa, los resultados del análisis de riesgo obtenido permitieron establecer un Plan de Tratamiento de Riesgos (ver anexo 18) con diez acciones concretas para crear las condiciones de fortalecimiento de las capacidades de prevención, detección, respuesta y recuperación ante potenciales riesgos de seguridad de la información.

c) **Objetivo 3: Incrementar el grado de concienciación al personal en seguridad de la información.**

Para incrementar el grado de concienciación en seguridad de la información, se desarrolló un Plan de Concienciación y Capacitación como parte del modelo de seguridad de la información, ello bajo la premisa de que el factor

humano o las personas, deben ser el eslabón fundamental en la cadena de la seguridad de la información. Por ello la importancia de contar con personal sensibilizado y entrenado en seguridad de la información.

Se estableció la medición de la siguiente manera:

Objetivo: Medir el % de personas que han aprobado el examen del Programa de Concientización en Seguridad de la Información.
Métrica: A = Número de personas que han aprobado el examen del Programa de Concientización en Seguridad de la Información. B = Número total de personas de personas que rindieron el examen del Programa de Concientización en Seguridad de la Información
Función: M = (A/B)*100%

d) Objetivo 4: Validar el modelo de seguridad de la información para medir su efectividad y usabilidad en la propuesta de valor al negocio.

Para validar el modelo de seguridad de la información se sometió a una evaluación de juicio de expertos, en ella, se contó con la participación de tres profesionales (k = 3) con trayectoria reconocida y certificada en seguridad de la información. Basada en la propuesta de Escobar y Cuervo, se desarrolló un formato de validación de expertos para el modelo propuesto (anexo 26) con la finalidad de valorar aspectos de suficiencia, realidad, coherencia y relevancia de cada una de las actividades que contempla el modelo de seguridad de la información (N = 17).

Para obtener resultados basados en las apreciaciones de los expertos (anexo 26), se utilizó el coeficiente de concordancia W de Kendall con un nivel de significancia de 0.05, es decir con 95% de confianza. La estadística sigue una distribución chi-cuadrada ($\chi 2$) con N – 1 grados de libertad.

El coeficiente de concordancia de Kendall puede variar de 0 a 1, mientras mayor sea el valor de Kendall entonces más fuerte será la concordancia. De acuerdo con los resultados obtenidos se plantean dos hipótesis:

- H0: No existe concordancia entre las opiniones de los evaluadores (W = 0).
- H1: Existe concordancia entre las opiniones de los evaluadores (W > 0).

A través del proceso estadístico del software SPSS, se evaluó la concordancia de cada uno de los criterios del juicio de expertos, obteniendo los siguientes resultados:

Tabla 19. Estadístico de prueba W de Kendall

	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
N	17	17	17	17
W	0.381	0.607	0.381	0.474
$\chi 2$	12.943	20.642	12.943	16.128
gl	2	2	2	2
p	0.002	0.000	0.002	0.000

Fuente: Elaboración propia

De acuerdo con los resultados, dado que el valor de W es mayor que cero en los criterios de suficiencia, claridad, coherencia y relevancia, se rechaza la hipótesis nula y se concluye que existe concordancia en las apreciaciones de los expertos, siendo además el valor de $p < 0.05$ lo cual indica que el valor es "significativo".

Para demostrar la confiabilidad del instrumento en el contexto de las empresas editoras, se utilizó el coeficiente alfa de Cronbach, obteniéndose el siguiente resultado:

Tabla 20. Estadístico de confiabilidad Alfa de Cronbach

ALFA DE CRONBACH	ALFA DE CRONBACH BASADOS EN ELEMENTOS ESTANDARIZADOS	N.º ELEMENTOS
0.621	0.621	17

Fuente: Elaboración propia

Considerando lo especificado por Herrera (1998) los valores hallados pueden ser comprendidos entre la siguiente tabla:

Tabla 21. Valores para estimar el nivel confiabilidad

VALOR	CONCLUSIÓN
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabilidad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy Confiable
0,72 a 0,99	Excelente confiabilidad
1.0	Confiabilidad perfecta

Fuente: Elaboración propia

Conforme los valores de la tabla, se considera que el coeficiente de confiabilidad obtenido es de valor Confiable.

5.3 Aplicabilidad del Modelo de Seguridad de la Información

Los resultados obtenidos permiten demostrar que la propuesta del modelo de seguridad de la información acotada a una de las tres empresas del sector editorial de la región Lambayeque, permiten afirmar, sostener y validar su implementación, ya que, a través de una adecuada gestión de riesgos, adopción de buenas prácticas y una cultura de seguridad de la información, basados en un ciclo de mejora continua, se obtendría y reforzaría las capacidades del negocio para así lograr sus objetivos estratégicos.

V. Discusión

En el presente apartado analiza los resultados del modelo de seguridad de la información propuesto y a su vez, estos son comparados con los antecedentes planteados en líneas superiores.

El modelo de seguridad de la información propuesto busca respaldar la disponibilidad de las operaciones estratégicas de una empresa editora del medio local, pero con resonancia y alcance nacional, identificando y dimensionando adecuadamente los riesgos de seguridad de la información, tal como Jara Pérez, Diana [7] describe en su proyecto de investigación sobre la importancia de una adecuada identificación, análisis y valoración de los riesgos de seguridad de la información, reconociendo previamente los procesos críticos o más relevantes, delimitando y estableciendo así un alcance para la protección de los principales activos de informacion.

Cruz, Miguel Ángel [9] propone el diseño e implementación de un sistema de gestión de seguridad de la informacion para la clínica Medcam Perú, basándose en el ciclo de Deming o PDCA (Plan, Do, Check, Act) y en la norma ISO 27001, por lo que proteger los principales activos de información del negocio se torna altamente relevante por la sensibilidad y confidencialidad del tipo de información que gestionan en ella y por las exigencias regulatorias que deben cumplir (Ley 29733, Ley de Protección de Datos Personales).

A diferencia Mera Balseca, Sebastián [2] que propone el diseño de un modelo de seguridad la información basada en la norma ISO 27002 y COBIT 5 para la empresa EP Petroecuador para establecer un conjunto de metas corporativas e implementar controles de seguridad de la información; la presente propuesta plantea un alcance adicional al establecer un estado objetivo de madurez de la ciberseguridad alineadas en un modelo de gestión de seguridad de la información, dado que las características del negocio (empresa editora), le permiten y exigen el uso de tecnología de la operación (OT).

A su vez, el presente modelo de seguridad de la información permitió fortalecer las capacidades de la organización y salvaguardar los activos de informacion críticos, ello tomando como estrategia principal la concientización y sensibilización del personal, dado que es una de las barreras que debe ser reforzada y uno de los eslabones débiles en la cadena de la seguridad de la información. Es decir, el factor humano requirió someterse a un programa de capacitación dirigido, pues en las encuestas aplicadas un 33% afirmó que conocía y comprendía la importancia de la seguridad de la información, y solo un 27% manifestó adoptar medidas preventivas y buenas practicas de seguridad de la información.

En general, la presente investigación se sustenta en la armonización de estándares, normas y buenas practicas de seguridad IT/OT para proponer un modelo de seguridad de la información que permita respaldar la disponibilidad de las operaciones estratégicas del negocio, diferenciándose así de los antecedentes citados, los cuales se basan en una norma o estándar específico, no contando con la pluralidad que enriquece el modelo de seguridad de la información propuesto.

La propuesta de modelo de seguridad de la información fue valorada por juicio de expertos, donde se utilizó el coeficiente de concordancia W de Kendall con un nivel de confianza del 95%, planteándose y obteniéndose valores positivos en los criterios de suficiencia, claridad, coherencia y relevancia. Además, la confiabilidad del instrumento mostró como resultado 0.621, el cual de acuerdo con Herrera (1998) se considera como valor Confiable.

VI. Conclusiones

El modelo de seguridad de la información propuesto fue validado a través del juicio de tres expertos, en el cual se analizaron los criterios de suficiencia, claridad, coherencia y relevancia (anexo N° 28) y es a través de la aplicación del método Alfa de Cronbach, que se obtuvo un valor de fiabilidad de 0.62. Adicionalmente, a través de la aplicación del coeficiente de Kendall se obtuvieron índices mayores a cero, evidenciándose así, el rechazo de la hipótesis nula. Dichos resultados permiten afirmar la congruencia en las apreciaciones de los expertos respecto al modelo de seguridad de la información.

El Modelo de Seguridad de la Información para respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque, se sustenta en la armonización y alineamiento de metodologías, estándares y buenas prácticas de seguridad de la información. En ella se permite validar su consistencia, fiabilidad y potencial aplicabilidad para mejorar las capacidades de la organización frente a escenarios de riesgos emergentes (anexo 4 y anexo 5)

Para medir el cumplimiento de requisitos de seguridad de la información se realizaron análisis de brechas basados en la norma ISO/IEC 27001 anexo A y la herramienta de evaluación AudiScripts para CIS Controls, donde se comparó el estado inicial respecto al estado objetivo de la organización en estudio. En la fase de pre-implementación se obtuvo un 37% de cumplimiento respecto a los controles de seguridad de la información en IT y en OT un 55% (CSC N° 1 y CSC N°2), en contraste, en la fase de post-implementación se obtuvo un 50% de cumplimiento en IT y en OT un 70%. De esta manera se demuestra que las capacidades de prevención, detección, respuesta y recuperación frente a la materialización de riesgos tecnológicos, en la empresa editora, se vieron fortalecidas.

El factor humano también fue un componente identificado como fundamental en el reforzamiento y mejora de la seguridad de la información, debiéndose desarrollar y desplegar un Programa de Concienciación y Capacitación en seguridad de la

información, es así, que para lograr obtener datos que permitan medir la efectividad de la campaña de concienciación se seleccionó a 50 empleados de los procesos del Alcance, quienes llevaron el curso y fueron sometidos a una evaluación, obteniéndose un 74% de aprobación (37 personas). El resultado permitió evidenciar la mejora o incremento del grado de concienciación del personal.

La pandemia de la Covid-19 ha producido un cambio de paradigma en materia de seguridad de la información, la disrupción generó un impacto económico y acelero la adopción de una transformación digital para continuar operando. Es en este escenario que el modelo de seguridad de la información propuesto permitirá reforzar las bases para enfrentar un escenario caracterizado por la incertidumbre y riesgos emergentes de seguridad de la información.

VII. Recomendaciones

La pandemia de la COVID-19 es uno de los eventos más transformacionales en la historia de la humanidad y los retos que trae consigo ha acelerado de manera exponencial la transformación digital y la superficie de potenciales riesgos cibernéticos, por lo que se hace imperativo implementar un programa de seguridad de la información y ciberseguridad más robusto y que permita enfrentar los riesgos asociados a la misma, de la mano con la urgente implementación de nuevos controles de seguridad.

El modelo de seguridad de la información del presente proyecto ha permitido identificar y dimensionar riesgos de seguridad de la información y ciberseguridad para tecnologías de la operación (procesos industriales), sin embargo, estas resultarán insuficientes para enfrentar los actuales escenarios de incertidumbre, por lo que, se recomienda desplegar esfuerzos para lograr una certificación ISO 27001, ello con el propósito de fortalecer la confianza de los clientes y stakeholders.

Proteger los activos de información requieren de una correcta sincronización entre el presupuesto y las necesidades identificadas para dicho propósito, es decir, se debe asignar mayores recursos financieros para dotar de mejores controles y estrategias de seguridad, que permitan reforzar las defensas de seguridad de la información y ciberseguridad. Por ello se hace necesario un cambio de paradigma para invertir en proveer de los recursos necesarios para proteger los principales activos de la informacion de la organización.

Existen barreras en la comunicación hacia la Alta Dirección que deben ser superadas, es decir se debe articular los riesgos de seguridad de la información en términos comerciales, reconociéndose los impactos financieros y reputacionales por una afectación a la confidencialidad, integridad y disponibilidad de los activos de información más relevantes de la organización. El lenguaje de comunicación a usar debe contener menos tecnicismos, para que la Alta Dirección vislumbre mejor los riesgos hacia el negocio.

VIII. Referencias

[1] S. d. M. y. Valores, «Superintendencia de Mercado y Valores,» 02 11 2018. [En línea]. Available: http://www.smv.gob.pe/.

[2] A. S. M. Balseca, «Diseño del modelo de gestión de seguridad de la información del». Ecuador Enero 2014.

[3] C. A. C. O. y. otros, «Desarrollo de un SGSI para los Colegios Profesionales en la Región Lambayeque. Caso de estudio : Colegio de Ingenieros». Perú - Lambayeque 2015.

[4] J. C. R. Medina, «Modelo de gestión de seguridad de la información para el E-Gobierno». Perú - Lima Mayo 2016.

[5] C. R. López, «Diseño de un framework para el gobierno de información con base en COBIT». Colombia Abril 2016.

[6] J. G. S. Souza, «Análisis de tratamiento de seguridad de la información». Brasil Abril 2017.

[7] D. F. J. Pérez, «Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del cliente TGE de la empresa Assurance ControlTech». Colombia - Bogotá 2017.

[8] C. E. A. Araujo, «Propuesta de implantación del Cyber Security Framework (CSF) del NIST, usando COBIT en Honda del Perú». Perú - Lima Julio 2017.

[9] M. Á. C. D. y. otros, «Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica MEDCAM PERÚ SAC». Perú - Lima 2017.

[10] J. E. B. L. y. otros, «Análisis de la preparación de las organizaciones». Perú - Lima 18 Julio 2018.

[11] ISACA, «COBIT 5 para seguridad de la información». EEUU. (Rollings Meadows) 2012.

[12] C. d. N. y. d. F. d. B. C. n. A. (INDECOPI), «TECNOLOGÍA DE LA INFORMACIÓN. NTP-ISO/IEC 27001: 2014 Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos».

[13] INDECOPI, «TECNOLOGÍA DE LA INFORMACIÓN- Técnicas de seguridad. Gestión del riesgo en la Seguridad de la información». 2013.

[14] ISACA, «COBIT 5».

[15] N. I. o. S. a. Technology.

[16] I. s. m. m. model, «ISM3». 2007.

IX. Anexos

Anexo 1: Reporte de incidencias de empresa editora 1

Reporte área Rotativa por productos impresos – Email informe de actividad de los procesos.	
OBJETIVOS: AREA ROTATIVA - Informar a las áreas y jefaturas los detalles de inicio y fin de producción e incidencias. AREA PRE-PRENSA - Email informativo sobre eventos en el proceso de producción.	**AÑO:** 2019
RESPONSABLE: Coordinador de rotativa. - Coordinador de pre-prensa	

Entrada Nº 04:

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	Nº PAGINAS:	Nº PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted]	Lambayeque	200000025124	24	24	596	28	9.65
Tiraje: 5,583	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	21:21	21:57	21:57		22:03	22:03	22:10
MATERIALES USADOS (PAPEL)							
FORMATO	TAMAÑO BOBINA	CANTIDAD DE BOBINAS	MARCA		OPERARIO SPLICER	CANT. ROT. EMPALME	CANT. ROT. PRODUC.
Tabloide	61	3	Resolute		José Bustamante Chiroque.	0	0

Entrada Nº 04:

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	Nº PAGINAS:	Nº PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted]	Depor	200000025125	24	24	549	25.8	1.50
Tiraje: 36,088	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	22:08	22:17	22:17		22:20	22:20	23:23
PARADAS DE IMPRESION							
INICIO	FIN	MOTIVO					TIPO
23:02	23:05	Parada x cambio de portada - Trujillo. (Aviso 40036846)					Redacción

Entrada Nº 05:

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	Nº PAGINAS:	Nº PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted]	[redacted]	200000025126	28	28	1,414	77.5	1.79
Tiraje: 77,545	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	22:24	22:37	23:23		23:42	23:42	01:40
PARADAS DE IMPRESION							
INICIO	FIN	MOTIVO					TIPO
00:32	00:33	Parada x empalme Splicer 4. Aviso (40036847)					Mecánico
01:22	01:23	Parada x empalme Splicer 4. Aviso (40036847))					Mecánico
MATERIALES USADOS (PAPEL)							
FORMATO	TAMAÑO BOBINA	CANTIDAD DE BOBINAS	MARCA		OPERARIO SPLICER	CANT. ROT. EMPALME	CANT. ROT. PRODUC.
Tabloide	30.5	1	Resolute		José Bustamante Chiroque.	0	0
Tabloide	61.0	3	Resolute		José Bustamante Chiroque.	0	0

EMAIL DE INFORME AREA PRE-PRENSA

De: NORT Preprensa
Enviado el: martes, 01 de noviembre de 2016 11:01 p.m.
Para: NORT Mecánica <mecanica_norte@comercio.com.pe>; NORT Manrique Cely Hugo <hmanrique@comercio.com.pe>; NORT Electrónica <electronica_norte@comercio.com.pe>; NORT Rotativa <rotativa_norte@comercio.com.pe>; NORT Despacho <despacho_norte@comercio.com.pe>; NORT Carmona Pupuche Carlos Eduardo <carlos.carmona@comercio.com.pe>; NORT Preprensa <preprensa_norte@comercio.com.pe>
Asunto: ACTIVAR CONTINGENCIA FTP

Señores,
Se ha perdido la comunicación con el servidor arkitex de Lima, por favor activar la contingencia para recibir los archivos via FTP..

Saludos,

Atte,
Ricardo Nakano
Preprensa Norte

REPORTE AREA ROTATIVA FINALIZACION DE PRODUCCION

Entrada Nº 05

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	N° PAGINAS:	N° PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted]	Lambayeque	200000025142	24	24	212	10	3.65
Tiraje: 5,598	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	21:49	22:04	00:02		00:12	00:12	00:23

MATERIALES USADOS (PAPEL)

FORMATO	TAMAÑO BOBINA	CANTIDAD DE BOBINAS	MARCA	OPERARIO SPLICER	CANT. ROT. EMPALME	CANT. ROT. PRODUC.
Tabloide	61	3	Resolute	Christian Rivera Cubas	0	0

Entrada Nº 07

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	N° PAGINAS:	N° PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted] GESTION	[redacted] N	200000025143	32	32	511	32	26.12
Tiraje: 1,445	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	21:06	22:14	00:23		00:40	00:40	00:43

MATERIALES USADOS (PAPEL)

FORMATO	TAMAÑO BOBINA	CANTIDAD DE BOBINAS	MARCA	OPERARIO SPLICER	CANT. ROT. EMPALME	CANT. ROT. PRODUC.
Tabloide	61	4	BIOBIO	Christian Rivera Cubas	0	0

Entrada Nº 08

PRODUCTO:	SECCION:	ORDEN DE PRODUCCIÓN:	N° PAGINAS:	N° PÁG. COLOR:	MACULATURA UND.	MACULATURA KILOS	% MACULATURA
[redacted] El Comercio	A	200000025144	32	32	1,971	174.5	44.52
Tiraje: 2,456	CIERRE REDACCIÓN	ENTREGA PLACAS	INICIO AJUSTE		FIN AJUSTE	INICIO PRODUCCIÓN	FIN PRODUCCIÓN
	22:31	23:20	00:43		03:16	03:16	03:22

PARADAS DE IMPRESIÓN

INICIO	FIN	MOTIVO	TIPO
01:23	03:16	Parada por problemas con el servidor arkitex (Preprensa)	Mecánica

MATERIALES USADOS (PAPEL)

FORMATO	TAMAÑ	CANTIDAD DE BOBINAS	MARCA	OPERARIO SPLICER	CANT. ROT. EMPALME	CANT. ROT. PRODUC.
Berlinés	88	2	Resolute	Christian Rivera Cubas	0	0
Berlinés	44	1	Resolute	Christian Rivera Cubas	0	0

(Ctrl)

DESCRIPCION:

- El primer grafico muestra un reporte emitido por el área de rotativa donde informa los detalles del `proceso de impresión de un producto como el tiraje, maculatura, inicio y fin de producción, incidencias, etc.
- El grafico 02 muestra un email evidenciando la indisponibilidad de un servicio o sistema editorial que soporta el flujo de las páginas de los diarios.
- El tercer grafico evidencia un reporte caracterizado por el evento crítico y cuya repercusión influyo en el tiempo de finalización de impresión de los diarios.

CONCLUSION:

- El anexo sustenta una de las problemáticas descritas en la investigación y evidencia la necesidad de formular estrategias que mitiguen el impacto de la indisponibilidad del servicio Arkitex.

Anexo 2. Análisis estadísticos del cuestionario aplicado

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A	B	C	D	E
Elaboración de políticas de seguridad de la información	Aplicación de políticas de seguridad de la información	Hacer de conocimiento al personal las políticas de seguridad de la información	Realizar y actualizaciones constantes de las políticas de seguridad de la información	Políticas de seguridad de la información están basadas en algún estándar nacional o internacional
67%	0%	0%	0%	67%

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A	B	C	D	E	F	G
Persona asignada para labores exclusivas de seguridad de la información	Formalización dentro del organigrama del área de seguridad de la información	Comité de seguridad de la información a nivel de alta dirección	Asesoramiento especializado en materia de seguridad de la información	Mecanismo de cooperación con organizaciones públicas o privadas referidas a seguridad de la información	Evaluaciones de seguridad de la información a través de entidades públicas o privadas	Requerimiento de seguridad de la información al realizar contratos con empresas externas
0%	0%	0%	0%	0%	0%	0%

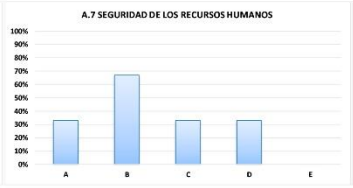
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

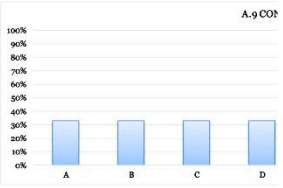
A	B	C	D	E
Preparación de usuario a reportar incidentes de seguridad de los sistemas de información	Acuerdos con el personal sobre la confidencialidad de la información	Capacitación actualizada a usuarios en temas de seguridad de la información	Procedimientos de respuesta a incidentes y anomalías en materia de seguridad de la información para aplicar a usuarios	Guía que establezca expectativas de seguridad del rol de empleados, contratistas, y terceros
33%	67%	33%	33%	0%

A.8 GESTIÓN DE ACTIVOS

A	B	C	D
Clasificación de activos informáticos (hardware, software)	Automatización de activos informáticos mediante un sistema software	Actualización de inventario de activos informáticos	Actualización de etiquetas (nombres de contenidos, fechas, ubicación, versiones y responsables de activos)
100%	0%	33%	0%

A	B	C	D
Políticas de control de acceso a los sistemas informáticos de usuarios en la red de datos	Aplicación de políticas de control de acceso a los sistemas informáticos de usuarios en la red de datos.	Registro permanente a los sistemas informáticos de usuarios en la red de datos	Administración de los privilegios para acceder a los sistemas informáticos
33%	33%	33%	33%





A.9 CONTROL DE ACCESO

E	F	G	H	I	J	K
Administración de contraseñas de usuarios a los sistemas informáticos	Políticas de uso de los servicios de la red de datos	Establecimiento de mecanismos de autenticación de usuarios para los conexiones externas a la red de datos	Establecimiento de horarios para conexiones externas a la red de datos	Asignación de sistemas informáticos críticos del personal no autorizado	Mecanismos de monitoreo del uso de los sistemas informáticos	Establecimiento de controles de seguridad informática para usuarios que usen computadores portátiles
33%	33%	0%	0%	0%	0%	0%

A.10 CRIPTOGRAFÍA

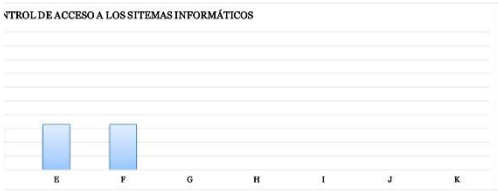
A	B
Políticas sobre uso de controles criptográficos	Gestión de claves criptográficas
0%	0%

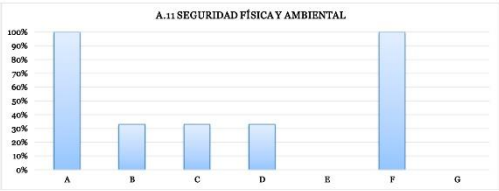
A.11 SEGURIDAD FÍSICA Y AMBIENTAL

A	B	C	D	E	F	G
Identificación de áreas físicas seguras donde se encuentren los sistemas de información	Establecimiento de controles de ingreso de personal a las áreas físicas donde se encuentran los sistemas de información	Preparación para mantener el correcto funcionamiento del suministro eléctrico en caso de algunas falla	Preparación para mantener el correcto funcionamiento del cableado de datos en caso de algunas falla	Mecanismos de seguridad de la información para equipos que ingresan y salen de la organización	Mantenimiento periódico del hardware y software en los equipos informáticos	Técnicas que permiten que información de dispositivos de almacenamiento con data sensible no sea recuperable
100%	33%	33%	33%	0%	100%	0%

A.12 SEGURIDAD EN LAS OPERACIONES

A	B	C	D	E	F	G	H	I
Procedimientos y responsabilidades operativos del uso y acceso a los sistemas informáticos	Documentación de los procedimientos operativos del uso y acceso de los sistemas informáticos	Procedimientos para reportar incidentes de las comunicaciones de datos y operaciones de los sistemas informáticos	establecidos controles en la red de datos contra software malicioso (antivirus, antispyware, etc)	Registro de acceso y uso de las aplicaciones y servicios de la red de datos del personal operativo	Registro de fallo de las comunicaciones de datos	Control documentado de toda la información referida a la red de datos	Mecanismos de seguridad para proteger la documentación de los sistemas de información	Controles de seguridad de los medios de almacenamiento de información en tránsito
0%	0%	0%	33%	0%	0%	0%	0%	0%





Anexo 3: Validación del Instrumento

CONSTANCIA DE VALIDACION DEL INSTRUMENTO APLICADO PARA LA APLICACIÓN DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE

Quien suscribe, **OLGA NAYDA DE LA CRUZ SANCHEZ**, con documento de identidad N° **40239681**, de profesión **Estadística**, con grado de **Licenciada**.

Por medio de la presente hago constar que he revisado con fines de Validación el instrumento (encuesta), a los efectos de su aplicación en las empresas de editoras de la Región Lambayeque.

Luego de haber aplicado la prueba de confiabilidad KR20 de Kuder de Richarson, se obtuvo que la confiabilidad del instrumento es muy alta, obteniendo como resultado 0.98; es decir, el 98% de confiabilidad de que el instrumento es aceptable.

Se aplicó la siguiente fórmula:

$$KR20 = \frac{k}{k-1}\left[\frac{S^2T(aciertos) - \sum p * q(aciertos)}{S^2T(aciertos)}\right]$$

Donde:

$k = 73$	: Número	de Ítems
$\sum p * q = 5.33$	: Sumatoria	de proporciones de aciertos por desaciertos
$S^2T = 148$	: Varianza	total de aciertos.

Por lo expuesto, se puede confirmar que el instrumento tiene relación entre sus Ítems, comprensión en su contenido y claridad en su redacción.

Fecha: 29 de enero de 2018

DNI N°40239681

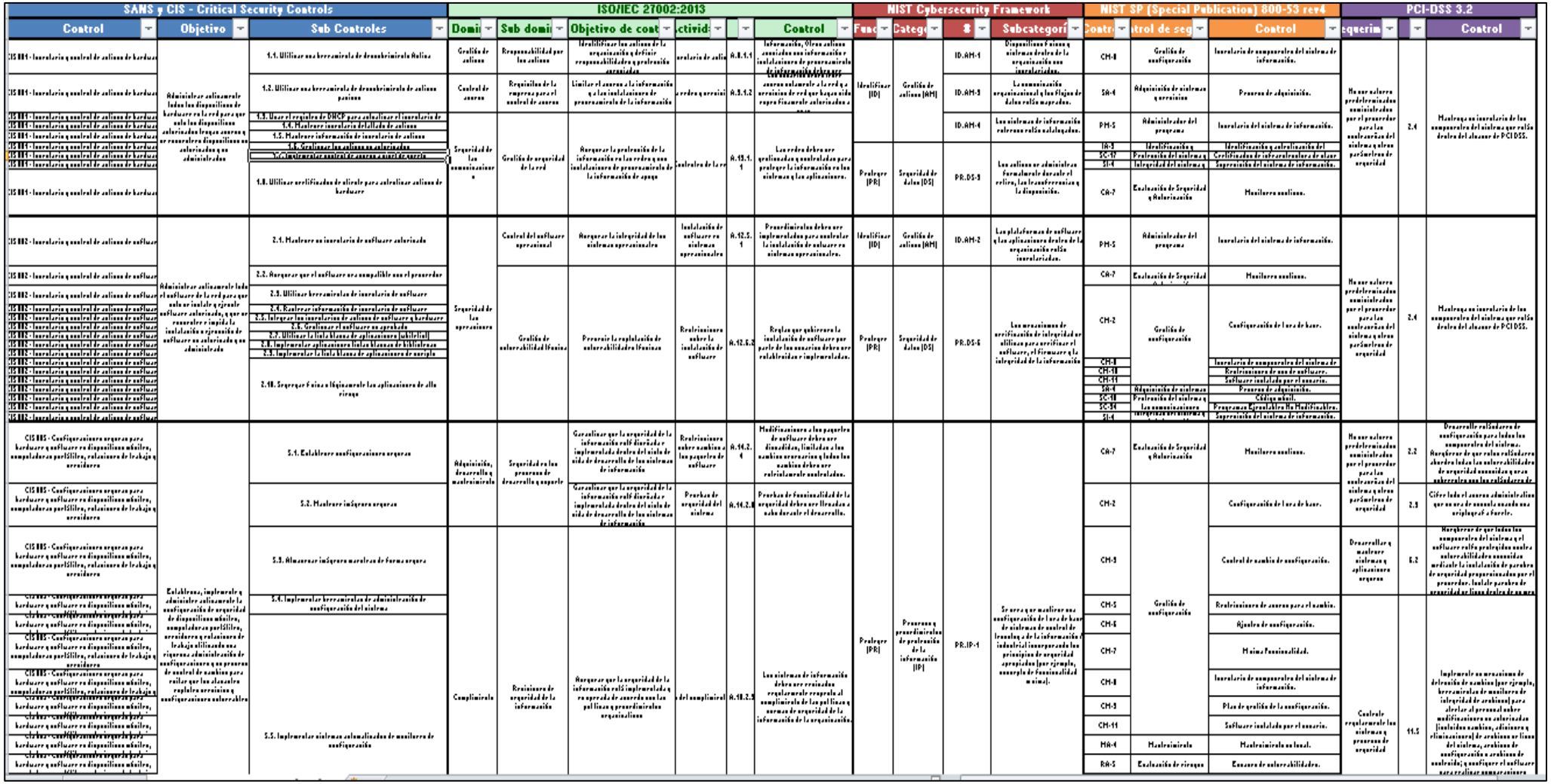
Anexo 4: Matriz de valoración de Normas, Estándares y Marcos de Trabajo de Seguridad de la Información

Ciclo de Deming - PDCA	NIST Cybersecurity Framework		ISO/IEC 27001:2013			Cobit 5 para Seguridad de la Información		ISO/IEC 27032:2012		
	Fases	Descripción	Fases	Sub fase	Descripción	Fases	Descripción	Fase	Sub fase	Descripción
Plan	I - Priorizar y Alcance	La organización identifica sus objetivos de negocio / misión y las prioridades de alto nivel. Con estos resultados se adopta decisiones estrategicas respecto a las implementaciones de ciberseguridad y determina el Alcance de los sistemas y activos que dan soporte al proceso o linea de negocio seleccionado. El marco de referencia puede ser adaptado para brindar soporte a las diferentes linea de negocio o procesos dentro de la organización, el cual puede tener diferentes necesidades de negocio y tolerancia a los riesgos asociados.	I - Establecimiento	1.1 Contexto y comprensión de la organización	Esta fase de compone de cuatro capitulos de la norma, donde se realiza un entendimiemto de la organización y su contexto, estudio de los procesos que serán abordados, la determinación del Alcance del SGSI, las partes interesadas, el compromiso de la Alta dirección, el establecimiento de planes de capacitación y la metodologia de riesgos a utilizarse, todos ellos en su conjunto generarán entregables o documentos de cumplimiento a la norma.	1. Reconocer la necesidad de actuar	El propósito de la fase es comprender la amplitud y profundidad de los cambios previstos, las diversas partes interesadas que están afectadas, la naturaleza del impacto y la participación de cada grupo de partes interesadas, así como la preparación y capacidad de adaptarse al cambio. Esta responde a la pregunta: ¿Cuales son los motivos? La fase 1 identifica los motivadores actuales de cambio y crea, a nivel de dirección ejecutiva, un deseo de cambio que entonces es expresado en un esquema de caso de negocio	- Establecimient	1.1 Comprensión de la organización	Objetivos principales: Comprender la organización y su entorno, reunir la información necesaria para planificar la implementación del programa de ciberseguridad, asegurarse de que los objetivos de la ciberseguridad esten alineados con los objetivos de negocio de la organización. La dificultad de esta etapa es comprender con exactitud como esta estructurada la organización internamente y la forma en que se situa en su ambiente externo. Reune toda la información necesaria, que es un requisito previo para la realización del análisis de brecha entre el sistema actual y el deseado. El analisis puede ser un resumen, no hay necesidad de un analisis completo de la organización.
				1.2 Liderazgo						
				1.3 Planeación						
	II - Orientar	Basado en los resultados de la fase anterior donde se determino el Alcance del programa de ciberseguridad, la organización identifica los sistema y activos relacionados, los requisitos regulatorios y el enfoque integral de riesgo. Luego se identifica las amenazas y vulnerabilidades de dichos sistemas y activos.		1.4 Soporte		2. Revisar el estado actual	La Fase está enfocada en definir el alcance de la iniciativa de implementación o mejora. Un diagnóstico a alto-nivel puede ser de utilidad para determinar el alcance y conocer las áreas de mayor prioridad en las cuales enfocarse. Se realiza entonces una evaluación del estado actual de cada fase, y se identifican cuestiones o deficiencias a través de una evaluación de capacidades de procesos. Las iniciativas de gran escala deben ser estructuradas como interacciones múltiples del ciclo de vida. Para cualquier iniciativa de implantación que exceda los 6 meses, existirá un riesgo de perder el impulso, el foco y la aceptación de los grupos de interés. Esta fase responde a la pregunta: ¿Donde estamos ahora? La fase 2 alinea los objetivos relacionados con TI con la estrategia de la empresa y el riesgo y prioriza los principales objetivos de la empresa, los objetivos relacionados con TI y los procesos. Dados los objetivos de la empresa y de TI seleccionados, se identifican los procesos críticos que se necesitan para asegurar resultados exitosos.		1.2 Liderazgo	+
	III - Crear un perfil actual	La organización desarrolla un perfil actual, indicando los resultados de categorias y subcategorias del nucleo central del Marco de Referencia (Core) y que se encuentran definidos en la literatura del framework.		1.4.1 Diseño de Plan de Capacitación y Concientización		3. Definir el estado objetivo	Durante la Fase 3, se fija un objetivo de mejora, acompañado de un análisis más detallado utilizando esta publicación y otras guías (ver sección III, 2.2 Creando el Entorno Apropiado) para identificar desajustes y posibles soluciones. Algunas soluciones pueden ser ganancias rápidas y otras, actividades más retadores y a más largo plazo. La prioridad debe ser dada a las iniciativas que sean más sencillas de conseguir y aquellas que probablemente rindan los mayores beneficios. La fase responde a la pregunta: ¿Donde queremos ir? La fase 3 establece los objetivos de mejora seguidos por un análisis comparativo para identificar las potenciales soluciones. Algunas soluciones serán fácilmente aplicables y otros serán un reto, tareas a largo plazo.		1.3 Politica	Objetivos principales: Comunicar formalmente las intenciones y dirección general de la organización. Proveer a la ciberseguridad, orientación y apoyo de la dirección, de acuerdo con los requerimientos del negocio, leyes y reglamentos aplicables. Mejorar la concienciación de la organización respecto de la ciberseguridad. Basicamente la politica se identifica comunmente como la expresión formal de las normas de conducta aplicables dentro de la organización. Esta puede ser la politica General de alto nivel, politicas de alto nivel relacionadas con un tema especifico o politicas detalladas.
	IV - Evaluación de riesgos	La evaluación podria guiarse mediante el proceso de gestión integral de riesgo de la organización. La organización analiza el entorno operacional a fin de discernir la probabilidad de ocurrencia de un evento de ciberseguridad y el impacto que dicho evento podria tener en la organización. Es necesario buscar incorporar los datos de riesgos, amenazas y vulnerabilidades emergentes para facilitar una solida comprensión de la probabilidad de ocurrencia e impacto de los eventos de ciberseguridad.		1.4.2 Diseño del Plan de Comunicaciones		4. Construir mejoras	La Fase 4 planea soluciones prácticas definiendo proyectos apoyados por casos de negocio justificables. También se desarrolla un plan de cambio para la implantación. Un caso de negocio bien desarrollado ayuda a asegurar que los beneficios del proyecto son identificados y controlados. Se pueden definir y supervisar medidas usando los objetivos y métricas de COBIT 5 Seguridad de la Información para asegurar que la alineación con el negocio está garantizada y mantenida y el rendimiento pueden ser medido. La fase responde a la pregunta: ¿Que es preciso hacer? La fase 4 consiste en soluciones prácticas y viables mediante la definición de proyectos apoyados por casos de negocios justificables y el desarrollo de un plan de cambio para la implementación.		1.4 Gestión de riesgos	Objetivos principales: Seleccionar y definir un enfoque para la evaluación de riesgos que este alineado con la dirección de la organización. Seleccionar y definir una metodologia de evaluación de riesgos adaptada a las necesidades de la organización. Identificar, analizar y evaluar el riesgo de incidentes disruptivos para la organización. La gestión de riesgos de ciberseguridad es la gestión de los riesgos cibernéticos hasta alcanzar un nivel aceptable.
	V - Crear un perfil objetivo	La organización crea un perfil objetivo que se centra en la evaluación de las categorias y subcategorias del Marco de Referencia donde se describe los resultados de ciberseguridad deseados. Tambien se puede desarrollar categorias o subcategorias particulares para considerar riesgos particulares en la organización. Tambien se puede considerar las influencias y requisitos de las partes interesadas externas como las entidades del sector, clientes y socios de negocio al momento de crear un perfil objetivo.		1.4.3 Diseño de la gestión de la documentación						

DO	**VI - Determinar, analizar y priorizar las brechas**	La organización compara el perfil actual y el perfil objetivo a fin de determinar las brechas. Con esta base se diseña un plan de acción priorizado para tratar aquellas brechas respecto de lo definido por los impulsores de la misión, analisis de costo / beneficio y la compresión de los riesgos para alcanzar los resultados del perfil objetivo. Posteriormente la organización determina los recursos necesarios para tratar las brechas. Al tratar los perfiles de esta manera es posible tomar decisiones informadas acerca de las actividades de ciberseguridad con soporte a la gestión de riesgos y realizar mejoras debidamente orientadas y rentables.	**II - Implementación y Operación**	1.5 Operación	Se realiza una evaluación y gestión de riesgos de seguridad de la información, ejecutandose las medidas de control definidas y reevaluando cada periodo de tiempo ante posibles cambios en los mismos riesgos.	**5. Implantar mejoras**	La Fase 5 implementa las soluciones propuestas en prácticas del día a día. Para tener éxito, es necesario el compromiso y la demostrada implicación del equipo de alta dirección, así como la toma de propiedad por las partes afectadas del negocio y las partes interesadas de TI. Esta fase responde a la pregunta: ¿Como conseguiremos llegar? a fase 5 prevé la implementación de la solución propuesta en las prácticas del día a día y el establecimiento de medidas y sistemas de supervisión para asegurar que se consigue la alineación con el negocio y que el rendimiento puede ser medido.	**II - Implementación y operación**	2.1 Mecanismos de ataque	El objetivo de esta etapa es explicar las ciberamenazas y vectores de mitigación de ataques basados en la web, aplicaciones web, redes zombies, denegación de servicio, amenaza interna, phishing, mitigación de spam, kit de herramientas de explotación, fuga de información, ciberespionaje, etc
										2.2 Controles de ciberseguridad	El objetivo de la etapa es definir controles de ciberseguridad. Para cada situación de riesgo de ciberseguridad identificada, se deberá seleccionar e implementar los controles que correspondan y que soportan los requisitos de seguridad. Estos controles se clasifican en controles de nivel de aplicación, creación de un sistema de servidor seguro, controles de usuario final
										2.3 Intercambio de información y coordinación	Los objetivos principales de la etapa es definir los pasos para el intercambio de información y coordinación. Identificar todas las partes involucradas, definir los roles y responsabilidades de las partes involucradas. Establecer las politicas. Identificar los estandares y sistemas técnicos y realizar prurbas de manera regular. La ISO 27032 en su cláusula 13.1 menciona que los incidentes de ciberseguridad a menudo cruzan las fronteras geograficas y organizacionales, y la velocidad de flujo de información y los cambios de incidentes de despliegue con frecuencia dejan un tiempo limitado para actuar, por ello es
										2.4 Programa de capacitación y concientización	La etapa busca garantizar la competencia de los involucrados en las operaciones del programa de ciberseguridad, concientizar a los actores de la organización sobre los desafios de la gestión de la ciberseguridad y garantizar la adopción de comportamientos deseados en ese campo. Se busca informar a los interesados de la organización acerca de las acciones, mejoras, cambios relacionados al programa
										2.5 Continuidad de negocio	La etapa busca proporcionar un marco de referencia eficaz, aplicable, predefinido y documentado. Se establece un proceso para permitir la gestión de la continuidad de negocio, abordando los procesos y actividades críticas de
										2.6 Gestión de incidentes de ciberseguridad	Se encarga de asegurar de que los eventos de ciberseguridad son debidamente detectados e identificados. Se busca reducir el posible impacto de los incidentes sobre las operaciones de la organización. Se mejora los controles de seguridad de la organización utilizando diferentes herramientas y técnicas
										2.7 Recuperación y respuesta a incidentes de ciberseguridad	La etapa aborda la respuesta a incidentes de ciberseguridad y su recuperación, se identifican recursos externos a fin de responder al incidente, se implementa análisis forense y se identifica las lecciones aprendidas.

CHECK	**VII - Implementar un plan de acción, monitoreo y revisión**	La organización determina que acciones se deben tomar en cuanto a las brechas identificadas en la fase anterior, luego se supervisa sus actuales practicas de ciberseguridad contra el perfil objetivo. Para mayor orientación, el Marco de Referencia identifica referencias normativas de ejemplo relacionadas con las categorias y subcategorias. Se debe determinar que normas, guias y prácticas funcionan mejor para sus necesidades. Se deberá repetir los pasos necesarios para evaluar y mejorar de manera continua la ciberseguridad de la organización. Se evaluara el grado de cumplimiento de los controles, acciones y tareas, por lo que se dará seguimiento y reevaluar mejoras en los controles e identificación de nuevos riesgos para la mejora continua.	**III - Monitoreo y Revisión**	3.1 Evaluación del desempeño	Se revisan el grado de cumplimiemto de los controles, se gestionan indicadores y el grado de efectividad del plan de acción. Ejecución de Auditorias internas y se diseñan planes de mejora.	**6. Operar y medir**	La Fase 6 se focaliza en la sostenibilidad de las operaciones de los nuevos o mejorados catalizadores y la supervisión de la consecución de los beneficios esperados. En otras palabras, esta fase sirve para determinar si los objetivos se han alcanzado y son sostenibles. Esta fase responde a la pregunta: ¿Hemos conseguido llegar? La fase 6 se centra en la transición sostenible de las prácticas de gobierno y de gestión mejoradas a las operaciones comerciales cotidianas así como la supervisión de las mejoras a través de las métricas de rendimiento y los beneficios esperados.	**III - Evaluación del desempeño**	3.1 Pruebas en ciberseguridad	Esta etapa busca garantizar la eficacia de los planes y procedimientos de la continuidad de ciberseguridad. Se despliegan actividades como prueba de los controles de seguridad, prueba de sistemas, pruebas de integración, documentación de resultados de las pruebas, etc
										2 Medición del desempe	En esta etapa se mide el desempeño de la ciberseguridad y se evalua la eficacia de los procesos y procedimientos implementados. En la cláusula 9.1 de la norma: Supervisión, medición, ánalisis y evaluación, se establece que la organización deberá determinar lo que debe ser objeto de seguimiento y medición, incluidos procesos y controles de seguridad de la información. Se estipula que se debe determinar cuando deberan ser llevados a cabo el
ACT			**IV - Mantenimiento y mejora**	1.7 Mejora	Registro, seguimiento y ejecución/implementación de las acciones correctivas y oportunidades de mejora del SGSI Se analizan y se evaluan metricas Se levantan observaciones por	**7. Supervisar y evaluar**	Durante la Fase 7, se revisa el éxito en conjunto de la iniciativa, se identifican requerimientos adicionales para la seguridad de la información de la empresa, y se refuerza la necesidad de mejora continua. Con el tiempo, el ciclo de vida debe ser seguido de forma iterativa mientras se construye un acercamiento sostenible a la seguridad de la información. La fase responde a la pregunta: ¿Como nos mantenemos? La fase 7 examina el éxito global de la iniciativa, identifica requisitos adicionales para el gobierno o la gestión y refuerza la necesidad de las mejoras continuas	**IV - Mantenimiento y mejora**	4.1 Mejora Continua	Esta etapa tiene por objetivo mejorar continuamente la eficacia de la ciberseguridad, asegurando que los objetivos de la ciberseguridad se mantienen alineados con los objetivos de negocio de la organización. Se garantiza que los planes y procedimientos son continuamente actualizados en relación de la continuidad de negocio.

Anexo 5: Matriz de valoración de Controles de Seguridad y Estándares de Seguridad de la Información



Anexo 6: Análisis del Contexto y partes interesadas (el anexo es declarado en la tabla 5 plantilla de análisis de contexto y partes interesada de la fase 1 del modelo).

LOGO	**ANÁLISIS DEL CONTEXTO Y PARTES INTERESADAS**		Empresa editora1
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO: **MSI-001**	VERSIÓN:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Elaborado por:

Revisado por:

Aprobado por:

1. Objetivo

Identificar los factores internos, externos y las necesidades expectativas de las partes interesadas que son relevantes y que pueden afectar a la capacidad de lograr los resultados deseados del Modelo de Seguridad de la Información de la organización.

2. Alcance

El presente análisis tiene como alcance la definición de los factores internos y externos que influyen en la seguridad de la información en la empresa editora 1.

Procesos del alcance	Nivel de importancia	Priorización	Alcance del Modelo
Gestión Operativa de Planta	15	35	x
Gestión Editorial	15	38	x

Sistemas de Información. Los sistemas de información reúnen y procesan datos de diferentes actividades y para el Modelo de Seguridad de la Información de editora 1, la inclusión de estos se da contemplando la información que proveen las actividades con las cuáles se relacionan a continuación:

Sistemas de Información.

Sistema DSS	Sistema HMI	Sistema SAP	Sistemas Arkitex
Control de agua	Rotativa	Rotativa	Redacción
Control de presión en Rotativa	Pre-prensa	Despacho	Pre-prensa
Transporte de tinta	Despacho	Pre-prensa	Rotativa
Control de Torres			
Control de transportadora			

Análisis Externo. De acuerdo con el análisis externo se ha identificado las siguientes áreas y ellos interactúan con los diferentes proveedores realizando diferentes actividades.

Cuadro definición del Contexto Externo

Área	Proveedor	Actividad
Sistemas	Telefónica	Internet, celular
	Level 3	Contingencia enlaces comunicaciones
	SolarWinds	Monitoreo de redes
	Symantec	Antivirus
	Cisco	Abastecimiento de equipos

Electrónica	Siel Electric	Implementación sistemas SCADA y PLC
Rotativa	SolTrack	Proveedor de lubricantes
	Ferreyros	Mantenimiento maquinaria pesada
	rockwell	Sistemas de automatización
	Schneider Electric	Sistemas de automatización

ANALISIS FODA

FORTALEZA

Infraestructura y capacidad adecuada.
Solida estrategia para la mejora de los procesos.
Liderazgo reconocido a nivel nacional en: reputación, imparcialidad, objetividad, responsabilidad.
Alto potencial de creación de nuevos productos.
Sedes y plantas en principales ciudades del país.

OPORTUNIDAD

Obtención de nuevas plantas de producción.
Continuidad del convenio de gracia tributaria editoras.
Reglas claras para reinversión de utilidades.
Escenario propicio para potenciar la transformación digital y creación de nuevos negocios de e-comerse.
Adquisición de otros diarios.

DEBILIDADES

Dependencia de proveedores especializados en el abastecimiento de insumos, repuestos y asistencia.
Activos de información críticos no identificados.
Falta de concientización y capacitación en seguridad de la información.

AMENAZAS

Desarrollo de nuevos productos en medios escritos y digitales.
Prensa “amarilla”.
Vandalismo hacia las sedes y plantas de producción.
Tendencia de consumo de productos digitales.
Inestabilidad política y social.

Partes interesadas. En la siguiente tabla, se muestra la lista de grupos de interés, así como los medios de involucramiento y sus principales expectativas.

Partes interesadas del Modelo de Seguridad de la Información.

Grupos de interés	Medios de involucramiento	Principales expectativas
Accionistas	Informes trimestrales y anuales. Reuniones trimestrales	Mantener una excelente reputación en el mercado financiero
AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES (MINJUS)	Normas y reglamentos. Resoluciones. Correo electrónico. Web del MINJUS. Archivos diversos.	Protección de los datos personales de la organización. Requisitos de la Ley 29733 y su Reglamento. Medidas de Seguridad Jurídica, Organizativa y Técnica de la Directiva de Seguridad.
AFP, ONP Y BANCOS	Correo electrónico. Web institucional.	Protección de datos de planillas y de los trabajadores. Pago de los derechos previsionales y haberes de los trabajadores.

Anexo 7: Alcance del Modelo de Seguridad de la Información (el anexo es declarado en la tabla 6).

<table>
<tr><td rowspan="4">LOGO</td><td colspan="2">ALCANCE DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN</td><td rowspan="4">Empresa editora1</td></tr>
<tr><td colspan="2">MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS</td></tr>
<tr><td>CÓDIGO: MSI-002</td><td>VERSIÓN:</td></tr>
<tr><td>FECHA DE ELABORACIÓN:</td><td>PÁGINA 1 DE</td></tr>
<tr><td colspan="4">Elaborado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Revisado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Aprobado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">1. Objetivo</td></tr>
<tr><td colspan="4">Establecer los límites y la aplicabilidad del modelo de seguridad de la información para definir su alcance.</td></tr>
<tr><td colspan="4">2. Alcance</td></tr>
<tr><td colspan="4">Aplica a toda la documentación y actividades dentro del modelo de seguridad de la información.</td></tr>
<tr><td colspan="4">3. Referencia normativa</td></tr>
<tr><td colspan="4">Aplica a toda la documentación y actividades dentro del modelo de seguridad de la información.</td></tr>
<tr><td colspan="4">Definición del alcance</td></tr>
</table>

• La organización define a través del presente apartado de alcance del modelo de seguridad de la información, los límites pertinentes en el que decide qué información requieren proteger.
• La información deberá ser protegida independientemente si es almacenada, procesada o transferida dentro o fuera del alcance del modelo de seguridad de la información.

Tomando en cuenta los requisitos legales, normativos, contractuales, las necesidades y expectativas de

las partes interesadas y de otra índole, se define el alcance del modelo de seguridad de la información

en las siguientes instancias operativas del negocio:

Empresa editora. Guía elaboración":

- Gestión operativa.
- Gestión editorial.

Organización

En función de los procesos y subprocesos del alcance del modelo de seguridad de la información, se definen las unidades organizacionales correspondientes a los procesos y subprocesos antes mencionados, los mismos que se muestran en el Gráfico 1.

Gráfico 1 – Organigrama de Alto Nivel del Alcance el modelo de seguridad de la información de <nombre empresa>

<inserte el organigrama aquí…> "Empresa editora. Guía elaboración"

Ubicación geográfica

Describir dirección es oficinas centrales, instalaciones de proceso, sucursales, etc.

Sistemas y servicios de tecnología de información

El alcance a nivel de sistemas y servicios de tecnología de información está dado de acuerdo con lo siguiente:

UBICACÓN	NOMBRE	CÓDIGO DATA CENTER	FUNCIÓN
Planta norte	Telefónica SA	TLM	Otorga servicios de red y aplicaciones
Planta norte	Sala de servidores 0	SRV0	Otorga servicios de red y de aplicaciones
Planta norte	Sala de servidores 1	SRV1	Otorga servicios de red y de aplicaciones

Exclusiones del alcance

Se excluyen del alcance del modelo de seguridad de la información los procesos en los que el nivel de importancia de acuerdo con el CID (Confidencialidad, Integridad y Disponibilidad) y del impacto al negocio no es significativo y no resulta de prioridad para los responsables del negocio.

Anexo 8: Política de Seguridad de la Información (el anexo es declarado en la tabla 7).

<table>
<tr><td rowspan="4">LOGO</td><td colspan="2">POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</td><td rowspan="4">Empresa editora1</td></tr>
<tr><td colspan="2">MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS</td></tr>
<tr><td>CÓDIGO: MSI-003</td><td>VERSIÓN:</td></tr>
<tr><td>FECHA DE ELABORACIÓN:</td><td>PÁGINA 1 DE</td></tr>
<tr><td colspan="4">Elaborado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Revisado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Aprobado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">1. Objetivo</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">2. Alcance</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">3. Referencia normativa</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Política de Seguridad de la Información</td></tr>
<tr><td colspan="4">Con la finalidad de proteger la información de los procesos de negocio, en cumplimiento con la normativa vigente y en línea con los objetivos estratégicos de la organización, el Gerente General en representación de los colaboradores, se compromete a:

• Establecer, implementar, operar, monitorear, mantener y mejorar un Modelo de Seguridad de la Información que permita administrar los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de la información.
• Mantener un Modelo de Seguridad de la Información, tomando en cuenta los objetivos y estrategias de la organización, los análisis internos y externos, y las necesidades y expectativas de las partes interesadas.
• Promover la concienciación y capacitación al personal y terceras partes para que contribuyan en el cumplimiento de lo establecido en las políticas y procedimientos de seguridad de la información.</td></tr>
</table>

Anexo 9: Matriz de Roles y Responsabilidades (el anexo es declarado en la tabla 9).

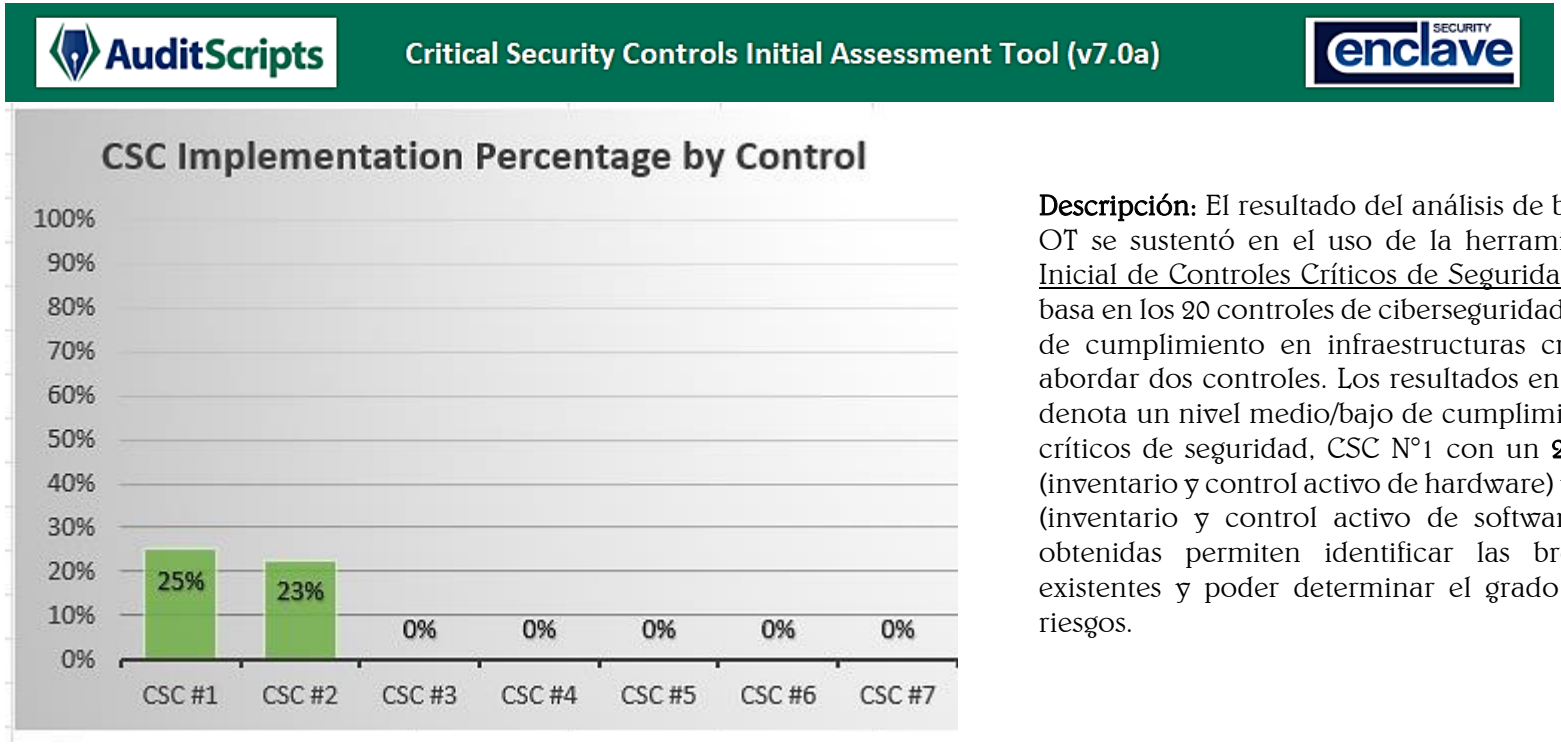
<table>
<tr><td rowspan="4">LOGO</td><td colspan="2">MATRIZ DE ROLES Y RESPONSABILIDADES</td><td rowspan="4">Empresa editora1</td></tr>
<tr><td colspan="2">MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS</td></tr>
<tr><td>CÓDIGO: MSI-004</td><td>VERSIÓN:</td></tr>
<tr><td>FECHA DE ELABORACIÓN:</td><td>PÁGINA 1 DE</td></tr>
<tr><td colspan="4">Elaborado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Revisado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Aprobado por:</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">1. Objetivo</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">2. Alcance</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">3. Referencia normativa</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Identificación de los responsables</td></tr>
<tr><td colspan="4">Se genera la necesidad de vincular de forma efectiva al personal que estará vinculado al proceso de desarrollo del modelo de seguridad de la información, para que su apoyo y/o gestión permita la planificación, implementación y operación del modelo de seguridad de la información.</td></tr>
<tr><td colspan="4">Definición de Roles y Responsabilidadesn del Modelo de Seguridad de la Información</td></tr>
<tr><td>ROL</td><td colspan="2">CARGO</td><td>RESPONSABILIDADES</td></tr>
<tr><td>Rol 1</td><td colspan="2">Cargo 1…</td><td>Responsabilidad 1</td></tr>
<tr><td>Rol 2</td><td colspan="2">Cargo 2…</td><td>Responsabilidad 2</td></tr>
<tr><td>Rol …</td><td colspan="2">Cargo 3…</td><td>Responsabilidad 3</td></tr>
</table>

Anexo 10: Análisis de Brechas en Tecnología de la Operación – OT.

Definición del estado actual con herramienta Critical Security Controls Initial Assessment Tool v7. 0

La herramienta está disponible por el Centro de Seguridad de Internet – CIS, actualmente es la responsable de diseñar, crear, mejorar y difundir los Controles Críticos de Seguridad para entornos OT.

Nivel de cumplimiento de los controles críticos de seguridad – OT



Fuente: Herramienta Centro de Seguridad de Internet - CIS

Descripción:

Descripción: El resultado del análisis de brechas en tecnología OT se sustentó en el uso de la herramienta de "Evaluación Inicial de Controles Críticos de Seguridad de AudiScripts". Se basa en los 20 controles de ciberseguridad para evaluar su nivel de cumplimiento en infraestructuras críticas. Se determinó abordar dos controles. Los resultados en la empresa editora 1 denota un nivel medio/bajo de cumplimiento en los controles críticos de seguridad, CSC N°1 con un **25%** de cumplimiento (inventario y control activo de hardware) y CSC N°2 con un **23%** (inventario y control activo de software). Las valoraciones obtenidas permiten identificar las brechas de seguridad existentes y poder determinar el grado de exposición a los riesgos.

Descripción y/o definiciones de los criterios que sustentan la evaluación de la herramienta respecto al nivel de cumplimiento.

Definiciones de campo	
ID	Este es el número de ID de la referencia de control de control de seguridad crítica específica que se incluye en la documentación de Controles de seguridad críticos.
Detalle crítico de control de seguridad	Este es el detalle detrás de cada sub-control específico como se define en la documentación de Controles de seguridad críticos.
Sensor o línea de base	Este es el tipo de sistema técnico o línea de base que creemos que es necesario para implementar el sub controlador específico.
Política aprobada	Esta pregunta determina si la organización tiene actualmente una política definida que indica que deben implementar el control secundario definido.
Control implementado	Esta pregunta determina si la organización actualmente ha implementado este control secundario y hasta qué punto se ha implementado el control.
Control automatizado	Esta pregunta determina si la organización actualmente ha automatizado o no la implementación de este control secundario y hasta qué punto se ha automatizado el control.
Control reportado al negocio	Esta pregunta determina si la organización está informando o no de este control secundario a los representantes comerciales y en qué medida se ha informado el control.

Análisis brecha CSC #1– Resultados de medición de cumplimiento.

ID	Critical Security Control Detail	NIST CSF	Sensor or Baseline	Policy Defined	Control Implemented
1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	Identify	Active Device Discovery System	No Policy	Not Implemented
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Identify	Passive Device Discovery System	No Policy	Not Implemented
1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	Identify	Log Management System / SIEM	No Policy	Not Implemented
1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Identify	Asset Inventory System	Partial Written Policy	Implemented on Some Systems
1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Identify	Asset Inventory System	Partial Written Policy	Implemented on Some Systems
1.6	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	Respond	Asset Inventory System	No Policy	Not Implemented
1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Protect	Network Level Authentication (NLA)	Partial Written Policy	Implemented on Some Systems
1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	Protect	Public Key Infrastruture (PKI)	Partial Written Policy	Implemented on Some Systems

Análisis brecha CSC #2 – Resultados de medición de cumplimiento.

ID	Critical Security Control Detail	NIST CSF	Sensor or Baseline	Policy Defined	Control Implemented
2.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	Identify	Software Application Inventory	Partial Written Policy	Implemented on Some Systems
2.2	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	Identify	Software Application Inventory	Partial Written Policy	Implemented on Some Systems
2.3	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	Identify	Software Application Inventory	Partial Written Policy	Implemented on Some Systems
2.4	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the	Identify	Software Application Inventory	Partial Written Policy	Implemented on Some Systems
2.5	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single	Identify	Software Application Inventory	No Policy	Not Implemented
2.6	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	Identify	Software Application Inventory	Informal Policy	Not Implemented
2.7	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	Protect	Software Whitelisting System	Partial Written Policy	Parts of Policy Implemented
2.8	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.	Protect	Software Whitelisting System	No Policy	Not Implemented
2.9	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.	Protect	Software Whitelisting System	No Policy	Not Implemented
2.10	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.	Protect	:work Firewall / Acess Control Syst	Informal Policy	Not Implemented

Anexo 11: Análisis de brechas basado en la norma ISO 27002.

LOGO	**ANÁLISIS DE BRECHAS ISO 27002**		Empresa editora1
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO:	VERSIÓN:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Elaborado por:
Revisado por:
Aprobado por:
1. Objetivo
2. Alcance
3. Referencia normativa
Descripción
Para la definición del Estado Actual de la tecnología IT, se utilizó la herramienta de Evaluación basado en la norma ISO 27002, la cual permitió tener un alcance inicial de Editora 1

Evaluación de cumplimiento de controles

No.	DOMINIO	Estado actual de cumplimiento	Estado de cumplimiento a mediano plazo	Estado de cumplimiento a largo plazo
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	60	80
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	0	40	80
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	20	40	80
A.8	GESTIÓN DE ACTIVOS	50	60	80
A.9	CONTROL DE ACCESO	36	60	80
A.10	CRIPTOGRAFÍA	0	40	80
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	43	60	80

A.12	SEGURIDAD DE LAS OPERACIONES	10	40	80
A.13	SEGURIDAD DE LAS COMUNICACIONES	33	60	80
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	70	80	85
A.15	RELACIONES CON LOS PROVEEDORES	25	40	80
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	67	80	85
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	80	85
A.18	CUMPLIMIENTO	60	80	85
PROMEDIO EVALUACIÓN DE CONTROLES		37	59	81

Anexo 12: Identificación de Activos de la Información.

LOGO	IDENTIFICACIÓN DE ACTIVOS		*<nombre de empresa>*
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO:	VERSION:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Proceso:

Tipo de Activo:

ID	Subproceso	Nombre del Activo	Descripción del Activo	Categoría del Activo	Subcategoría del Activo	Activo de Soporte Principal Relacionado	Ubicación Física	Ubicación Lógica	Usuario del Activo	Custodio	Propietario	Requerimientos Legales, Normativos y Contractuales	Clasificación	Nivel C	Valor C	Nivel I	Valor I	Nivel D	Valor D	Nivel L	Valor L	Nivel N	Valor N	Importancia Relativa
C001	Rotativa	Informacion de produccion.	Informacion relacionada al estado de la produccion, velocidades de maquina, niveles de tinta, consumo de papel, distribucion de fardos y calibraciones de torres de impresión.	Sistema OT	Información Operativa	Sistema Scada	Data center Level 3	N/A	Colaboradores de rotativa, despacho y electronica	Supervisor de rotativa	Gerente de planta Norte	Información Interna	Confidencial	Poco Sensible a la Divulgación (Público Restringido)	4	Sensible a la Modificación (Íntegro)	5	De Uso Frecuente (Crítico)	5	Basado en Política Interna	3	Táctico	3	4
C002	Preprensa	Informacion de indicadores de Arkitex	Valores del estado de desarrollo de los diarios	Sistema IT	Información Operativa	Sistema Arkitex	Data center Level 3	N/A	Personal preprensa y redaccion	Director periodistico	Gerente de operaciones	Información Interna	Confidencial	Poco Sensible a la Divulgación (Público Restringido)	5	Sensible a la Modificación (Íntegro)	5	De Uso Frecuente (Crítico)	5	Basado en Política Interna	3	Táctico	3	4,2

Anexo 13: Factor de Probabilidad.

Operaciones	Descripción de la Incertidumbre	Proyectos	Factor de Probabilidad
Teniendo en cuenta el sitio, y experiencia en el sector y las condiciones futuras esperadas, el evento de riesgo:		En base a experiencia en el sector y las condiciones futuras esperadas, con los estudios o proyectos similares, el riesgo:	
Podría ocurrir más de una vez en un año	Casi Cierto	Podría esperarse que ocurra más de una vez durante el estudio o entrega del proyecto.	**10**
Podría ocurrir durante el período presupuestario de 1 a 2 años	Probable	Podría fácilmente ocurrir y generalmente ha ocurrido en estudios o proyectos similares.	**3**
Podría ocurrir durante el período de Planificación Estratégica de 5 años.	Posible	Ha ocurrido en una minoría de estudios o proyectos similares.	**1**
Podría ocurrir durante el período de tiempo de 5 a 20 años.	Improbable	Se sabe que puede ocurrir, pero en raras ocasiones	**0.3**
Podría ocurrir durante el periodo de tiempo de 20 a 50 años.	Raro	No ha ocurrido en estudios o proyectos similares, pero podría.	**0.1**
Por una falla de sistema: • Esta consecuencia no ha ocurrido en la industria en los últimos 50 años. Por un peligro natural (terremoto, inundación, huracán, etc.): • El período de retorno previsto para un riesgo de esta fuerza / magnitud es uno en 100 años o más.	Muy Raro	Concebible, pero solo en circunstancias extremas.	**0.03**

Anexo 14: Análisis de riesgos / dimensiones con herramienta Bow Tie – Gestión Editorial.

Tipo	Seguridad de la Información
Clasificación	Negocio

Dueño	Gerente de Planta
Fecha (dd/mm/aaaa)	05/05/2019

CAUSAS

Código	Descripción
GE-CA100	Divulgación intensionada individual o en confabulación para favorecer intereses particulares (información periodística).
GE-CA101	Acceso lógico no autorizado al sistema Arkitex.
GE-CA102	Ataque de ingeniería social (phishing, vishing, smishing).
GE-CA103	Exposición de credenciales de acceso (en papeles, papel adhesivos, etc.)

Gestión Editorial

Perdida de la confidencialidad de la información en el proceso de Gestión Editorial.

IMPACTOS

Código	Categoría	Descripción	Nivel SEV	Nivel MPE
GE-IM1	S&S	0. Evaluado y no considerado		
GE-IM2	Ambiente	0. Evaluado y no considerado		
GE-IM3	Social	0. Evaluado y no considerado		
GE-IM4	Reputación	0. Evaluado y no considerado		
GE-IM5	Legal	0. Evaluado y no considerado		
GE-IM6	Financiero	2. ≥S/. 25000 to <S/. 500000	2	3

Controles Preventivos Existentes		Causa	Dueño
GE-CP100	Reglamento interno de trabajo (incluye procedimiento de medidas disciplinarias).	GE-CA100	Gerente de recursos humanos
GE-CP101	Política de control de acceso.	GE-CA101	Gerente de sistemas
GE-CP102	Software antivirus, sistema antispam, y firewall.	GE-CA102	Gerente de sistemas
GE-CP103	Campaña de sensibilización y capacitación.	GE-CA102, GE-CA103	Gerente de sistemas

Controles Mitigantes Existentes		Impacto	Dueño

Acciones de Mejora		Dueño	Causa	Inicio/Fin	Estado
GE-AM100	Implementar un proceso de revisiones de accesos periódicos a los sistemas identificados como críticos.	Gerente de sistemas	GE-CA101		En evaluación

SEVERIDAD	
S/.	Fatalidades
45,000.00	0

FACTOR DE SEVERIDAD	FACTOR DE PROBABILIDAD	NIVEL DE RIESGO RESIDUAL
3	1.00	3

MAXIMA PÉRDIDA ESTIMADA	
S/.	Fatalidades
91.00	0

SUSTENTO PARA LA ESTIMACIÓN DE LA SEVERIDAD
El sustento de escenario de severidad es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

SUSTENTO PARA LA ESTIMACIÓN DE LA PROBABILIDAD
El sustento de la estimación de probabilidad es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

SUSTENTO PARA LA ESTIMACIÓN DE LA MPE
Datos de máxima perdida estimada MPE, es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

Anexo 15: Análisis de riesgos / dimensiones con herramienta Bow Tie – Gestión Editorial.

Tipo	Seguridad de la Información
Clasificación	Negocio

Dueño	GERENTE DE PLANTA
Fecha (dd/mm/aaaa)	05/05/2019

CAUSAS

Código	Descripción
GE-CA200	Ataque de ingeniería social (phishing, vishing, smishing).
GE-CA201	Acceso lógico no autorizado al sistema Arkitex.
GE-CA202	Manipulación, borrado y/o eliminación de información periodística almacenada en el sistema Arkitex.
GE-CA203	Vulnerabilidades no identificadas en servidores de correo electrónico y Arkitex
GE-CA204	Acceso no autorizado a equipos de cómputo desatentidos (Área editorial).

Gestión Editorial

Perdida de la integridad de la información en el proceso de Gestión Editorial.

IMPACTOS

Código	Categoría	Descripción	Nivel SEV	Nivel MPE
GE-IM100	S&S	0. Evaluado y no considerado		
GE-IM101	Ambiente	0. Evaluado y no considerado		
GE-IM102	Social	0. Evaluado y no considerado		
GE-IM103	Reputación	0. Evaluado y no considerado		
GE-IM104	Legal	0. Evaluado y no considerado		
GE-IM105	Financiero	2. ≥S/. 25000 to <S/. 500000	2	3

Controles Preventivos Existentes		Causa	Dueño
GE-CP200	Software antivirus, sistema antispam, y firewall.	GE-CA200, GE-CA203	Gerente de sistemas
GE-CP201	Campaña de sensibilización y capacitación.	GE-CA200, GE-CA204	Gerente de sistemas
GE-CP202	Política de control de acceso.	GE-CA201	Gerente de sistemas
GE-CP203	Rutinas de Backup semanal de base de datos historica de sistema Arkitex	GE-CA202	Gerente de sistemas
GE-CP204	Reglamento interno de trabajo (incluye procedimiento de medidas disciplinarias).	GE-CA202	Gerente de recursos humanos
GE-CP205	Activación de bloqueo de escritorio por inactividad (despues de 5 minutos)	GE-CA204	Gerente de sistemas

Controles Mitigantes Existentes		Impacto	Dueño

Acciones de Mejora		Dueño	Causa	Inicio/Fin	Estado
GE-AM202	Desarrollo de lineamientos para gestión de vulnerabilidades IT/OT.	Gerente de Sistemas	GE-CA203		En evaluación

SEVERIDAD	
S/.	Fatalidades
25,000.00	0

FACTOR DE SEVERIDAD	FACTOR DE PROBABILIDAD	NIVEL DE RIESGO RESIDUAL
3	3.00	9

MAXIMA PÉRDIDA ESTIMADA	
S/.	Fatalidades
51.00	0

SUSTENTO PARA LA ESTIMACIÓN DE LA SEVERIDAD
El sustento de escenario de severidad es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

SUSTENTO PARA LA ESTIMACIÓN DE LA PROBABILIDAD
El sustento de la estimación de probabilidad es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

SUSTENTO PARA LA ESTIMACIÓN DE LA MPE
Datos de máxima perdida estimada MPE, es considerada como información altamente confidencial. Por esta razon no se muestran en el estudio. Sin embargo se establece un monto aproximado de impacto.

Anexo 16: Análisis de riesgos / dimensiones con herramienta Bow Tie – Gestión Operativa.

CAUSAS	
Código	**Descripción**
CA300	Falla física de servidores SCADA y SAP.
CA301	Corte de suministro electrico en planta.
CA302	Falla de la red y de las comunicaciones de los sensores PLC y DCS (Red de control.
CA303	Falla de dispositivos PLC y DCS (sensores, variados, y otros).
CA304	Saturación de espacio de disco en servidores, memoria RAM insuficiente, ancho de banda.
CA305	Manipulación de parametros de PLCs y sistema SCADA por ataque cibernetico.
CA306	Ataque de ingeniería social (phishing, vishing, smishing).
CA307	Acceso físico no autorizado a data center.
CA308	Fallas en funcionamiento de aire acondicionado en data center.

SISTEMA AUTOMATIZADO DE PLANTA
Perdida de la disponibilidad de la información en el proceso de gestión operativa de planta.

IMPACTOS				
Código	**Categoría**	**Descripción**	**Nivel SEV**	**Nivel MPE**
IM1	S&S	0. Evaluado y no considerado		
IM2	Ambiente	0. Evaluado y no considerado		
IM3	Social	0. Evaluado y no considerado		
IM4	Reputación	1. Preocupación publica restringida a reclamos locales.	**1**	**2**
IM5	Legal	2. Asuntos legales menores, no cumplimientos y violaciones a los	**2**	**3**
IM6	Financiero	4. ≥S/. 100 000 to <S/. 250 000	**4**	**6**

Controles Preventivos Existentes		Causa	Dueño
CP300	Programa de mantenimiento de servidores, equipos de comunicación e infrestructura de soporte.	CA300, CA304, CA308	Gerente de sistemas
CP301	Suministro de energia electrico UPS y grupo electrógeno.	CA301	Gerente de planta
CP302	Programas de mantenimientos y/o calibracióna asignadas en sistema SAP.	CA302, CA303	Gerente de sistemas
CP303	Pruebas de validación de la data en componentes de sistema SCADA.	CA305	Gerente de sistemas
CP304	Software antivirus, sistema antispam, y firewall.	CA306	Gerente de sistemas
CP305	Campaña de sensibilización y capacitación.	CA306	Gerente de sistemas
CP306	Reglamento interno de trabajo (incluye procedimiento de medidas disciplinarias).	CA307	Gerente de sistemas

Controles Mitigantes Existentes		Impacto	Dueño

Acciones de Mejora		Dueño	Causa/Control	Inicio/Fin	Estado
AM300	Adquisición y/o implementación de software SIEM para análisis de Logs y monitoreo de comportamiento de dispositivo y/o componentes OT	Gerente de sistemas	CA305		En evaluación
AM301	Adquisición y/o implementación de software SolarWinds para la gestión de la capacidad.	Gerente de sistemas	CA304		En evaluación
AM302	Desarrollo de lineamientos para gestión de vulnerabilidades IT/OT.	Gerente de sistemas	CA305		En evaluación
AM303	Evaluación de adquisición de redundancia en equipamiento de aire acondicionado.	Gerente de planta	CA308		En evaluación

SEVERIDAD	
S/.	Fatalidades
300.00	**0**

FACTOR DE SEVERIDAD	FACTOR DE PROBABILIDAD	NIVEL DE RIESGO RESIDUAL
100	**1.00**	**100**

MAXIMA PÉRDIDA ESTIMADA	
S/.	Fatalidades
550.0	**0**

Anexo 17: Factor Severidad.

LOGO	METODOLOGÍA DE GESTIÓN DE RIESGOS		*<nombre de empresa>*
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO:	VERSIÓN:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Nivel de Severidad	TIPOS DE IMPACTO						Factor de Severidad
	Salud y Seguridad	Medio Ambiente	Social	Reputación	Legal	Financiero	
7	>50 fatalidades. Discapacidad Permanente >30% del cuerpo a más de 500 personas.	Impacto/s permanentes graves a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Quiebre total del orden social. Empresa directamente responsable o cómplice de graves y generalizadas consecuencias de largo plazo en materia de derechos humanos.	Condena Internacional prolongada (>2 meses) de múltiples organismos o de los medios de comunicación.	Toma de control hostil. Descontento público de los accionistas que resulta en la pérdida del Gerente General / Directorio. Quiebra o cierre de operaciones de la organización o de sus accionistas.	>US$ 1 M	1000
6	>20 fatalidades. Discapacidad permanente >30% del cuerpo a más de 100 personas.	Impacto/s graves (>20 años) a la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Quiebre del orden social. Empresa directamente responsable o cómplice de graves consecuencias de largo plazo en materia de derechos humanos	Condena internacional. Grandes protestas con violencia (>100 personas) que resultan en lesiones mortales.	Falta de licencias de operación, obligan el cierre de la operación. Derecho de la competencia o Investigación de prácticas de corrupción externas.	≥US$ 500 000 <US$ 1 M	300
5	2 -20 fatalidades. Discapacidad permanente >30% del cuerpo a más de 10 personas.	Impacto/s graves o extensos (< 20 años) a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Impactos sociales extensos de largo plazo. Empresa directamente responsable o cómplice de múltiples impactos agravados en materia de derechos humanos	Protesta seria pública o de los medios nacionales (cobertura internacional). Grandes protestas (>100 personas) con violencia significativa y lesiones graves múltiples.	Multas y procesos judiciales relativos a infracciones penales incluyendo penas de cárcel y ser objeto de investigación pública por el gobierno.	≥US$ 250 000 to <US$ 500 000	100
4	1 fatalidad. Discapacidad permanente >30% del cuerpo a una o más personas.	Impacto/s importante (< 5 años) a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Impactos sociales importantes de largo Empresa directamente responsable o cómplice de los principales impactos en materia de derechos humanos.	Atención adversa significativa de los medios nacionales y público. Protestas de 20 a 100 personas reprimidas por la fuerza, detenciones y heridos. Reputación de la empresa mayormente impactada.	Litigios civiles serios incluyendo demandas colectivas.	≥US$100 000 <US$250 000	30
3	Discapacidad permanente <30% del cuerpo a una o más personas. Días perdidos debido a lesión o enfermedad.	Impacto/s moderados (< 1 año) a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Impactos sociales moderados de mediano plazo o frecuentes problemas sociales. Impactos temporales moderados en materia de derechos humanos.	Atención de los medios regionales y acentuada preocupación de la comunidad local. Reputación de la empresa afectada negativamente.	Incumplimiento de la legislación. Falta de licencias validas de exploración.	≥US$50 000 to <US$100 0000	10

2	Discapacidad objetiva pero reversible. Tratamiento médico debido a lesión o	Impacto/s menores (<3 meses) a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Impactos sociales menores de mediano plazo en un número pequeño de personas. Impacto temporal menor en materia de derechos humanos.	Atención adversa de los medios locales y protestas públicas. Acentuado control del regulador. Reputación de la empresa afectada por un pequeño número de personas.	Asuntos legales menores, no cumplimientos y violaciones a los reglamentos.	≥US$25 000 to <US$ 50 000	3
1	Bajo nivel de molestias o síntomas subjetivos en corto plazo. No requiere tratamiento médico.	Impacto/s de bajo nivel a la tierra, la biodiversidad, servicios de los ecosistemas, recursos hídricos o el aire.	Impactos sociales de bajo nivel. Impacto mínimo en materia de derechos humanos.	Preocupación publica restringida a reclamos locales. Bajo nivel de interés de los medios y/o del regulador.	Asunto legal de bajo nivel	<US$25 000	1

Anexo 18: Plan de tratamiento de Riesgos producto del análisis de riesgos.

FORMATO DE MATRIZ DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Fecha:	5/5/2019	Responsable:

Nro.	Proceso	Código de riesgo	Riesgo	NRR	Dimensión CID afectada	Acciones de tratamiento	Tipo de acción	Estado	Fecha	Responsable de Gestión
1	Gestión editorial	GR20190505-GEDI-001	Pérdida de la confidencialidad de la información procesada en la gestión editorial.	3	Confidencialidad	1. Implementar un proceso de revisiones de accesos periódicos a los sistemas identificados como críticos.	Preventiva	En evaluación		Gerente de sistemas
		GR20190505-GEDI-002	Pérdida de la Integridad de la información procesada en la gestión editorial.	9	Integridad	2. Desarrollo de lineamientos para gestión de vulnerabilidades IT/OT. **[Aplica para Integridad y Disponibilidad]**	Preventiva	En evaluación		Gerente de sistemas
						3. Adquisición y/o implementación de software SolarWinds para la gestión de la capacidad.	Preventiva	En evaluación		Gerente de sistemas
		GR20190505-GEDI-003	Pérdida de la Disponibilidad de la información procesada en la gestión editorial.	9	Disponibilidad	4. Evaluación de adquisición de redundancia en equipamiento de aire acondicionado.	Preventiva	En evaluación		Gerente de planta
2	Gestión operativa	GR20190505-GOPE-001	Pérdida de la confidencialidad de la información procesada en la gestión operativa.	3	Confidencialidad	1. Implementar un proceso de revisiones de accesos periódicos a los sistemas identificados como críticos.	Preventiva	En evaluación		Gerente de sistemas
		GR20190505-GOPE-002	Pérdida de la integridad de la información procesada en la gestión operativa.	9	Integridad	2. Implementar acciones y/o rutinas de backup en la nube.	Preventiva	En evaluación		Gerente de sistemas
						3. Adquisición y/o implementación de software SPLAN para analisis de Logs y monitoreo de comportamiento de dispositivo y/o componentes OT. **[Aplica para Integridad y Disponibilidad]**	Preventiva	En evaluación		Gerente de sistemas
						4. Desarrollo de lineamientos para gestión de vulnerabilidades IT/OT. **[Aplica para Integridad y Disponibilidad]**	Preventiva	En evaluación		Gerente de sistemas
		GR20190505-GOPE-003	Pérdida de la disponibilidad de la información procesada en la gestión operativa.	100	Disponibilidad	5. Adquisición y/o implementación de software SolarWinds para la gestión de la capacidad.	Preventiva	En evaluación		Gerente de sistemas
						6. Evaluación de adquisición de redundancia en equipamiento de aire acondicionado.	Mitigante	En evaluación		Gerente de planta

Anexo 19: Declaración de Aplicabilidad del Modelo de Seguridad de la Información.

LOGO	**DECLARACIÓN DE APLICABILIDAD DEL MODELO DE SEGURIDAD DE LA INFORMACION**		Empresa editora1
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO:	VERSIÓN:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Elaborado por:

Revisado por:

Aprobado por:

1. Objetivo

El objetivo del presente documento es definir qué controles son adecuados para implementar en <nombre empresa> y aprobar riesgos residuales y la implementación de los controles mencionados.
Este documento incluye todos los controles detallados en el Anexo A de la norma ISO 27001 y los controles de Ciberseguridad del Cis, los cuales aplican a todo el alcance del modelo de seguridad de la información.

Con la finalidad de determinar el contexto de la implementación de los controles de seguridad de la información en <nombre empresa> se ha elaborado la presente Declaración de Aplicabilidad, con carácter de política de acuerdo con la estructura de información documentada requerida por la Norma ISO/IEC 27001:2013 en su apartado 6.1.3.d como documentación asociada al modelo de seguridad de la información.
La Declaración de Aplicabilidad parte del análisis realizado en la evaluación de los riesgos, y en la misma se detallan:
• Los objetivos de control y controles seleccionados, con las correspondientes justificaciones de su selección.
• Los objetivos de control y controles no seleccionados, con las correspondientes justificaciones de su exclusión.

NUM.	TIPO DE CONTROL	APLICABLE	JUSTIFICACIÓN	RESPONSABLE
A.05				
A.05.1				
A.05.1.1	General	Si	Justificación	Responsable 1
A.05.1.2	General	Si	Justificación	Responsable 2
A.06				
A.06.1				
A.06.1.1	General	Si	Justificación	Responsable 1

A.06.1.2	General	Si	Justificación	Responsable 2
A.06.1.3	General	Si	Justificación	Responsable 3
A.06.1.4	General	Si	Justificación	
A.06.1.5	Específico	Si	Justificación	
A.06.2				
A.06.2.1	Específico	Si	Justificación	
A.06.2.2	Específico	No	Justificación	No aplica
A.07				
A.07.1				
A.07.1.1	General	Si	Justificación	
A.07.1.2	General	Si	Justificación	

Anexo 20: Objetivos de Seguridad de la Información.

LOGO	**OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN**		Empresa editora1
	MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS		
	CÓDIGO:	VERSIÓN:	
	FECHA DE ELABORACIÓN:	PÁGINA 1 DE	

Elaborado por:
Revisado por:
Aprobado por:
1. Objetivo
<nombre empresa> establece los siguientes objetivos de seguridad de la información alineados a sus objetivos estratégicos: Objetivo de seguridad de la información N°1: Fortalecer la confidencialidad, integridad y disponibilidad de la información de la empresa en busca de lograr la reducción de costos y el mantenimiento de la competitividad, Objetivo de seguridad de la información N°2: Minimizar el tiempo de respuesta de los incidentes de seguridad de la información identificados. Objetivo de seguridad de la información N°3: Asegurar la toma de conciencia y la capacitación en temas de seguridad de la información en forma aplicada a las actividades mineras. <relacionar con objetivo estratégico>. Objetivos estratégicos Los objetivos estratégicos, están alineados a pilares estratégicos que están direccionados a sostener la creación de valor y reputación de <nombre empresa> y sus partes interesadas.

Pilares Estratégicos	**Objetivos Estratégicos**
PILAR ESTRATÉGICO 1	Objetivos estratégicos relacionados al pilar estratégico 1
PILAR ESTRATÉGICO 2	Objetivos estratégicos relacionados al pilar estratégico 2
PILAR ESTRATÉGICO 3	Objetivos estratégicos relacionados al pilar estratégico 3
PILAR ESTRATÉGICO …	Objetivos estratégicos relacionados al pilar estratégico …

Anexo 22: Ejecución del plan de concienciación.

TEMARIO ABORDAR EN LAS CONCIENTIZACIONES									
N°	Temas	2019							
		Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
1	Internet Seguro.								
2	Contraseñas Seguras.								
3	Software permitido y no permitido en equipos.								
4	Seguridad de los equipos (Controles de seguridad y backups).								
5	Protección contra virus, código malicioso, phishing, correo SPAM, etc.								
6	Pasos a seguir en caso de incidentes.								
7	Cumplimiento de la política de seguridad de la información y sanciones en caso de incumplimiento.								
8	Seguridad física.								

EVALUACIÓN DEL PROGRAMA DE CAPACITACIÓN Y CONCIENTIZACIÓN			
Número total de usuarios	% de aprobados	% de desaprobados	% de inasistencia
54	92	4	4

Afiche de concienciación difundido por medios digitales internos

Anexo 23: Matriz integral de seguimiento de acciones del modelo de seguridad de la información.

Código Acción	Acción	Fuente	Periodicidad	Responsable de la Acción	Inicio	Fin	Prioridad	Duración	Estado	Responsable de Seguimiento	Referencia	SOA/ISO	Comentario estado actual Comentario estado actual /detalle de la acción	Analisis de Causa	Hallazgo	Seguimiento
GR201810-01	Acuerdos de confidencialidad firmados por trabajadores y socios estratégicos del alcance	Gestión de Riesgos					Media	2 meses	**Pendiente**		RI-SI-001 RI-SI-007	A.13.2.4				
GR201810-02	Evaluar la implementación de un proceso de backup centralizado en algunos equipos y medios extraibles criticos.	Gestión de Riesgos					Alta	2 meses	**Pendiente**		RI-SI-007	A.12.3.1				
GR201810-03	Clasificar la información de Operaciones Planta	Gestión de Riesgos							**Pendiente**		RI-SI-007	A.8.2.1				
GR201810-04	Elaborar Ethical Hacking - Pruebas de penetración (Pen Testing)	Gestión de Riesgos					Alta	1 mes	**Pendiente**		RI-SI-008 RI-SI-009	A.12.2.1 A.18.2.3				
GR201810-05	Evaluar la implementación de alertas o alarmas ante una detección temprana de inconsistencia de datos entre los PLCs e instrumentos y el HMI que lo controla a fin de verificar la integridad de los datos	Gestión de Riesgos					Alta	2 meses	**Pendiente**		RI-SI-008	CSC6				
GR201810-06	Elaborar un plan de mantenimiento para cada equipo critico (Desktop) tecnológico de la planta (Salas de Control) y en general de cualquier centro de monitoreo	Gestión de Riesgos					Alta	1 mes	**Pendiente**		RI-SI-009	A.11.2.4				
GR201810-07	Establecer las estrategias y elaborar el plan de plan de recuperacion de servicios de tecnología que soporta los servicios criticos de TI en Operaciones Planta.	Gestión de Riesgos					Media	1 mes	**Pendiente**		RI-SI-009	A.17.1.1 A.17.2.1				

Anexo 24: Constancia de validación de instrumento.

CONSTANCIA DE VALIDACION DEL INSTRUMENTO APLICADO PARA LA APLICACIÓN DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE

Quien suscribe, **OLGA NAYDA DE LA CRUZ SANCHEZ**, con documento de identidad N° **40239681**, de profesión **Estadística**, con grado de **Licenciada**.

Por medio de la presente hago constar que he revisado con fines de Validación el instrumento (encuesta), a los efectos de su aplicación en las empresas de editoras de la Región Lambayeque.

Luego de haber aplicado la prueba de confiabilidad KR20 de Kuder de Richarson, se obtuvo que la confiabilidad del instrumento es muy alta, obteniendo como resultado 0.98; es decir, el 98% de confiabilidad de que el instrumento es aceptable.

Se aplicó la siguiente fórmula:

$$KR20 = \frac{k}{k-1}\left[\frac{S^2T(aciertos) - \sum p * q(aciertos)}{S^2T(aciertos)}\right]$$

Donde:

$k = 73$	: Número	de Ítems
$\sum p * q = 5.33$	: Sumatoria	de proporciones de aciertos por desaciertos
$S^2T = 148$	: Varianza	total de aciertos.

Por lo expuesto, se puede confirmar que el instrumento tiene relación entre sus Ítems, comprensión en su contenido y claridad en su redacción.

Fecha: 29 de enero de 2018

DNI N°40239681

Anexo 25: Formato validación juicio de expertos del modelo propuesto.

Estimado Ingeniero:

A través de la presente me dirijo a usted con la finalidad de solicitar su colaboración para la validación de la propuesta realizada en la investigación denominada **MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE**. Para tal fin, se anexa el cuestionario de validación.

FECHA :
NOMBRES Y APELLIDOS :
FORMACIÓN ACADÉMICA :
AREAS DE EXPERIENCIA PROFESIONAL :
TIEMPO DE EXPERIENCIA :
CARGO ACTUAL :
INSTITUCIÓN :

Objetivo de la investigación:

Respaldar la disponibilidad de las operaciones estratégicas en las empresas editoras de la región Lambayeque mediante el desarrollo de un modelo de seguridad de la información.

Objetivo del juicio de expertos:

Verificar la validez del modelo propuesto en relación con la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba:

Determinar la utilidad del modelo propuestas en empresas editoras de la región Lambayeque

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión, pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y	1 No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con

semántica son adecuadas.		su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1 no cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Anexo 26: Validación de Juicio de Expertos

Validación de experto N. ° 1

Validación - MODELO DE SEGURIDAD DE LA INFORMACIÓN

Reenvió este mensaje el Jue 23/05/2019 2:49.

CV Carlos Vega
Mar 21/05/2019 18:23
jessie Bravo

pdf Validacion_modelo_seguridad...
767 KB

Estimado Ing. Jessie Bravo Jaico:

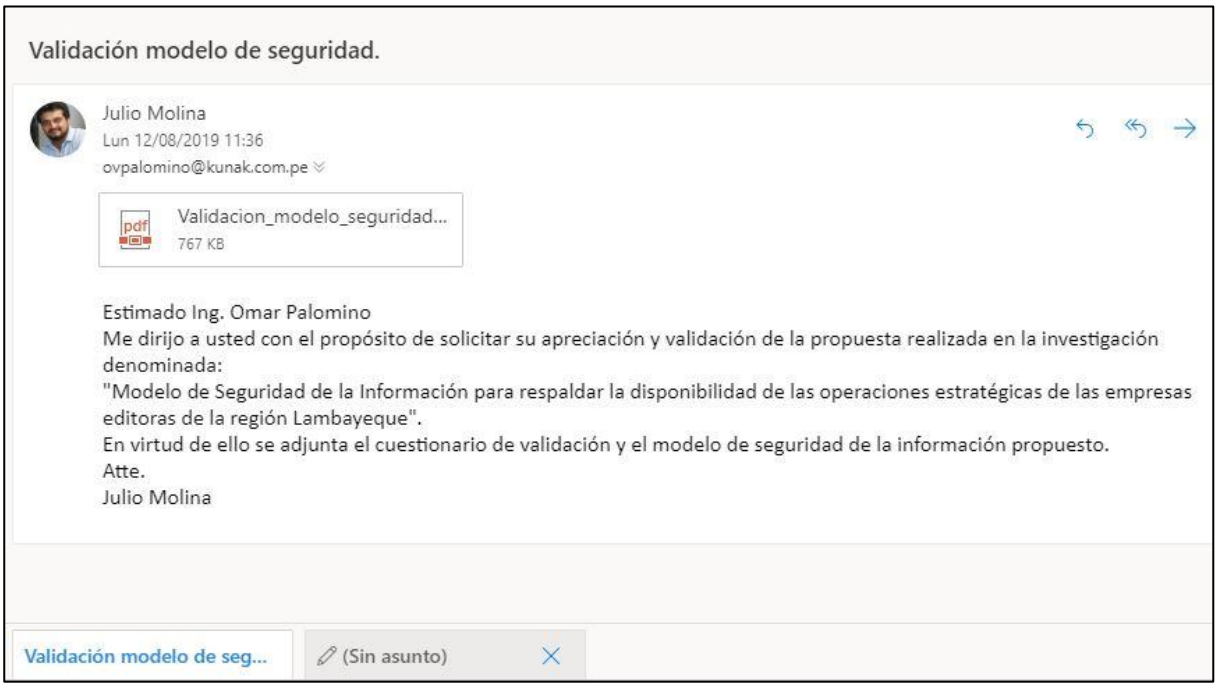
A través de la presente nos dirigimos a usted con el fin de solicitarle su ayuda para la validación de nuestro trabajo de investigación denominado **MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE,**
Para tal fin, se anexa el archivo del modelo a validar que contiene el cuestionario de validación(pagina 18 y 19):

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE.

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I - Definición del alcance y diagnóstico	Análisis de Contextos y Partes Interesadas	3	3	4	4	
	Alcance del Modelo de Seguridad de la Información.	4	4	4	4	
	Definición de Roles y Responsabilidades de Seguridad de la Información	4	4	4	4	
	Definición del Perfil Actual	4	3	4	4	
II - Planificación	Definición de la Metodología de Gestión de Riesgos.	4	4	4	4	
	Identificación. análisis y evaluación de Riesgos de Seguridad de la Información.	4	4	4	4	
	Tratamiento de riesgos de seguridad de la información.	3	4	4	4	
	Identificación de aplicabilidad de controles.	3	4	4	4	
	Definición de los Objetivos de Seguridad de la Información	4	4	3	4	
	Capacitación y Concienciación del Modelo de Seguridad de la Información.	4	3	4	4	
	Proceso de Comunicación.	4	3	4	4	
	Definición del Perfil Destino.	4	4	3	4	
III - Implementación	Operacionalización de estrategias de Securización.	4	4	4	4	
	Gestión de Incidentes	3	4	4	4	
VI - Evaluación del desempeño.	Definición de Indicadores del Modelo de Seguridad de la Información.	4	4	4	4	
	Monitoreo y Medición.	4	4	4	4	
V - Mejora continua	Plan de Mejora Continua.	3	3	4	4	

JESSIE LEILA BRAVO JAICO
ING. COMP. Y SIST.
R. CIP. 71196

Validación de experto N. ° 2



Validación modelo de seguridad.

Julio Molina
Lun 12/08/2019 11:36
ovpalomino@kunak.com.pe

Validacion_modelo_seguridad...
767 KB

Estimado Ing. Omar Palomino
Me dirijo a usted con el propósito de solicitar su apreciación y validación de la propuesta realizada en la investigación denominada:
"Modelo de Seguridad de la Información para respaldar la disponibilidad de las operaciones estratégicas de las empresas editoras de la región Lambayeque".
En virtud de ello se adjunta el cuestionario de validación y el modelo de seguridad de la información propuesto.
Atte.
Julio Molina

Validación modelo de seg... (Sin asunto)

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE.

Fase	Actividad	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
1. Definición del alcance y diagnostico	Análisis de contextos y partes interesadas	4	4	4	4	
	Alcance del modelo de seguridad de información	4	4	4	4	
	Definición de roles y responsabilidades de seguridad de la información	4	4	4	4	
	Definición de perfil actual	4	3	3	4	
2. Planificación	Definición de la metodología de Gestión de Riesgos	4	4	4	4	
	Identificación, análisis y evaluación de riesgos de seguridad de información	4	4	4	4	
	Tratamiento de riesgos de seguridad de información	4	4	4	4	
	Identificación de aplicabilidad de controles	4	4	4	4	
	Definición de objetivos de seguridad de la información	4	4	4	4	
	Capacitación y concientización del modelo de seguridad de la información	4	4	4	4	
	Proceso de comunicación	4	3	3	3	
	Definición del perfil destino	3	4	4	4	
3. Implementación	Operacionalización de estrategias de securización	4	4	4	3	
	Gestión de incidentes	4	4	4	3	
4. Evaluación de desempeño	Definición de indicadores del Modelo de seguridad de la información	4	4	4	4	
	Monitoreo y medición	4	4	4	4	
5. Mejora continua	Plan de mejora continua	4	4	4	4	

Ing. Omar Palomino Huamaní

DNI: 44160860

Validación de experto N. ° 3

Saludos/Tesis/USAT-SGSI

Mensaje enviado con importancia Alta.

Villacrez Eder Jair
Vie 9/07/2019 21:19
Martin Valdivia

Validacion_modelo_seguridad...
767 KB

Estimado Ing. Martin, buenas noches.

De acuerdo a lo conversado hace un tiempo, hemos desarrollado como parte de investigación en el curso de TESIS un modelo de seguridad de la información.

El estudio de investigación tiene como titulo ***MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE***

Como parte del proceso de validación del modelo es conveniente se realice el juicio de experto, es por ello que recurrimos a usted para que nos ayude con ello. Así mismo estoy adjuntando documento el cual ayudará al proceso.

Desde ya agradecemos infinitamente por su apoyo. Si tiene alguna duda u observación por favor me avisa.

Saludos,

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA RESPALDAR LA DISPONIBILIDAD DE LAS OPERACIONES ESTRATÉGICAS EN LAS EMPRESAS EDITORAS DE LA REGIÓN LAMBAYEQUE.

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I - Definición del alcance y diagnóstico	Proceso Análisis de Contextos y Partes Interesadas	4	4	4	4	
	Proceso Alcance del Modelo de Seguridad de la Información.	4	4	4	4	
	Proceso Liderazgo y Compromiso.	4	4	4	4	
	Proceso Definición de Roles y Responsabilidades de Seguridad de la Información	4	4	4	4	
	Proceso Definición del Perfil Actual	4	4	4	4	
II - Planificación	Proceso Definición de la Metodología de Gestión de Riesgos.	4	4	4	4	
	Proceso Identificación, análisis y evaluación de Riesgos de Seguridad de la Información.	4	4	4	4	
	Proceso Tratamiento de riesgos de seguridad de la información.	4	4	4	4	
	Proceso Identificación de aplicabilidad de controles.	4	3	4	4	
	Proceso Definición de los Objetivos de Seguridad de la Información	4	4	4	4	
	Proceso Capacitación y Concienciación del Modelo de Seguridad de la Información.	4	4	4	4	
	Proceso de Comunicación.	4	4	4	4	
	Proceso Definición del Perfil Destino.	4	4	4	4	
III - Implementación	Proceso Operacionalización de estrategias de Securización.	4	4	4	4	
	Proceso Gestión de Incidentes	4	4	4	4	
VI - Evaluación del desempeño.	Proceso de Monitoreo y Medición.	4	4	4	4	
V - Mejora continua	Proceso de Mejora Continua.	4	4	4	4	

Anexo 27: Cuestionario de validación del modelo de seguridad de la información.

FASE	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
I - Definición del alcance y diagnóstico	Análisis de Contextos y Partes Interesadas					
	Alcance del Modelo de Seguridad de la Información.					
	Definición de Roles y Responsabilidades de Seguridad de la Información					
	Definición del Perfil Actual					
II - Planificación	Identificación, análisis y evaluación de Riesgos de Seguridad de la Información.					
	Tratamiento de riesgos de seguridad de la información.					
	Identificación de aplicabilidad de controles.					
	Definición de los Objetivos de Seguridad de la Información					
	Capacitación y Concienciación del Modelo de Seguridad de la Información.					
	Definición del Perfil Destino.					
III - Implementación	Operacionalización de estrategias de Securización.					
	Gestión de Incidentes					
IV - Evaluación del desempeño.	Monitoreo y Medición.					
V - Mejora continua	Plan de Mejora Continua.					

Fuente: Elaboración propia.

Anexo 28: Matriz de indicadores propuestos para medir la eficacia del modelo.

1. INDICADORES DE EFICACIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Nro.	CONTROL DE SI	DESCRIPCIÓN	NOMBRE DEL INDICADOR	OBJETIVO DEL INDICADOR	TIPO DE INDICADOR	MÉTRICA	FUNCIÓN	UMBRAL	RESPONSABLE	FUENTE DE VERIFICACIÓN DE DATOS	META DEL INDICADOR			PERIODICIDAD DE MEDICIÓN	LÍNEA BASE
											DEFICIENTE	MEJORABLE	ÓPTIMO		
A.11.2.4.	Mantenimiento de equipos	Los equipos deben mantenerse de manera correcta para asegurar la continuidad del negocio y la disponibilidad de la información	SGSI-NI-35	IS35 : Verificar el Cumplimiento del cronograma de mantenimiento anual de servidores criticos	Operativo	-# de servidores criticos que se les realiza mantenimiento preventivo = B1 -# total de servidores criticos= B2	M35 = (B1/B2)*100	M35 = 95% de equipos que se hicieron mantenimiento	Por definir	Registro de equipos que se les dio mantenimiento	<=80%	81% - 90%	>90%	Trimestral	
A.12.2.1.	Controles contra códigos maliciosos	Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación	SGSI-NI-37	IS37: Verificar que los equipos de computo se encuentren con antivirus actualizado	Operativo	-# Total de equipos con antivirus actualizado con la última versión=B1 -# Total de equipos con antivirus=B2	M37 = (B1/B2)*100	M37 = 80% de equipos con antivirus actualizado	Por definir	Bitacora de resgistro de incidentes de seguridad de la información	<=80%	81% - 89%	>=90%	Trimestral	
			SGSI-NI-38	IS38: Verificar que los equipos de computo se encuentren gestionados por el antivirus	Operativo	-# Total de equipos de computo que cuenten con antivirus = B1 -# Total de equipos de computo = B2	M38 = (B1/B2)*100	M38 = 90% de equipos de computo cuentan con antivirus	Por definir	Bitacora de resgistro de incidentes de seguridad de la información	<=80%	81% - 89%	>=90%	Trimestral	
			SGSI-NI-39	IS39: Verificar que los incidentes ocasionado por software malicioso se encuentren correctamente gestionados	Operativo	-# de incidentes ocasionados por software malicioso que fueron controlados y gestionados por el antivirus = B1 -# total de incidentes ocasionados por software malicioso = B2	M39 = (B1/B2)*100	M39 = 100% de incidentes ocasionados por software malicioso que estan controlados y gestionados	Por definir	Bitacora de resgistro de incidentes de seguridad de la información	<=80%	81% - 89%	>=90%	Trimestral	
			SGSI-NI-40	IS40: Número de sistemas afectados por software malicioso que no cuentan con una solución contra el software malicioso actualizada	Operativo	-# de incidentes de código malicioso por usuarios repetitivo = B1 -# total de incidentes ocasionados por software malicioso = B2	M40 = (B1/B2)*100	M40 = 20% de incidentes de código malicioso por usuarios repetitivos	Por definir	Bitacora de resgistro de incidentes de seguridad de la información	51>=%	20% - 50%	<=20%	Trimestral	
A.12.3.1.	Respaldo de información	Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	SGSI-NI-44	IS44: Evaluar la ejecución de pruebas de restauración total de servidores	Operativo	- # de ejecución de pruebas de restauración de backups total de servidores ejecutados con exito . = B1 - # total de ejecución de pruebas de restauración de backups total de servidores planificados y ejecutados. = B3	M44 = (B1/B2)*100	M44 = 100% que se efectua las pruebas de restauración con éxito total de los servidores	Por definir	Sistema o solución que realiza los backups automatizados	<=80%	81% - 90%	>90%	Anual	
A.13.1.2	Mecanismos de seguridad asociados a servicios de red	Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados	SGSI-NI-54	IS54: Evaluar el número de conexiones de software de acceso remoto autorizados	Operativo	-#de equipos con conexiones de software de acceso remoto permitido= B1 -#total de equipos conexiones de software de acceso remoto= B2	M54 = (B1/B2)*100	M54 = 95% de conexiones de software de acceso remoto permitido	Por definir	Software de administración	<=80%	81% - 90%	>=90%	Trimestral	
			SGSI-NI-55	IS55: Evaluar el desempeño actual de los controles de seguridad perimetral	Operativo	-#de intrusos detectados y bloqueados= B1 -#de intrusos detectados= B2	M55 = (B1/B2)*100	M55 = 100% de intrusos detectados y bloqueados	Por definir	Consola de administración de firewall	<=80%	81% - 90%	>=90%	Trimestral	
			SGSI-NI-56	IS56: Verificar si la cantidad de puertos abiertos son requeridos para el correcto funcionamiento de los servidores críticos	Operativo	-#de puertos abiertos requeridos y gestionados por los sistemas de información en los servidores críticos= B1 -#total de puertos abiertos de los servidores críticos= B2	M56 = (B1/B2)*100	M56= 100% de puertos abiertos requeridos y gestionados por los sistemas de información en los servidores	Por definir	Consola de administración de firewall	<=80%	81% - 90%	>=90%	Semestral	
A.17.2.1.	Instalaciones de procesamiento de la información	Los recursos de tratamiento de la información deberían ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad	SGSI-NI-65	IS65: Verificar el correcto funcionamiento de los tiempos de recuperación propuesto para la restauración de backups	Operativo	-Tiempo de recuperación (Tiempo real de duración de restauración de backup) = B1 -Tiempo objetivo de duración del restore = B2	M65= (B1/B2)*100	M65= 90% del tiempo estimado de recuperación según nuestro tiempo objetivo de duración del restore	Por definir	Informe de pruebas de contingencia	<=80%	81% - 90%	>90%	Trimestral	
			SGSI-NI-66	IS66: Verificar el correcto funcionamiento de los equipos redundantes	Operativo	- # de equipos redundantes, configurado y gestionados que funcionaron correctamente en pruebas de continuidad operativa= B1 - # total de equipos redudantes configurados y gestionados = B2	M66= (B1/B2)*100	M66 = 100% de equipos redundantes, funcionan correctamente	Por definir	•Informe de pruebas de contingencia •Plataforma administrativa del software	<=80%	81% - 90%	>90%	Trimestral	

NOMBRE DEL INDICADOR	Primer Trimestre 2019					Segundo Trimestre 2019					Tercer Trimestre 2019					Cuarto Trimestre 2019				
	Fecha de Medición	Atributo 1	Atributo 2	Resultado	Evaluación	Fecha de Medición	Atributo 1	Atributo 2	Resultado	Evaluación	Fecha de Medición	Atributo 1	Atributo 2	Resultado	Evaluación	Fecha de Medición	Atributo 1	Atributo 2	Resultado	Evaluación
SGSI-NI-35		5	20	25%	Deficiente		33	33	100%	Óptimo										
SGSI-NI-37		6	6	100%	Óptimo		40	60	67%	Deficiente										
SGSI-NI-38		5	6	83%	Mejorable		3	6	50%	Deficiente										
SGSI-NI-39		7	9	78%	Deficiente		4	5	80%	Deficiente										
SGSI-NI-40		7	9	78%	Deficiente		6	7	86%	Mejorable										
SGSI-NI-44		6	6	100%	Óptimo															
SGSI-NI-54		6	6	100%	Óptimo		7	7	100%	Óptimo										
SGSI-NI-55		0	6	0%	Deficiente		7	9	78%	Deficiente										
SGSI-NI-56							5	6	83%	Mejorable							5	5	100%	Óptimo
SGSI-NI-65		1	6	17%	Deficiente		2	2	100%	Óptimo										
SGSI-NI-66		4	6	67%	Deficiente		3	5	60%	Deficiente										