ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA BIBLIOTECAS BASADO EN UNA METODOLOGÍA MEJORADA DE ANÁLISIS DE RIESGOS COMPATIBLE CON LA NORMA ISO/IEC 27001:2013

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE MÁSTER EN SOFTWARE MENCIÓN SEGURIDAD

MARÍA JOSÉ BRAVO RAMOS
mariajosebravo1992@gmail.com

DIRECTOR: SANG GUUN YOO, Ph.D.
sang.yoo@epn.edu.ec

Quito, Noviembre 2018

AVAL DEL DIRECTOR

Certifico que el presente trabajo fue desarrollado por Bravo Ramos María José bajo mi supervisión.

_____

Sang Guun Yoo, Ph.D.
DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Bravo Ramos María José, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Bravo Ramos María José

AGRADECIMIENTO

A Dios por permitirme venir a este mundo y brindarme la sabiduría y fortaleza para llegar hasta donde estoy y seguir cumpliendo muchos sueños y metas. ¡¡Gracias mi Señor por todo!!

A mis padres, Lorgia y Walter, por estar siempre a mi lado en las buenas y malas apoyándome cuando he estado a punto de desfallecer, además de inculcarme buenos valores y por ser mi ejemplo a seguir, por enseñarme que para conseguir algo en esta vida se debe trabajar mucho para que se haga realidad. ¡¡Los quiero mucho papitos!!

A mi hermano Jhon, tú eres mi inspiración para luchar por mis sueños quiero ser tu modelo a seguir para que también cumplas todos tus anhelos y que sepas que nada es imposible en esta vida, solo se requiere esfuerzo y dedicación para conseguir todas las metas. ¡¡Te quiero mucho hermanito...!!

A Leoncito, amor mío, gracias por todo el apoyo que me has brindado en el desarrollo de este trabajo, en todos los proyectos realizados y aquellos pendientes por realizar. Sin ti no hubiera sido posible finalizarlo, gracias por darme ánimo a continuar siempre y más aún cuando hubo momentos en los cuales ya no quería avanzar. ¡Te amo mi ángel…!

A mi director de tesis, Sang Guun Yoo, por ser una excelente persona y un gran profesional, gracias por compartir sus conocimientos, por su dirección y paciencia en el desarrollo de este proyecto. ¡¡Muchísimas gracias por todo!!

A todos ustedes les estoy eternamente agradecida por todo, que Dios les bendiga enormemente. ¡¡¡¡Simplemente gracias…!!!!

María José

DEDICATORIA

A papito Dios, todos mis proyectos cumplidos y por cumplir te los ofrezco a ti puesto que todo es posible si es tu voluntad.

A mi mamita, por todo el esfuerzo que has hecho para hacerme la mujer que soy. ¡Eres mi orgullo!

A mi hermanito, ánimo y lucha también por lo que sueñas.

María José

INDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Las bibliotecas universitarias son centros custodios de información vital para una comunidad universitaria, donde el conocimiento que estas resguardan puede ser compartido con estudiantes, docentes e investigadores.

Al denominarse a una biblioteca como centro de acopio de información, es necesario que la seguridad con la que esta cuenta se priorice y se le dé la importancia que esta merece.

Ante esta situación, este trabajo aborda las necesidades específicas de estos centros de información en materia de seguridad. Como parte del mismo, se plantea realizar un análisis y optimización de las metodologías de riesgos existentes (Magerit V.3, Octave V.2 y NIST). Una vez obtenida la metodología mejorada para las bibliotecas universitarias públicas de Quito, se tomó como caso de estudio, el sistema de bibliotecas de la Escuela Politécnica Nacional (EPN).

Palabras clave

Bibliotecas universitarias públicas; Gestión de la seguridad de la información; Tecnologías de la información y comunicación; Sistemas de Gestión de Seguridad de la Información; Seguridad de la información; Metodologías de análisis de riesgos.

ABSTRACT

University libraries are guardians of information that share information with students, teachers and researchers for the university community.

Libraries are centers for gathering information, and therefore, it is necessary to prioritize security. For this reason, an analysis and optimization of existing risk methodologies was proposed (Magerit V.3, Octave V.2 and NIST). Once the improved methodology for Quito's public university libraries was obtained, it was applied in the library system of the Escuela Politécnica Nacional (EPN).

Keywords

Public university libraries; Information security management; Information and communication technologies; Information Security Management Systems; Information Security; Methodologies for risk analysis.

1. INTRODUCCIÓN

Con la constante evolución tecnológica, la seguridad de la información es una necesidad de cualquier organización, ya que se convierte en el recurso más valioso al momento de tomar decisiones y plantear nuevas estrategias del negocio. Al manejar la información en la organización se deben considerar las vulnerabilidades existentes y las posibilidades de ataques por cibercriminales. Es común escuchar acerca del tráfico, espionaje y robo de información; empresas como Adobe, eBay, Heartland y Sony PlayStation Network, cada una con más de 100.000 millones de cuentas de usuario, fueron objeto de ataques informáticos que dieron como resultado el robo de información como: cuentas bancarias, números de tarjetas, listas de correos electrónicos, y contraseñas (ED economíaDigital, 2016).

Con estos antecedentes, se presenta la necesidad de considerar a la seguridad de la información como un requisito fundamental de la organización, basándose en un conjunto de medidas que tienen el objetivo de prevenir, resguardar y proteger la información, buscando asegurar los tres pilares de la seguridad: disponibilidad, integridad y confidencialidad. Para ello, es importante la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) (Susanto, Nabil Almunawar, & Chee Tuan, 2017) que garantice que la información no esté disponible a personas no autorizadas, manteniéndose exacta y completa, y, que esta pueda ser dispuesta por personas y organizaciones autorizadas cuando lo requieran.

Las bibliotecas manejan información sensible sobre sus usuarios tales como: cuentas de usuario, gestión de multas y la información bibliográfica de las publicaciones. Estos datos constituyen la materia prima para la gestión y funcionamiento del negocio, lo que la convierte en un activo de gran importancia que se debe proteger desde su origen hasta su destino. Sin embargo, no existe un sistema que gestione la seguridad de la información (Bayona, Chauca, Lopez, & Maldonado, 2015).

Con el desarrollo de un SGSI, basado en una metodología propia de análisis de riesgos para bibliotecas en particular y que además sea compatible con la ISO/IEC 27001: 2013, se permitirá garantizar los principios de seguridad de la información de los usuarios de las bibliotecas de la EPN. Este trabajo permite evitar la alteración, robo, pérdida y falta de disponibilidad de la información, solventar vulnerabilidades y mitigar riesgos en los sistemas que la afectan y contribuir a que los procesos del negocio en el sistema de bibliotecas de la EPN se realicen de manera segura (Bayona, Chauca, Lopez, & Maldonado, 2015).

Debido a que las bibliotecas manejan activos y procesos particulares afines a su línea de negocio, se realizó una revisión sistemática de la literatura de los SGSI orientado a las bibliotecas con el fin de entender las propuestas de gestión de la seguridad en esta área. En este estudio, se encontró como resultado el uso de modelos de gestión de seguridad que no son aplicables exclusivamente a Bibliotecas sino a negocios en general. Estos modelos están basados en el uso de la familia de normas ISO (Susanto, Nurbojatmiko, & Shobariah, 2016), (Valencia-Duque & Orozco-Alzate, 2017), (Aginsa, Matheus Edward, & Shalannanda, 2016), (Rodal Castro, 2016) y (Livshitz & Nikiforova, 2016).

En cada caso se utilizan metodologías de gestión de riesgos distintas como MAGERIT, OCTAVE, NIST 800-30, mostrándose como las más eficientes para la implementación de un SGSI. No obstante, es importante estudiar cada una de ellas con el objetivo de obtener una metodología mejorada y más eficiente que optimice la gestión de riesgos para los procesos de una biblioteca en particular, descartando pasos que no sean acordes e implementando aquellos que se ajusten a este modelo de negocio.

La norma ISO/IEC 27001:2013 ha sido desarrollada con el fin de servir como modelo para el establecimiento, implementación, seguimiento y mejora de un SGSI en cualquier tipo de organización (INTERNATIONAL STANDARD ISO/IEC 27001, 2013), basándose en sus propios objetivos y requerimientos de seguridad usando además, los controles sugeridos en la norma ISO/IEC 27002 (INTERNATIONAL STANDARD ISO/IEC 27002, 2013).

Esta norma ofrece orientación, coordinación, simplificación y unificación de criterios de seguridad de la información, pero no indica los pasos para su implementación, mostrándose necesario el uso de metodologías adicionales a esta norma como es el ciclo de Deming (Planear – Hacer – Chequear – Actuar) y metodologías de análisis de riesgos como MAGERIT, OCTAVE y NIST 800-30. Sin embargo, como las metodologías de análisis de riesgos son genéricas para cualquier tipo de organización, se realiza un análisis y optimización de las metodologías existentes para los activos y procesos de las bibliotecas, para finalmente adoptar esta metodología compatible con las normas ISO 27001 en la Biblioteca de la Escuela Politécnica Nacional para comprobar su eficiencia.

1.1. Pregunta de investigación

¿Es posible generar una metodología de análisis de riesgos optimizada para bibliotecas y aplicarlo en un SGSI basado en el ISO/IEC 27001:2013?

1.2. Objetivo general

Desarrollar un sistema de gestión de la seguridad de la información para bibliotecas basado en una metodología mejorada de análisis de riesgos optimizado para los activos y procesos de una biblioteca y que sea compatible con la norma ISO/IEC 27001:2013

1.3. Objetivos específicos

- Inventariar los procesos de negocio, los procesos de tecnologías de la información que dan soporte a los procesos de negocio y finalmente, los activos relacionados con estos procesos.
- Identificar las amenazas a las cuales están expuestas los activos y procesos de las bibliotecas.
- Diseñar una metodología de análisis de riesgo optimizado para los activos y procesos de bibliotecas en base al estudio de metodologías existentes compatibles con la ISO /IEC 27001:2013
- Identificar y analizar los riesgos de seguridad de la información de los principales procesos identificados, aplicando la metodología diseñada.

1.4. Marco Teórico

1.4.1 Sistema de Gestión de la Seguridad de la Información

Un sistema de gestión de la seguridad de la información (SGSI) es un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

Un SGSI es, para una organización, el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. (INTERNATIONAL STANDARD ISO/IEC 27001, 2013)

1.4.2 ISO/IEC 27001:2013

Se ha puesto de manifiesto que las bibliotecas universitarias públicas deben afrontar el reto de gestionar la seguridad de su información, para ello, se utilizan normativas actuales relativas a dicho campo, la que se toma en cuenta en el presente proyecto es la ISO/IEC 27001:2013.

La ISO 27001 es una norma internacional que describe cómo gestionar la seguridad de la información en una empresa; puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. La revisión más reciente fue publicada en el 2013.

Su objetivo es asegurar la integridad, confidencialidad y disponibilidad de la información, esto se logra investigando los potenciales problemas que podrían afectar la información, posteriormente, definiendo lo necesario para evitar que estos problemas se produzcan nuevamente. Por tanto, el enfoque principal de las normas ISO 27001 está basado en gestionar riesgos y tratarlos sistemáticamente (INTERNATIONAL STANDARD ISO/IEC 27001, 2013).

Las medidas de seguridad que se van a implementar se presentan, bajo la forma de políticas, procedimientos, personas, bienes, etc. Por tal razón, la ISO 27001 detalla todos estos elementos dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Por eso, la gestión de la seguridad de la información no trata únicamente la seguridad de TI, sino también tiene que ver con la gestión de procesos, talento humano y protección física (INTERNATIONAL STANDARD ISO/IEC 27001, 2013).

Ventajas de la ISO/IEC 27001:2013

Las ventajas que una organización obtiene al implementar esta norma para asegurar su información son:

- **Obtener ventaja comercial:** Si la organización obtiene la certificación y sus competidores no lo hacen, se tiene una ventaja sobre ellos ante los clientes que requieren mantener la seguridad de su información, puesto que se incrementa su nivel de confianza.
- **Cumplir con requerimientos legales:** La norma proporciona una metodología adecuada para cumplir con todas las leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información.
- **Mejor organización:** Alienta a las organizaciones a definir sus procesos y procedimientos principales, incluso aquellos que no están relacionados con seguridad de la información, puesto que garantiza la continuidad del negocio.
- **Menores costos:** La implementación de la norma ayuda a evitar que se produzcan incidentes de seguridad, puesto que por cada incidente presentado sea este grande o pequeño se origina un gasto. Por tal motivo, esta norma ayuda a la organización a ahorrar dinero.

Estructura de la ISO/IEC 27001:2013

La ISO/IEC 27001:2013 proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un SGSI sin importar su enfoque empresarial; se divide en 11 secciones; las secciones 0 a 3 no son obligatorias para la implementación, mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar otros requerimientos si quiere cumplir con la norma (INTERNATIONAL STANDARD ISO/IEC 27001, 2013).

Descripción de las principales secciones

0. **Introducción:** Explica el objetivo de la norma y su compatibilidad con otras normas de gestión.
1. **Alcance:** Explica que esta norma es aplicable a cualquier tipo de organización.
2. **Referencias normativas:** Se proporcionan términos y definiciones del estándar
3. **Términos y definiciones:** Proporciona una guía de términos y definiciones consistente.
4. **Contexto de la organización:** Se identifican los problemas internos y externos que se presentan en la organización
5. **Liderazgo:** Destaca las responsabilidades de la Alta Dirección respecto al SGSI para demostrar su compromiso.
6. **Planeación:** Se definen los objetivos de seguridad, los que deben ser claros y específicos para ser alcanzados.
7. **Soporte:** Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye recursos, talento humano y comunicación de las partes interesadas.
8. **Operación:** Establece los requerimientos para medir el funcionamiento del SGSI y el cumplimiento del estándar.
9. **Evaluación del desempeño:** Se utilizan las auditorías internas para medir la efectividad y desempeño del SGSI.
10. **Mejora:** El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Ciclo de vida de la gestión de seguridad de la información

La gestión de la seguridad de la información consiste en un ciclo de planificar, hacer, revisar y actuar (PHVA). Este ciclo afecta a todos los niveles de la organización y se considera el Ciclo de vida de la gestión de la seguridad de la información. Su objetivo es asegurar la correcta comprensión de las necesidades del negocio y sus riesgos asociados de forma que se diseñen formas de buen gobierno, estrategias, tácticas y operaciones de seguridad sólidas (Vivancos Cerezo, 2018).

La norma ISO/IEC 27001:2013 adopta este modelo (PHVA) para aplicar a todos los procesos SGSI. A continuación, se detalla cada una de las etapas del modelo PHVA:

Planear: Establecer SGSI

En esta etapa se define la política de seguridad de la organización que incluya objetivos de seguridad, los activos que son protegidos, los responsables de cumplir dicha política, y debe estar aprobada por la directiva de la organización. Además, definir la metodología de evaluación de riesgos (inventario de activos, amenazas, vulnerabilidades, impactos) y analizar los riesgos (Narvaez Barreiros, 2018).

Ejecutar: Implementar y utilizar el SGSI

En esta etapa se cuenta con un plan de tratamiento de riesgos, para establecer de forma precisa los controles que son requeridos, además de asignar responsabilidades y establecer procedimientos, además de esquemas de controles necesarios que permitan una solución rápida a los incidentes de seguridad (Narvaez Barreiros, 2018).

Revisar: Monitorear y revisar el SGSI

En esta etapa se ejecuta procedimientos de revisión y monitoreo con el fin de detectar errores que pueden generarse en los resultados obtenidos en el procesamiento de información, y detectar posibles incidentes de seguridad. El objetivo es determinar si los controles implementados en el punto anterior fueron efectivos (Narvaez Barreiros, 2018).

Actuar: Mantener y mejorar el SGSI

En esta etapa se implementa en el SGSI las mejoras identificadas asegurándose que las mismas alcancen los objetivos previstos. PCDA es un ciclo de vida continuo motivo por el cual es obligatorio implementar el SGSI cada cierto tiempo (Narvaez Barreiros, 2018).

Controles de seguridad de la norma

Para gestionar la seguridad, la ISO/IEC 27002:2013 provee una lista de medidas de seguridad (dominios) que pueden ser usadas para mejorar la seguridad de la información (INTERNATIONAL STANDARD ISO/IEC 27002, 2013). Los controles quedan agrupados de la siguiente forma:

- A.5 Política de seguridad: Su propósito es escribir y revisar las políticas de seguridad
- A.6 Organización de la información de seguridad: controles acerca de cómo se asignan las responsabilidades.
- A.7 Seguridad de los recursos humanos: Su propósito es definir controles respecto al recurso humano de la organización.
- A.8 Gestión de recursos: lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento
- A.9 Control de acceso: controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario
- A.10 Criptografía: controles relacionados con la gestión de encriptación y claves
- A.11 Seguridad física y ambiental: controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.
- A.12 Seguridad operacional: muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.
- A.13 Seguridad de las comunicaciones: controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.
- A.14 Adquisición, desarrollo y mantenimiento de sistemas: controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte

- A.15 Relaciones con los proveedores: controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores

- A.16 Gestión de incidentes en Seguridad de la Información: controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias

- A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio: controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI

- A.18 Cumplimiento (legales, de estándares, técnicas y auditorías): Controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información

1.4.3 Gestión de riesgos

En el mundo de las TICS existen varias metodologías para tratar los riesgos; en este trabajo se detalla el análisis de algunas metodologías de gestión de riesgos para identificar sus bondades. Las metodologías a analizar son: MAGERIT v.3, OCTAVE v.2 y NIST 800-30.
MAGERIT y OCTAVE están basados en la familia de las normas ISO 27001 y son las más utilizadas a nivel mundial, esto se debe a que la documentación de MAGERIT está en idioma español y la documentación de OCTAVE es muy resumida en cuanto a la identificación de los activos de la organización y no los clasifica en exceso. NIST tiene como objetivo primordial la evaluación de los riesgos que soportan los sistemas de tecnología de la información.
Con estas premisas, se explican las metodologías antes mencionadas y los pasos utilizados para analizar el negocio, identificar las amenazas, las vulnerabilidades asociadas, determinar la probabilidad de ocurrencia, además del impacto de esas amenazas en caso de su materialización y por último, la obtención del riesgo al que está expuesto.

Metodología MAGERIT

La metodología MAGERIT se encarga de analizar los riesgos mediante un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización teniendo en cuenta los riesgos derivados del uso de las TICS. La versión 3.0

es compatible con las normas ISO 27001:2013 alineando la gestión de riesgos a un marco de trabajo de la organización (Portal de Administración Electrónica, 2012).

Los objetivos de MAGERIT son los siguientes:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Según la guía de Magerit, se deben seguir cinco pasos para analizar los riesgos en una organización, los cuales abarcan todas las posibles situaciones que se pueden presentar en los distintos negocios. A continuación, se detallan los pasos de la metodología:

1. **Activos:** Son los elementos del sistema de información susceptibles a ser atacados que soportan la misión del negocio. Magerit ofrece una lista normalizada de activos los cuales se seleccionan en base a la necesidad del negocio. (Esquema Nacional de Seguridad, 2012)

   Una vez identificados los activos, surge la necesidad de protegerlos, para ello, se requiere dimensiones de seguridad para valorar las consecuencias de la materialización de una amenaza; por tanto, se valora en base a:

   - Integridad
   - Confidencialidad
   - Disponibilidad
   - Autenticidad
   - Trazabilidad

Para determinar la valoración de cada dimensión se realizan evaluaciones cualitativas y cuantitativas.

2. **Amenazas:** Son incidentes que pueden afectar a los activos identificados causando daños potenciales en la organización. Magerit ofrece una lista normalizada de posibles amenazas (Esquema Nacional de Seguridad, 2012).

Una vez identificadas las amenazas que pueden perjudicar los activos, se debe valorar la influencia sobre el activo al que afecta, su probabilidad de ocurrencia y riesgo potencial. Para ello, también se realiza, una valoración cualitativa del nivel de daño que causa en el activo.

3. **Salvaguardas**: Son medidas de protección desplegadas para que aquellas amenazas no causen daño (Esquema Nacional de Seguridad, 2012).

4. **Impacto residual:** Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual. El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación (Esquema Nacional de Seguridad, 2012).

5. **Riesgo residual:** Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual (Esquema Nacional de Seguridad, 2012).

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento. Existen múltiples formas de tratar un riesgo, tales como: evitar las circunstancias que lo provocan, reducir las posibilidades de que ocurra, acotar sus consecuencias, compartirlo con otra organización (típicamente contratando un servicio o un seguro de cobertura), o en última instancia, aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario.

Las tareas de análisis y tratamiento de los riesgos son importantes en gestión de riesgos puesto que no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad. Finalmente elaborar la documentación del proceso siguiendo plantillas estandarizadas por Magerit (Esquema Nacional de Seguridad, 2012).

Metodología OCTAVE

Actualmente las organizaciones se centran únicamente en las deficiencias de la infraestructura; más no en sus activos de información. Por tal razón, Octave es una de las metodologías de análisis de riesgos más utilizadas por las empresas puesto que permite identificar los riesgos en sus activos más importantes y crear planes de mitigación para tratar dichos riesgos mediante criterios de OCTAVE; estos criterios se implementaran de manera diferente en una organización muy grande que en una muy pequeña, pero ambos pueden usar el mismo catálogo de prácticas.

El catálogo de prácticas comprende de una colección de buenas prácticas de seguridad para determinar qué se está haciendo actualmente bien con respecto a su estrategia de protección actual y lo que no está haciendo bien (sus vulnerabilidades organizacionales). También se usa como una base para definir estrategias de mejora de seguridad y planes de mitigación de riesgos (Alberts, Dorofee, & Allen, 2001).

Octave posee las siguientes características:

- Es diferente de los análisis tradicionales enfocados a la tecnología
- Es auto-dirigido
- Flexible

Los objetivos de OCTAVE son los siguientes:

- Permitir la comprensión del manejo de los recursos
- Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización
- Exige llevar la evaluación de la organización y del personal de la tecnología de información

Según el método Octave, se deben seguir tres fases para analizar los riesgos en una organización, los cuales abarcan todas las posibles situaciones que se pueden presentar en las distintas empresas. A continuación, se detalla cada una de ellas:

1. **Creación de perfiles de amenaza en base a los activos informáticos**: El equipo de análisis determina qué activos son los más importantes para la organización

(activos críticos) y que se está haciendo para protegerlos. Para ello, OCTAVE propone encuestas para recopilar la información sobre las buenas prácticas de seguridad, activos, amenazas y requisitos de seguridad utilizados en la organización desde el punto de vista de cada rol del equipo de trabajo. Una vez recopilada la información de todos los integrantes se crea perfiles de amenazas en base a los activos críticos seleccionados (Alberts, Dorofee, & Allen, 2001).

2. **Identificar vulnerabilidades de infraestructura:** Es una evaluación de la infraestructura de información, se examina los componentes operativos clave para las vulnerabilidades tecnológicas. Para ello, se identifica los sistemas y componentes clave de la tecnología de la información para cada activo crítico y evaluarlos, usando herramientas de vulnerabilidad (software, listas de verificación, scripts). Los resultados se examinan y se resumen, buscando la relevancia para los activos críticos y sus perfiles de amenazas (Alberts, Dorofee, & Allen, 2001).

3. **Desarrollar planes de seguridad y estrategia:** Durante esta parte de la evaluación, el equipo de análisis identifica los riesgos para los activos críticos de la organización identifica el impacto de las amenazas y decide si se deben abordar esos riesgos desarrollando una estrategia de protección para la organización y planes de mitigación para los activos críticos (Alberts, Dorofee, & Allen, 2001).

Esta metodología se basa en resultados puesto que después de la primera iteración (2-3 meses) se obtiene un plan a corto plazo y un plan estratégico a largo plazo para mitigar los riesgos detectados. En la siguiente iteración (después de 6 meses o un año) se parte de los resultados de la implantación de las acciones anteriores (Alberts, Dorofee, & Allen, 2001).

Metodología de riesgos NIST 800-30

Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito. Su objetivo final es ayudar a las organizaciones a gestionar mejor los riesgos la evaluación, mitigación y

análisis y evaluación del riesgo (National Institute of Standards and Technology, 2012). Por tanto, esta metodología está compuesta por 4 pasos básicos para la gestión del riesgo:

1. **Preparación para la evaluación**: En este paso, las actividades clave son: identificar el propósito y alcance de la evaluación de riesgos, identificar suposiciones y limitaciones bajo las cuales se realiza la evaluación del riesgo, identificar las fuentes de información sobre amenazas, vulnerabilidades e impactos en la evaluación de riesgos (National Institute of Standards and Technology, 2012).

2. **Evaluación de la conducta:** En este paso se realizan las siguientes tareas: identificar amenazas relevantes para la organización, identificar vulnerabilidades dentro de la organización que pueden ser explotadas por fuentes de amenazas, determinar la probabilidad de que las fuentes de amenazas identificadas inicien eventos de amenaza específicos y la probabilidad de que los eventos de amenaza sean exitosos, determinar los impactos adversos a las operaciones de la organización y activos y determinar los riesgos para la seguridad de la información como una combinación de la probabilidad de una amenaza de explotación de vulnerabilidades y el impacto de dicha explotación (National Institute of Standards and Technology, 2012).

3. **Comunicar resultados:** En este paso, las actividades claves son: determinar el método apropiado para comunicar a las partes interesadas los riesgos tal como un informe de resultados basándose en las políticas de la organización (National Institute of Standards and Technology, 2012).

4. **Mantener la evaluación:** Las tareas a realizar en este paso son: determinar los factores de riesgo clave que se han identificado para el monitoreo continuo, su frecuencia y las circunstancias bajo las cuales se necesita actualizar la evaluación de riesgo, llevar a cabo tareas de evaluación según sea necesario y comunicar los resultados de la evaluación de riesgos posteriores al personal de la organización (National Institute of Standards and Technology, 2012).

NIST se destaca por la gestión de riesgos en proyectos de TI y alcanza niveles satisfactorios en hardware, software, bases de datos, redes y telecomunicaciones, pues en su estructura se establecen criterios de seguridad, siendo los más comunes, la confidencialidad,

integridad y disponibilidad, los cuales son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los elementos de TI. No obstante, al ser una metodología tan robusta, esta propiedad se convierte en una limitante para su aplicación en pequeñas empresas con altas limitaciones de recursos humanos (National Institute of Standards and Technology, 2012).

1.4.4 Comparación general de las metodologías

Realizando un cuadro comparativo de las características más importantes de estas tres metodologías se obtiene lo siguiente:

Tabla 1 - Cuadro comparativo de las metodologías de gestión de riesgos

Característica	MAGERIT	OCTAVE	NIST
Identificación de activos	Divide los activos de la organización en grupos variados, para identificar riesgos y tomar medidas para evitar así cualquier inconveniente.	En los activos considera a más de los sistemas también a las personas	No contiene información acerca de esta característica
Valoración de activos	Caracterización del valor que representan los activos para la organización así como de las dependencias entre los diferentes activos	No contiene información acerca de esta característica	No contiene información acerca de esta característica
Identificación de amenazas	Relación de las amenazas a las que están expuestos los activos	Identifican vulnerabilidades tanto organizativas como tecnológicas que exponen a las amenazas creando un riesgo a la organización. Consolidación de la información y creación de perfiles de amenazas	Define amenazas, vulnerabilidades, riesgos y controles. Con los criterios de seguridad: confidencialidad, integridad y disponibilidad, realiza el análisis y valoración de amenazas e impactos sobre los elementos de TI
Identificación de vulnerabilidades	No contiene información acerca de esta característica	Identifica los elementos críticos y	No contiene información acerca

		las amenazas para los activos	de esta característica
Determinación del riesgo	Ofrece un método para analizar los riesgos detectados. Programa de seguridad que permiten materializar las decisiones de gestión de riesgos	Se especializa en el riesgo organizacional	Ayuda a las organizaciones a que los objetivos y alcance de la gestión de riesgos concluyan con éxito. Se destaca por la gestión de riesgos en proyectos de TI. Posee perfiles claves dentro de la organización respecto a la responsabilidad de la administración del riesgo
Selección y recomendación de contramedidas	Permite planificar las medidas adecuadas para mantener los riesgos bajo control Prepara a la organización para procesos de evaluación, auditoría, certificación, según corresponda en cada caso.	Desarrolla estrategias de protección tales como planes de mitigación de riesgos para mantener los objetivos organizacionales	No contiene información acerca de esta característica
Comunicar resultados	No contiene información acerca de esta característica	No contiene información acerca de esta característica	Determinar el método apropiado para comunicar a las partes interesadas los riesgos
Costo	Es gratuita pero limitada. Se puede solicitar la versión ampliada	Se debe pagar la licencia para su utilización	Se debe pagar costo de licencia

En la Tabla 1 se puede observar que las tres metodologías persiguen un mismo objetivo el cual es analizar y gestionar el riesgo y seguridad de la información de la organización.

1.4.5 Bibliotecas Universitarias: Conceptos Generales

Debido a que la metodología a desarrollarse está orientada a las Bibliotecas Universitarias, también es necesario conocer algunos conceptos generales de estas entidades.

Las bibliotecas universitarias

La información digital ofrece muchas posibilidades en todos los campos del saber, y sus aplicaciones, en el mundo actual. La propagación del uso de las tecnologías de la información ha revolucionado la existencia humana en todos los ámbitos: la educación, la economía, la cultura, la democracia, sociedad, etc., situando a la información en el centro de producción de riqueza.

En este entorno cambiante y globalizado, los sistemas y servicios bibliotecarios tradicionales están siendo reemplazados por nuevas prácticas: colecciones digitales, automatización de bibliotecas, redes y consorcios de bibliotecas, iniciativas de acceso abierto, etc.

Las bibliotecas universitarias, orientadas al soporte a la docencia y la investigación, se ven fuertemente afectadas por la expansión de las TICS, que ofrecen nuevas formas de comunicación y de difusión. Sus servicios tradicionales se ven desbordados por las posibilidades tecnológicas y los vertiginosos cambios que la sociedad de la información impone. También se vislumbran para las bibliotecas universitarias, nuevas oportunidades como gestoras del conocimiento universitario, en lugar del tradicional papel que tenían como depositarias del mismo; están experimentando cambios sustanciales como consecuencia de las nuevas tecnologías.

Desde los primeros pasos en la automatización, a los que siguieron los catálogos en línea y las bibliotecas digitales, hasta los proyectos actuales que incluyen la integración en las bibliotecas de servicios propios de la Web 2.0, entre otros: blogs, chats, foros y espacios wiki. Las bibliotecas universitarias van incorporando los cambios que ofrecen las tecnologías de acuerdo a su idiosincrasia particular, sus necesidades y los objetivos del entorno universitario en el que están inmersas; y tienen por objetivos:

- Ser agente difusor de los conocimientos de su universidad: los repositorios institucionales
- Ser un centro de recursos para el aprendizaje y la investigación para conseguir los fines educativos propuestos
- Ofrecer nuevos servicios: integración de bibliotecas digitales en los campus virtuales para potenciar el aprendizaje

- Brindar servicios de calidad al usuario final

Las Bibliotecas Universitarias tienen como público objetivo la comunidad universitaria. Formando parte de ésta podemos distinguir: los alumnos de la universidad a la que la biblioteca representa, los profesores e investigadores, el personal administrativo y usuarios particulares. Las TIC utilizadas son estándares entre las bibliotecas universitarias para los procesos técnicos y los servicios a través de la web con especial atención al acceso remoto a los recursos electrónicos. Además de las tecnologías básicas, cabe destacar que se cuenta con acceso inalámbrico (Wi-Fi) en las universidades. Mención singular, por su importancia para la seguridad de la información, merece la preservación de documentos físicos y digitales y datos de usuarios de la biblioteca.

Los entornos universitarios tienen ciertas características que afectan a la forma en la que aceptan e incorporan las tecnologías de la información:

- Son abiertos y flexibles por naturaleza facilitando la equidad en la distribución del conocimiento sin imponer límites a su difusión;
- Tanto si son de financiación pública como privada están sujetos a las regulaciones nacionales;
- Su estructura organizativa es mixta (docencia, investigación y gestión), con estamentos con niveles de autonomía dispares que hacen compleja la uniformidad de equipamiento y procesos informáticos.

Estas características influyen también en las bibliotecas universitarias en cuanto que forman parte de una universidad y contribuyen a los objetivos de ésta. De todo lo expuesto se desprende que la complejidad de los entornos universitarios se traslada a la organización de las TIC en las Bibliotecas. El caso más general en estas instituciones, las universidades, es que los recursos informáticos estén a cargo de un área específica en su organización que ofrecen sus servicios al resto de la estructura. Tal es el caso de la Escuela Politécnica Nacional y su sistema de bibliotecas, cuyos servicios reposan en el apoyo y soporte físico y lógico que presta la Dirección de Gestión de la Información y Procesos (DGIP), con personal dedicado exclusivamente a la Biblioteca.

La financiación de los fondos bibliográficos de las Bibliotecas Universitarias públicas es muy compleja porque sus fondos son adquiridos con presupuesto del estado, el cual le otorga directamente a la universidad a la que pertenece y se distribuye una cantidad muy escasa para la gestión de las bibliotecas.

2. METODOLOGÍA PARA EL DESARROLLO DEL PROYECTO

La metodología Action Research se define como un enfoque en el que el investigador y el cliente colaboran en el diagnóstico del problema y en el desarrollo de una solución basada en dicho diagnóstico. En otras palabras, una de las principales características de Action Research es la colaboración entre el investigador y los miembros de la organización con el fin de solventar problemas de la organización (Reason & Bradbury, 2001).

Esta metodología posee tres pasos que se adaptan fácilmente para el desarrollo del presente proyecto. A continuación, se explica los aspectos considerados en cada etapa de la metodología dimensionados al proyecto:

2.1. Explicación de la metodología

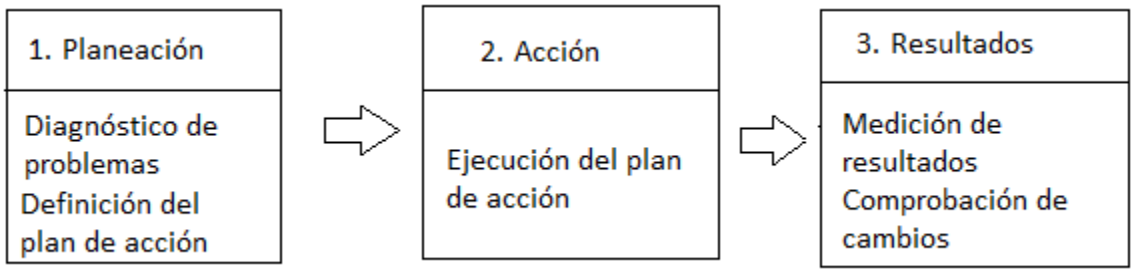

***Figura* 1 -** Pasos de la metodología Action Research

Creado en base al contenido de *(Reason & Bradbury, 2001)*

Como primer paso, se realiza una planificación procedente de un diagnóstico preliminar en el cual se detectan los problemas aún no identificados en la organización.

Como siguiente paso, se tiene la fase de acción, en esta etapa incluye acciones relacionadas con el problema con el fin de ejecutar cambios de comportamiento en la organización para dar solución al problema detectado y obtener resultados.

Finalmente, se evalúan los resultados obtenidos a fin de verificar si estos cumplen con los objetivos planteados en este proyecto. Mediante auditorías internas, se aplican técnicas tales como: entrevistas y encuestas (Reason & Bradbury, 2001). Cabe recalcar que esta metodología es cíclica.

En el presente proyecto a desarrollar, se informará oportunamente la aplicación de los pasos de esta metodología.

2.2. Análisis de las metodologías existentes de análisis de riesgos

2.2.1 Generalidades

Debido a que las bibliotecas manejan activos y procesos particulares afines a su línea de negocio, se realizó una revisión sistemática de la literatura de los SGSI orientado a las bibliotecas universitarias con el fin de entender las propuestas de gestión de la seguridad en esta área.

En estos casos de estudio que están basados en el uso de la familia de normas ISO 27000 (Susanto, Nurbojatmiko, & Shobariah, 2016), (Valencia-Duque & Orozco-Alzate, 2017), (Aginsa, Matheus Edward, & Shalannanda, 2016), (Rodal Castro, 2016) y (Livshitz & Nikiforova, 2016). En cada caso se utilizan metodologías de gestión de riesgos distintas como MAGERIT, OCTAVE, NIST 800-30, mostrándose como las más eficientes para la implementación de un SGSI. Del estudio realizado, se concluye que no existe un SGSI exclusivo para bibliotecas universitarias, por lo tanto, se plantea la importancia del desarrollo de una metodología de análisis de riesgos optimizada para bibliotecas universitarias.

En base al análisis realizado a las diferentes metodologías de gestión de riesgos mencionadas en el capítulo anterior, se puede rescatar lo más importante de cada una con el fin de estructurar una metodología de análisis de riesgos orientada al negocio de las bibliotecas universitarias públicas y que sean compatibles con la norma ISO/IEC 27001:2013.

Características de MAGERIT para bibliotecas

La norma ISO/IEC 27001:2013 exige la realización de un inventario de activos ya que es la mejor manera de comenzar a trabajar. Sin embargo, esta tarea resulta complicada cuando no se sabe lo que se tiene dentro de la organización. Por esta razón, es importante mantener actualizado el inventario de los activos con revisiones periódicas.

Los activos son materiales sobre los cuales se pueden tomar medidas preventivas para protegerlos, principalmente de amenazas como pueden ser: agua, fuego, etc., y otros activos que soportan la carga de información dentro del activo físico como son: servidores virtuales, sistemas de gestión de bibliotecas, sistemas gestores de bases de datos, etc.

Al poseer un inventario de activos detallado, es importante la identificación de amenazas, ya que permite detectar los riesgos que pueden afectar a los activos. Las amenazas de una organización dependen mucho de su entorno, localización y actividad. Sin embargo, existen un conjunto de amenazas comunes entre las que destacan las siguientes: fuego, pérdida, agentes climáticos, errores de usuario, daños por agua, sobrecargas eléctricas, accesos no autorizados, etc.

La función de salvaguarda, a la hora de implementar un SGSI según la ISO/IEC 27001:2013, es una acción de tipo actuación que nace de la decisión para reducir el riesgo ante la materialización de una amenaza. La práctica de una salvaguarda es un atributo que mide la resistencia del ataque directo y se mide la fuerza que tiene que emplear el agente agresor para doblegar las salvaguardas.

Para lograr desarrollar un SGSI que sea robusto y libre de errores en su implementación se puede reconocer como primer paso el inventariar los activos de las bibliotecas universitarias, como segundo paso, reconocer las amenazas a las que los activos se pueden enfrentar y como tercer paso es importante la selección de salvaguardas que ayuden a contrarrestar las amenazas identificadas.

Magerit propone un detalle de activos, inventario de amenazas y, por último, un catálogo de salvaguardas que corresponde a contrarrestar las amenazas. Por esto, se ha seleccionado estos tres pasos de esta metodología:

1. **Activos:** Son los elementos del sistema de información susceptibles a ser atacados que soportan la misión de la biblioteca. Se determinan los siguientes tipos de activos:
    a. Información: Es aquella que se maneja en la biblioteca y le permite prestar sus servicios tales como la información de carácter personal de los usuarios y del material bibliográfico existente.
    b. Aplicaciones informáticas: Es el software que le permite a la biblioteca gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios de préstamo y devolución de publicaciones, gestión de usuarios, catalogación y elaboración de informes. Para brindar dichos servicios, se utiliza el Sistema Integrado de Bibliotecas Koha versión 17.11.09 y el Repositorio Digital DSPACE para la visualización de archivos digitales.
    c. Equipos informáticos: Son medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la biblioteca, siendo pues

depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. En la biblioteca se cuenta con los siguientes: medios de impresión, escáneres, routers, teléfonos IP y varias computadoras personales y portátiles.

d. Soportes de información: Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. Se tiene CD-ROM los cuales contienen los requisitos de grado que los estudiantes entregan en la biblioteca previa a su graduación.

Magerit propone un amplio abanico de tipos de activos sin embargo, para el presente trabajo se seleccionaron únicamente cuatro (Información, Aplicaciones informáticas, Equipos informáticos y Soportes informáticos), puesto que estos se ajustan al modelo de negocio de las bibliotecas.

Una vez identificados los activos, surge la necesidad de protegerlos. Para ello, se requiere dimensiones de seguridad para valorar las consecuencias de la materialización de una amenaza. Magerit propone cinco dimensiones de seguridad como son integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad. Los cuatro primeros se ajustan al modelo de negocio a excepción de la última que es trazabilidad. Esta dimensión pretende disponer de un control completo de acciones y uso que se le da a un determinado activo, sin embargo, los activos de las bibliotecas no solo corresponden a esta dependencia, por ejemplo: la red de datos que es administrada por la Unidad de Informática de la organización y esta no puede contar con un control de acciones ya que se estaría involucrando en otro departamento.

Por tanto, los activos serán valorados en base a:

- Integridad: Se refiere a datos que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos. ¿Qué perjuicio causaría que los datos ingresados en el sistema estuvieran dañados o corruptos?
- Confidencialidad: Se refiere a información personal de los usuarios. ¿Qué daño causaría que esta información sea conocida por quien no debe?
- Disponibilidad: Es orientada a los servicios que presta la biblioteca. ¿Qué perjuicio causaría no tener o no poder utilizar el Sistema Integrado de Bibliotecas?

- Autenticidad: Se refiere a servicios (autenticidad del usuario) y datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar). ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho uso del Sistema Integrado de Bibliotecas?

Para determinar la valoración de cada dimensión se realizan evaluaciones cuantitativas con escalas de valoración desde 0 como irrelevante hasta 4 como daño extremadamente grave (Esquema Nacional de Seguridad, 2012).

2. **Amenazas:** Son incidentes que pueden afectar a los activos identificados causando daños potenciales en la biblioteca. Magerit brinda un catálogo de amenazas, de las cuales se seleccionó todas las categorías y solamente las subcategorías que se adaptan a las bibliotecas universitarias. Tomando en cuenta la situación actual, entre los problemas que se pueden presentar se identifica las siguientes:

- Desastres naturales: Terremotos, incendios,
- De origen industrial: Contaminación, fallos eléctricos, polvo, condiciones inadecuadas de temperatura, degradación de los soportes de información
- Errores y fallos no intencionados: Equivocaciones de las personas cuando usan los servicios, falta de registros, difusión de software dañino, escape de información, alteración accidental de información, pérdida accidental de la información, pérdida de equipos.
- Ataques intencionados: suplantación de la identidad del usuario, abuso de privilegios de acceso, uso de datos con fines personales, acceso no autorizado, interceptación de información, eliminación intencional de la información, revelación de la información y manipulación del sistema.

Una vez identificadas las amenazas que pueden perjudicar los activos, se debe valorar la influencia sobre el activo al que afecta, su probabilidad de ocurrencia y determinación del riesgo potencial. Para ello, también se realiza, una valoración cualitativa del nivel de daño que causa en el activo desde muy bajo hasta muy alto y la probabilidad de ocurrencia desde muy poco frecuente a muy frecuente (Esquema Nacional de Seguridad, 2012).
El riesgo crece con el impacto y la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento de riesgo:

- Zona 1: Riesgo muy probables y de muy alto impacto

- Zona 2: Desde riesgos improbables y de impacto medio hasta riesgos muy probables pero de impacto muy bajo
- Zona 3: Riesgos improbables y de bajo impacto
- Zona 4: Riesgos improbables pero de muy alto impacto

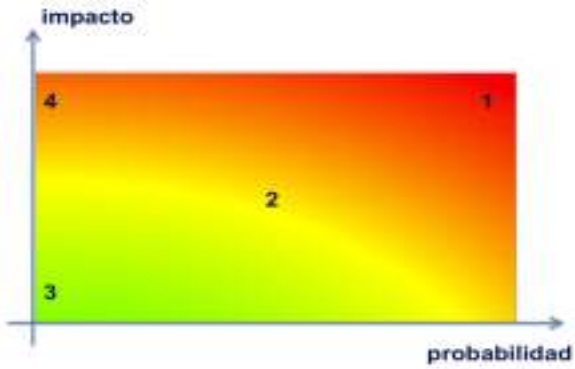

Figura 2 - El riesgo en función del impacto y la probabilidad

Fuente (Esquema Nacional de Seguridad, 2012)

3. **Salvaguardas**: Son medidas de protección desplegadas para que aquellas amenazas identificadas en las bibliotecas universitarias no causen daño en sus activos (Esquema Nacional de Seguridad, 2012).

Para seleccionar las salvaguardas, se debe considerar:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica
- Dimensión o dimensiones de seguridad que requieren protección
- Amenazas de las que necesitamos protegernos

Las salvaguardas que se ajustan a este modelo de negocio, se seleccionaron del catálogo de elementos de Magerit (Esquema Nacional de Seguridad, 2012) que a continuación se detallan:

- Copias de seguridad de los datos
- Protección de equipos informáticos
- Protección de los soportes informáticos
- Aseguramiento de la disponibilidad
- Reproducción de documentos
- Plan de recuperación de desastres

- Limpieza de contenido
- Climatización
- Identificación y autenticación
- Aseguramiento de la integridad
- Gestión de claves criptográficas
- Aplicación de perfiles de seguridad
- Uso de herramientas de chequeo de configuración
- Cifrado de la información
- Protección criptográfica del contenido de los soportes de información
- Uso de herramientas para análisis de logs
- Protección de la información
- Gestión de cambios
- Formación y concienciación al usuario
- Protección de la integridad de los datos intercambiados
- Protección criptográfica de la confidencialidad de los datos intercambiados
- Protección de las comunicaciones
- Autenticación del canal de comunicaciones

Características de OCTAVE para bibliotecas

Las vulnerabilidades de un activo frente a una amenaza siempre son asociadas a la pérdida de confidencialidad de su información, la integridad de la misma y su disponibilidad a la hora de ser utilizada por quien la necesite. Este concepto ayuda a identificar las vulnerabilidades de cada activo y con esto se reconocen los riesgos.

La norma ISO/IEC 27001:2013 supone llevar a cabo un plan de seguridad; esto conlleva a cumplir objetivos estratégicos, al permitir valorar el riesgo que la organización está enfrentando y concientizar a los sectores técnicos y de negocios de la importancia que ejerce la seguridad informática en una organización. Sin embargo, el objetivo que persigue la organización debe ser dinámico y aceptable, además de permitir que la gestión de la seguridad se realice desde un plano estratégico.

La metodología OCTAVE plantea la identificación de vulnerabilidades y el desarrollo de planes de seguridad y esto es un aporte importante ya que la metodología MAGERIT no propone como un paso independiente, la detección de debilidades en la organización. Por lo tanto, como complemento a los tres pasos obtenidos de Magerit (Activos, Amenazas y

Salvaguardas), se selecciona la identificación de vulnerabilidades y el desarrollo de planes de seguridad para robustecer esta metodología optimizada de riesgos para bibliotecas universitarias. A continuación, se da una breve explicación de los pasos tomados de la metodología OCTAVE:

1. **Vulnerabilidades:** Se identifica los sistemas y componentes clave de la tecnología de la información para cada activo crítico y evaluarlos usando la herramienta **Microsoft Security Assessment Tool,** la cual ayuda a empresas de menos de 1.000 empleados a evaluar los puntos débiles de su entorno de seguridad de TI. Los resultados obtenidos se examinan y se resumen, buscando la relevancia para los activos críticos y sus perfiles de amenazas (Alberts, Dorofee, & Allen, 2001).

2. **Desarrollar planes de seguridad:** Se elabora el plan de seguridad de la biblioteca con el fin de abordar los riesgos encontrados y desarrollar una estrategia de protección para la organización y para los activos críticos. Este documento contiene los siguientes puntos: Introducción, desarrollo de políticas de seguridad para varias áreas de la biblioteca, verificación de cumplimiento, presupuestos y resultados.

Características de NIST 800-30 para bibliotecas

Tanto la metodología Magerit como Octave, carecen de una propuesta de comunicación de resultados a diferencia de la metodología NIST. Es importante comunicar los resultados obtenidos luego del análisis de riesgos con el fin, que los involucrados tengan conocimiento de los hallazgos detectados. Por esto, se selecciona de la metodología NIST, comunicar los resultados como último paso de la metodología de análisis de riesgos optimizada para las bibliotecas universitarias. A continuación se da una breve explicación del paso tomado de la metodología de NIST:

1. **Comunicar resultados:** En este paso, las actividades claves son: determinar el método apropiado para comunicar a las partes interesadas los riesgos encontrados. En este caso puede ser útil una matriz de resultados basándose en las políticas de la organización (National Institute of Standards and Technology, 2012).

2.2.2 Cuadro de las características seleccionadas de las metodologías de análisis de riesgos existentes para aplicación en las bibliotecas

En la Tabla 2, se muestra las ventajas de cada una de las metodologías de riesgos aplicadas a las bibliotecas universitarias públicas. Por tal motivo, se puede combinarlas y aplicar una nueva metodología propuesta para este negocio. Se incorporan los elementos principales descritos anteriormente de cada una de las metodologías y valores que entregan como resultado una metodología nueva y consistente y a que a su vez permita aplicarla a la realidad de las bibliotecas universitarias públicas, en cuanto a riesgos informáticos se trate.

Tabla 2 - Características de las metodologías de riesgos

Característica	MAGERIT	OCTAVE	NIST
Recopilación de Activos	X		X
Identificación de Amenazas	X		
Selección de Salvaguardas	X		
Identificación de vulnerabilidades		X	
Desarrollar planes de seguridad		X	
Comunicar resultados			X

2.3. Propuesta de una nueva metodología de gestión de riesgos y su aplicación en un caso práctico

Una vez realizado el análisis de las metodologías existentes, se propone una metodología de Gestión de Riesgos para bibliotecas universitarias públicas, que permite identificar y gestionar los riesgos de tecnología de la información en cuestión.

Esta metodología propuesta tiene un enfoque de análisis de riesgos cualitativo, este enfoque emplea valoraciones de escala de niveles. Las escalas cualitativas permiten avanzar con rapidez, proporcionando el valor de cada activo en un orden relativo respecto de los demás.

2.3.1 Proceso (pasos)

Para la implementación del SGSI en las bibliotecas universitarias es necesario identificar ciertas características que ayudarán al levantamiento de la información, es decir, establecer un estado inicial del objeto de estudio, para luego realizar el análisis de riesgo. Esto ayudará a definir una correcta estructura del modelo del SGSI que se desea implementar. En la metodología se propone la ejecución de los siguientes pasos:

Paso 1: Identificación de roles

Las bibliotecas universitarias no se alejan de la realidad de una biblioteca tradicional ya que definen los mismos roles para su personal. Estos roles se pueden clasificar en:

- Miembros del equipo de biblioteca
- Director del proyecto, que normalmente será asignado al responsable de la Biblioteca

Paso 2: Análisis del Estado actual de la Biblioteca Universitaria

Una vez definido los roles, mediante una entrevista al equipo de proyecto, se obtiene el estado inicial de la organización. Para esto, se prepara un banco de preguntas tomadas de los controles especificados en la ISO/IEC 27002:2013 (ver Anexo J).

Paso 3: Análisis de riesgos basado en la metodología propuesta

Una vez identificado el estado de situación inicial de la biblioteca, se procede a implementar el SGSI con la metodología optimizada de análisis de riesgos, la cual cuenta con los siguientes pasos:

1. **Recopilación de Activos:** Se detalla los activos existentes en las bibliotecas universitarias especificando la cantidad, la ubicación y el responsable en la plantilla respectiva ubicada en el Anexo A. Los activos identificados, se los agrupa basándose en las cuatro categorías de activos seleccionadas de Magerit (Información, Equipos informáticos, Aplicaciones informáticas y Soportes Informáticos). Posteriormente, se procede a valorar cuantitativamente todos los activos respecto a las cuatro dimensiones de seguridad utilizando la plantilla ubicada en el Anexo B.

2. **Identificación de Amenazas**: Se identifica todas las amenazas que se puedan presentar basándose en las cuatro categorías seleccionadas de Magerit (Desastres naturales, de origen industrial, errores y fallos no intencionados y ataques intencionados) y se asocia al activo identificado que puede ser afectado. Esta información se recopila mediante la plantilla, ubicada en el Anexo C.

   A continuación, se procede a valorar cuantitativamente la materialización de la amenaza por cada activo afectado. Se considera el impacto y la probabilidad de ocurrencia de la misma. Con esta información se obtiene el riesgo potencial por activo clasificado en las zonas de riesgo que ofrece Magerit, se presenta la valoración de las amenazas utilizando el Anexo D.

3. **Identificación de vulnerabilidades:** Se ejecuta la herramienta Microsoft Security Assessment Tool para detectar las vulnerabilidades existentes en las bibliotecas universitarias. Esta herramienta contiene una serie de preguntas agrupadas por infraestructura, aplicaciones, operaciones y personal a las que se debe responder considerando la realidad del negocio, al final emite un informe de las debilidades existentes. Al entregar un informe muy extenso se debe rescatar las vulnerabilidades asociadas a los activos inventariados.

4. **Selección de Salvaguardas:** Para las amenazas identificadas, se seleccionan las salvaguardas que les hacen frente en caso de materializarse, además, se considera los controles de seguridad de la ISO/IEC 27002:2013 para cada amenaza. Todo lo expuesto se recopila en el Anexo E.

5. **Desarrollo de planes de seguridad:** Luego de identificar los problemas de seguridad y las acciones a tomar, se desarrolla un plan de seguridad para la ejecución de actividades que tienen como objetivo fortalecer la misma en las bibliotecas universitarias.

6. **Comunicación de resultados:** Mediante una matriz de resultados se comunican los hallazgos detectados al equipo de proyecto y responsable de bibliotecas en donde se detalla, por cada zona de riesgos, los activos afectados, las amenazas, vulnerabilidades y salvaguardas asociados a los mismos.

2.3.2 Implementación de la solución

Una vez desarrollada la metodología optimizada para bibliotecas, se la ha aplicado al sistema de bibliotecas de la Escuela Politécnica Nacional (EPN) con el fin de valorar si esta metodología se adapta de manera eficiente a este modelo de negocio, teniendo en cuenta que se han seleccionado pasos totalmente compatibles con la ISO/IEC 27001:2013. Adicionalmente, con esta aplicación práctica, se pretende que el sistema de bibliotecas de la EPN cuente con un SGSI que se adapte a sus necesidades y permita gestionar la seguridad de su información.

Descripción de la Organización del Caso del estudio: Bibliotecas de la EPN

Antes de aplicar los pasos iniciales para identificar los roles, estado actual y análisis de riesgo del objeto de estudio, es importante conocer su organización.

El Sistema de Bibliotecas de la EPN está conformado por la Biblioteca Central y diez Bibliotecas satélites localizadas en diferentes Facultades de la Institución, las cuales son gestionadas por veinte profesionales. A continuación, en la Tabla 3 se presenta cada Biblioteca, su distribución y el número de bibliotecarias con los que se cuenta:

Tabla 3 - Sistema de Bibliotecas de la EPN

Nombre	Ubicación	Bibliotecarios
Biblioteca Central	Planta baja del Edificio de Administración	6
Biblioteca de Ingeniería de Sistemas	Facultad de Sistemas, segundo piso	2
Biblioteca de Ingeniería Mecánica	Facultad de Mecánica, tercer piso	1
Biblioteca de Ingeniería Eléctrica y Electrónica	Facultad de Eléctrica, primer piso	2
Biblioteca de Ingeniería Civil y Ambiental	Facultad de Civil, tercer piso	1
Biblioteca de Ingeniería de Geología y Petróleos	Facultad de Geología y Petróleos	1
Biblioteca de Ingeniería Química y Agroindustria	Facultad de Química, sexto piso	2
Biblioteca del Instituto de Ciencias Biológicas	Museo de la EPN	1
Biblioteca de Ciencias	Edificio de Abastecimientos, quinto piso	1

Biblioteca de Ciencias Administrativas	Edificio del Medio Externo, cuarto piso	1
Biblioteca de Formación Básica	Edificio de Formación Básica, segundo piso	2
	Total	20

A continuación se describe la misión, visión, objetivos y estructura jerárquica del sistema de bibliotecas de la EPN, información obtenida a partir de una entrevista realizada a la Ing. Olga de Beltrán, Coordinadora de Bibliotecas de la EPN (Beltran, 2018).

Misión del Sistema de Bibliotecas de la EPN

"Proveer de recursos de información y materiales bibliográficos de calidad, a través de un sistema integrado dirigido a contribuir al desarrollo académico e investigativo de la comunidad politécnica." (Beltran, 2018).

Visión del Sistema de Bibliotecas de la EPN

"Satisfacer las necesidades de información de la comunidad politécnica y público en general automatizando procesos y servicios, basados en un sistema dinámico organizacional, mediante tecnología e innovación permanente" (Beltran, 2018).

Objetivo del Sistema de Bibliotecas de la EPN

"Tener una colección completa que responda a las necesidades educativas, formativas, investigativas y culturales, orientadas a suplir las necesidades de información de la comunidad politécnica y público en general, y constituirse en el fondo bibliográfico de mayor cobertura." Además, la biblioteca cuenta también con políticas de los servicios que brindan actualmente (Beltran, 2018).

Jerárquicamente dependen del Rectorado, a través de la Coordinación de Bibliotecas, como se representa en la Figura 3:

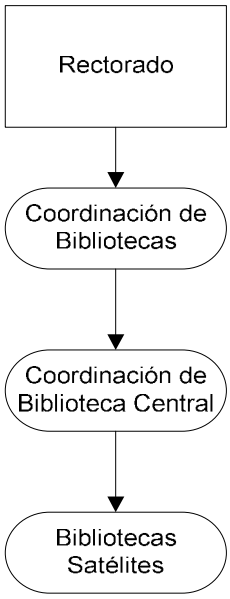

Figura 3 - Estructura Organizacional Bibliotecario

Fuente (Beltran, 2018)

Las bibliotecas de la EPN están divididas en las siguientes áreas:

- **Adquisición:** encargada de seleccionar el material demandado tomando en cuenta las necesidades de los usuarios (Bravo & Portilla, 2015).

- **Procesos Técnicos:** se encarga de recuperar el material bibliográfico físico dentro la misma. Los servicios brindados en esta área son:
  - **Catalogación:** extrae la información esencial que describe un libro como: título, autor, editorial, ISBN, etc. (Bravo & Portilla, 2015).

  - **Clasificación:** mantiene ordenada la colección de acuerdo al sistema de clasificación Dewey (Bravo & Portilla, 2015).

  - **Indización:** identifica la publicación en el sistema integrado de bibliotecas (Bravo & Portilla, 2015).

  - **Ingreso a Koha:** se encarga de ingresar las publicaciones en base al formato MARC 21 y reglas de catalogación RDA (Bravo & Portilla, 2015).

- **Circulación:** brinda el servicio de préstamo de las publicaciones, después de que estas pasaron por los procesos técnicos mencionados anteriormente. Las búsquedas de publicaciones se realizan mediante el catálogo electrónico institucional.
  A continuación, se describen los servicios y procesos que se brinda en el área de Circulación, considerada el área principal para el manejo de material bibliográfico físico dentro de la biblioteca (Bravo & Portilla, 2015).

    - **Préstamo de publicaciones:** Proporciona a los usuarios de la biblioteca el ítem solicitado y su respectiva devolución. El proceso comienza cuando el usuario realiza la búsqueda del ítem requerido; luego el usuario llena la ficha de pedido proporcionando al bibliotecario una credencial de identificación en del sistema. Una vez comprobada la existencia del usuario en el sistema, el bibliotecario hace la búsqueda del ítem solicitado en la colección y realiza la entrega del mismo (Bravo & Portilla, 2015).

    - **Reserva de publicaciones:** El estudiante realiza una reservación de publicaciones siempre y cuando el ítem solicitado se encuentre prestado, procediendo a solicitarle al bibliotecario que realice la reservación correspondiente (Bravo & Portilla, 2015).

    - **Renovación de publicaciones:** El proceso inicia cuando el usuario devuelve una publicación. El bibliotecario comprueba en el sistema que el ítem puede ser renovado, procediendo luego a realizar el préstamo durante el lapso de cuatro días, acatando a la norma de la Biblioteca Central: "*El estudiante tiene derecho a renovar su préstamo siempre y cuando exista más de un ejemplar en la colección del ítem.*" (Normas Biblioteca Central EPN, 2014).

    - **Generación y cobro de multas:** El proceso de generación de multas inicia cuando el usuario no entrega la publicación en el tiempo establecido. El sistema genera automáticamente el valor de la multa por día de atraso. Los valores establecidos para las multas de acuerdo a los perfiles de usuario son los siguientes:
        - Estudiantes: 25 centavos de dólar por día.
        - Docentes e investigadores: 50 centavos de dólar por día.

- Particulares: 1 dólar por día.

Una vez que el usuario devuelva el ítem, el bibliotecario procede a descargar el material bibliográfico de la cuenta del usuario y le informa el valor correspondiente de la multa; para el caso que el usuario cancele, esta es descargada de su cuenta, generando su respectivo recibo; caso contrario se mantiene la deuda pendiente hasta que esta sea cancelada. Los usuarios tienen acceso libre y gratuito a los fondos de la biblioteca con previa presentación del carné institucional o cédula de identidad los cuales son documentos personales e intransferibles (Bravo & Portilla, 2015).

- **Referencia:** proporciona una guía y ayuda al usuario con respecto a búsquedas de material bibliográfico; si éste no se encuentra en la Biblioteca General, el referencista envía al usuario a las bibliotecas satélites de la EPN o alguna de las bibliotecas que se encuentren dentro del perímetro externo siempre y cuando ellas dispongan del mismo (Bravo & Portilla, 2015).

A continuación, se detallan los servicios de esta área:

- **Biblioteca Digital:** La EPN posee suscripción a bases de datos multidisciplinares y especializados en distintas áreas del conocimiento a las que se puede acceder tanto dentro del Campus Politécnico como también vía remota (Bravo & Portilla, 2015).

- **Consulta en sala:** Para comodidad de los usuarios la biblioteca cuenta con un área confortable y segura para realizar consultas.

- **Servicio de Internet:** La biblioteca ofrece también un servicio gratuito de acceso a Internet con fines de búsqueda de información, estudio o investigación. El servicio está destinado a facilitar la consulta de recursos disponibles en la Red relacionados con las actividades académicas de la institución. Para hacer uso del servicio de Internet es necesario tener el carné de la EPN o la cédula de ciudadanía.

- **Firma del registro bibliográfico y formulario de no adeudar:** Servicio exclusivamente dirigido para los estudiantes en proceso de graduación. Este trámite se realiza únicamente en la Biblioteca Central; los requisitos previos a la firma se encuentran en la página de las Bibliotecas EPN, http://biblioteca.epn.edu.ec/ , en el apartado “Requisitos para Tesis”.

- **Repositorio digital:** A través de este servicio se puede acceder a toda la producción científica de la EPN, tanto tesis de pregrado y postgrado a partir del 2006 como otros contenidos académicos publicados por Investigadores y Docentes de la institución.

- **Capacitaciones:** Están dirigidas a investigadores, docentes, estudiantes y personal interno de bibliotecas sobre el uso y manejo de: Sistema de gestión de bibliotecas, reservas, renovaciones en línea, bibliotecas digitales, gestores bibliográficos y software antiplagio-turnitin, además de realizar vinculación con el medio externo.

- **Formación a usuarios:** La Biblioteca posee un programa permanente de formación de usuarios a través de capacitaciones cortas, disponiendo de manuales que explican cómo consultar en la biblioteca la bibliografía y los servicios que dispone.

- **Empastado y Reparaciones:** reparar el material bibliográfico deteriorado. En este caso, el bibliotecario entrega al auxiliar de biblioteca la publicación a ser reparada, pero si el deterioro se debe a una mala utilización por parte del usuario, se le pide que lo repare antes de su devolución (Bravo & Portilla, 2015).

Una vez que se ha entendido el objeto de estudio, se puede proceder a identificar los roles que existen dentro de esta organización.

Paso 1: Identificación de roles

En las bibliotecas de la EPN se han establecido roles predefinidos para su personal los cuales se detallan a continuación:

- Miembros del equipo de biblioteca:

    - Asistentes de TICS
    - Referencistas
- Director del proyecto:
    - Responsable de la Biblioteca

Paso 2: Situación del estado inicial del Sistema de Bibliotecas de la EPN

Como primer paso de la metodología Action Research “Planeación”, es necesario realizar un diagnóstico del estado inicial del sistema de bibliotecas de la EPN y definir el plan de acciones a tomar, para ello, se propone una entrevista al Asistente de TICS responsable (01 persona), quien puede ayudar a conocer la situación actual en materia de seguridad de este negocio. Los resultados obtenidos se detallan a continuación:

Tabla 4 - Resultados de la entrevista al equipo de proyecto

Preguntas	Respuestas
POLÍTICAS DE SEGURIDAD:	
¿Existen documento(s) de políticas de seguridad de Sistema de Información?	NO
¿Existe normativa relativa a la seguridad del Sistema de Información?	NO
¿Existen procedimientos relativos a la seguridad de Sistema de Información?	NO
¿Existe un responsable de las políticas, normas y procedimientos?	NO
¿Existen mecanismos para la comunicación a los usuarios de las normas?	NO
¿Existen controles regulares para verificar la efectividad de las políticas?	NO
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:	
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	NO
¿Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información?	NO
¿Participan la Dirección y las áreas de la Organización en temas de seguridad?	NO
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?	NO
¿Existen criterios de seguridad en el manejo de terceras partes?	NO
¿Existen programas de formación en seguridad para los empleados, clientes y terceros?	NO
¿Existe un acuerdo de confidencialidad de la información que se accede?	NO
¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?	NO
GESTIÓN DE ACTIVOS:	
¿Existen un inventario de activos actualizado?	NO
¿El Inventario contiene activos de datos, software, equipos y servicios?	NO
¿Se dispone de una clasificación de la información según la criticidad de la misma?	NO
¿Existe un responsable de los activos?	NO
¿Existen procedimientos para clasificar la información?	NO
¿Existen procedimientos de etiquetado de la información?	NO
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS:	
¿Se tienen definidas responsabilidades y roles de seguridad?	NO
¿Se tiene en cuenta la seguridad en la selección y baja del personal?	NO

¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	NO
¿Se imparte la formación adecuada de seguridad y tratamiento de activos?	NO
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?	NO
¿Se recogen los datos de los incidentes de forma detallada?	NO
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?	NO
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?	NO
¿Existe un proceso disciplinario de la seguridad de la información?	NO
SEGURIDAD FÍSICA Y AMBIENTAL:	
¿Existe perímetro de seguridad física (una pared, puerta con llave)?	NO
¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?	NO
¿Un área segura ha de estar cerrada, aislada y protegida de eventos naturales?	NO
¿En las áreas seguras existen controles adicionales al personal propio y ajeno?	NO
¿Las áreas de carga y expedición están aisladas de las áreas de SI?	NO
¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?	NO
¿Existen protecciones frente a fallos en la alimentación eléctrica?	NO
¿Existe seguridad en el cableado frente a daños e intercepciones?	NO
¿Se asegura la disponibilidad e integridad de todos los equipos?	NO
¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?	NO
¿Se incluye la seguridad en equipos móviles?	NO
SEGURIDAD EN LAS TELECOMUNICACIONES:	
¿Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados?	NO
¿Están establecidas responsabilidades para controlar los cambios en equipos?	NO
¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?	NO
¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?	NO
¿Existe una separación de los entornos de desarrollo y producción?	NO
¿Existen contratistas externos para la gestión de los Sistemas de Información?	NO

¿Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?	NO
¿Existen criterios de aceptación de nuevos Sistema de Información, incluyendo actualizaciones y nuevas versiones?	NO
¿Controles contra software maligno?	NO
¿Realizar copias de backup de la información esencial para el negocio?	NO
¿Existen logs para las actividades realizadas por los operadores y administradores?	NO
¿Existen logs de los fallos detectados?	NO
¿Existen rastro de auditoría?	NO
¿Existe algún control en las redes?	NO
¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	NO
¿Eliminación de los medios informáticos?	NO
¿Existe seguridad de la documentación de los Sistemas?	NO
¿Existen acuerdos para intercambio de información y software?	NO
¿Existen medidas de seguridad de los medios en el tránsito?	NO
¿Existen medidas de seguridad en el comercio electrónico?	NO
¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	NO
¿Existen medidas de seguridad en las transacciones en línea?	NO
¿Se monitorean las actividades relacionadas a la seguridad?	NO
CONTROL DE ACCESOS:	
¿Existe una política de control de accesos?	NO
¿Existe un procedimiento formal de registro y baja de accesos?	NO
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?	NO
¿Existe una gestión de los password de usuarios?	NO
¿Existe una revisión de los derechos de acceso de los usuarios?	NO
¿Existe el uso del password?	NO
¿Se protege el acceso de los equipos desatendidos?	NO
¿Existen políticas de limpieza en el puesto de trabajo?	NO
¿Existe una política de uso de los servicios de red?	NO
¿Se asegura la ruta (path) desde el terminal al servicio?	NO
¿Existe una autenticación de usuarios en conexiones externas?	NO
¿Existe una autenticación de los nodos?	NO
¿Existe un control de la conexión de redes?	NO
¿Existe un control del routing de las redes?	NO
¿Existe una identificación única de usuario y una automática de terminales?	NO
¿Existen procedimientos de log-on al terminal?	NO

¿Se ha incorporado medidas de seguridad a la computación móvil?	NO
¿Está controlado el teletrabajo por la organización?	NO
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:	
¿Se asegura que la seguridad está implantada en los Sistemas de Información?	NO
¿Existe seguridad en las aplicaciones?	NO
¿Existen controles criptográficos?	NO
¿Existe seguridad en los ficheros de los sistemas?	NO
¿Existe seguridad en los procesos de desarrollo, testing y soporte?	NO
¿Existen controles de seguridad para los resultados de los sistemas?	NO
¿Existe la gestión de los cambios en los Sistemas Operativos?	NO
¿Se controlan las vulnerabilidades de los equipos?	NO
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:	
¿Se comunican los eventos de seguridad?	NO
¿Se comunican las debilidades de seguridad?	NO
¿Existe definidas las responsabilidades antes un incidente?	NO
¿Existe un procedimiento formal de respuesta?	NO
¿Existe la gestión de incidentes?	NO
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:	
¿Existen procesos para la gestión de la continuidad?	NO
¿Existe un plan de continuidad del negocio y análisis de impacto?	NO
¿Existe un diseño, redacción e implantación de planes de continuidad?	NO
¿Existe un marco de planificación para la continuidad del negocio?	NO
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	NO
CUMPLIMIENTO:	
¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?	NO
¿Existe el resguardo de la propiedad intelectual?	NO
¿Existe el resguardo de los registros de la organización?	NO
¿Existe una revisión de la política de seguridad y de la conformidad técnica?	NO
¿Existen consideraciones sobre las auditorías de los sistemas?	NO

La evaluación muestra que las bibliotecas de la EPN no cuentan con la implementación de los controles de seguridad. Por tal motivo, se procede a implementar el SGSI utilizando además la metodología de análisis de riesgo propuesta para bibliotecas.

Paso 3: Análisis de riesgos con la implementación de la metodología creada

El segundo paso de la metodología Action Research "Acción", es la ejecución del plan de acción elaborado (Implementación de un SGSI) luego de conocer la situación inicial de las bibliotecas de la EPN. En base a lo expuesto y considerando la Tabla 2, en donde se muestra el análisis de las fortalezas de las tres metodologías estudiadas, se ha desarrollado una metodología híbrida de análisis de riesgos para las bibliotecas universitarias, con la cual se pretende que este negocio gestione sus riesgos adecuadamente.

Para comprobar la metodología de análisis de riesgo optimizada para bibliotecas universitarias, se utiliza la metodología PHVA en concordancia con la norma ISO/IEC 27001:2013.

1. Planear: Establecer el SGSI

Política de seguridad

El documento de Políticas de Seguridad es un conjunto de reglas que se aplican a recursos pertenecientes a la organización; se especifica las áreas que se desea proteger tales como la seguridad física, personal, administrativa y de redes. Además, esta política debe describir cómo se va a supervisar la efectividad de las medidas de seguridad.

Para desarrollar una política de seguridad, se debe definir claramente sus objetivos de seguridad, los mismos que cubren las categorías protección de recursos, autenticación, autorización, integridad y confidencialidad.

Por otro lado, la redacción del documento debe ser con lenguaje sencillo y de alto nivel para que pueda ser captado por toda la comunidad a la que está enfocado; y finalmente, debe ser presentado ante la alta dirección para que lo apruebe y pueda impulsar el proyecto a toda la organización.

A continuación, se describe la política de seguridad de la información de las bibliotecas de la EPN la cual hace parte del SGSI y se encuentra en el Anexo F ubicado en la sección Anexos de este documento.

Gestión de riesgos

En este apartado se describe la metodología a utilizar para la gestión de riesgos con el fin tomar decisiones correctas según los riesgos derivados de las tecnologías de la información, así como el inventario de activos de la organización y la valoración de estos, teniendo en cuenta la confidencialidad, integridad, disponibilidad y autenticidad de la

información, realizando de esta forma el análisis de amenazas y la valoración de los riesgos estimando así los riesgos a los que se puede encontrar expuesta la organización.
En este caso, se utiliza la metodología de análisis de riesgos optimizada para los procesos de la biblioteca misma que se explicó anteriormente.

1. Recopilación de Activos:

Un análisis de riesgos genera el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación de información. Primeramente, se realiza la recopilación de activos de la organización para ello se utiliza la plantilla que se encuentra en el Anexo A ubicada en la sección Anexos de este documento:

Tabla 5 - Recopilación de activos de la biblioteca (información)

Información	
Descripción: Es aquella que se maneja en la biblioteca con la cual brinda servicio a los usuarios de la misma. Se cuenta con la información de todo el material bibliográfico existente en las bibliotecas y la información de carácter personal y fotografías de los usuarios quienes la visitan.	
Responsable: María José Bravo	**Tipo:** Pública Confidencial
Ubicación: Base de datos	
Cantidad: Se cuenta con más de 79000 registros de material bibliográfico distribuidos en libros, revistas y tesis de grado. Además, aproximadamente 23000 registros de información personal de los usuarios de las bibliotecas.	

Tabla 6 - Recopilación de activos de la biblioteca (aplicaciones informáticas)

Aplicaciones informáticas	
Descripción: Es el software que le permite a la biblioteca gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios de circulación y préstamo, gestión de usuarios, catalogación y elaboración de informes. Se utiliza el Sistema Integrado de Bibliotecas Koha versión 17.11.09, Sistema de Gestión de Bases de Datos MySQL Server versión 5.5.60 y Repositorio Digital DSPACE v.5.	
Responsable: María José Bravo	**Tipo:** Koha DSPACE SGBD MySQL
Ubicación: Servidor virtual	
Cantidad: 1 servidor con todas las aplicaciones mencionadas	

Tabla 7 - Recopilación de activos de la biblioteca (equipos informáticos)

Equipos informáticos	
Descripción: Son medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la biblioteca, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.	
Responsable: Personal de bibliotecas	**Tipo:** Impresoras Escáneres Switch Router Teléfonos IP Computadoras Personales y portátiles Servidor virtual en producción
Ubicación: Oficinas, sala de lectura y sala de Internet.	
Número: 3 impresoras 1 escáner 2 routers 2 switchs 3 teléfonos IP 20 computadoras personales 2 laptop 1 servidor virtual en producción	

Tabla 8 - Recopilación de activos de la biblioteca (soportes informáticos)

Soportes informáticos	
Descripción: Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. Se tiene CD-ROM los cuales contienen los requisitos de grado que los estudiantes entregan en la biblioteca previo a su graduación.	
Responsable: María José Bravo	**Tipo:** CD-ROM
Ubicación: Archivo de la Biblioteca General	
Cantidad: 10000 CD-ROM aproximadamente	

Luego de recopilar los activos de la biblioteca, se presenta el inventario en la siguiente tabla:

Tabla 9 - Inventario de Activos

Tabla de inventario de activos	
Ámbito	**Activo**
Información	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas
Aplicaciones informáticas	Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
Equipos informáticos	Impresoras Escáner Router Teléfonos IP Computadoras personales Laptops Servidor virtual en producción
Soportes informáticos	CD-ROM

Siguiendo la metodología se utiliza la Tabla de Valoración de Activos, ubicada en el Anexo B de la sección de Anexos de este documento, con el fin de utilizarla sobre la tabla general de activos de información que depende de cuatro dimensiones de gran importancia para la seguridad de la información, las cuales son: Integridad [I], Confidencialidad [C], Disponibilidad [D] y Autenticidad [A] y se las valora de manera cuantitativa como se detalla a continuación:

Tabla 10 - Escala de valoración de activos

Valoración	Detalle
0	Irrelevante
1	Daño bajo
2	Daño moderado
3	Daño grave
4	Daño extremadamente grave

Tabla 11 - Valoración de activos (datos personales)

Datos personales de los usuarios		
Dimensión	**Valor**	**Justificación**
[I]	4	Los datos personales del usuario no pueden ser modificados por terceras, por tanto si llegaran a ser alterados se produciría un daño extremadamente grave.
[C]	4	Los datos personales del usuario no deben ser conocidos por personas no autorizadas, por tanto si llegaran a ser estar en manos de terceras personas se produciría un daño extremadamente grave.
[D]	0	En este caso, la disponibilidad es irrelevante puesto que se requiere que los datos estén disponibles para realizar los préstamos de material bibliográfico al usuario.
[A]	0	Es irrelevante puesto que se necesita acceder al sistema para realizar reservas y renovaciones del préstamo de material bibliográfico.

La valoración de los activos restantes se encuentra en el Anexo K.

2. Identificación de Amenazas

Las amenazas suelen ser causas potenciales de incidentes que ocasionan daños al sistema de información o a la organización. Tras el análisis de los activos se detectan las siguientes amenazas que se describen utilizando el Anexo C de la sección de Anexos de este documento.

Tabla 12 - Identificación de amenazas (Desastres naturales)

Desastres naturales	**Origen:** Accidental
Descripción: Sucesos que pueden presentarse sin intervención humana directa o indirecta tales como daño por agua, fuego, terremotos, tormenta eléctrica.	
Tipo de activo afectado: Equipos informáticos y Soportes informáticos	**Dimensión**: Disponibilidad

Tabla 13 - Identificación de amenazas (De origen industrial)

De origen industrial	**Origen:** Accidental
Descripción: Sucesos que pueden ocurrir de forma accidental causados por la actividad humana de tipo industrial tales como explosiones, sobrecarga eléctrica, suciedad, condiciones inadecuadas de temperatura o humedad y como consecuencia del paso del tiempo	
Tipo de activo afectado: Equipos informáticos y Soportes informáticos	**Dimensión**: Disponibilidad

Tabla 14 - Identificación de amenazas (Errores y fallos no intencionados)

Errores y fallos no intencionados	**Origen:** Actividad humana no intencional
Descripción: Fallos no intencionales causados por las personas tales como errores de uso, registros incompletos, propagación de virus, alteración accidental de información, pérdida accidental de información y saturación del sistema informático.	
Tipo de activo afectado: Información, soportes informáticos y aplicaciones informáticas	**Dimensión**: Integridad, Confidencialidad, Disponibilidad

Tabla 15 - Identificación de amenazas (Ataques intencionados)

Ataques intencionados	**Origen:** Actividad humana intencional
Descripción: Fallos causados por personas tales como suplantación de la identidad de usuario, abuso de privilegios de acceso, propagación intencionada de virus, alteración de datos, acceso no autorizado, análisis de tráfico e interceptación de información.	
Tipo de activo afectado: Aplicaciones informáticas y equipos informáticos	**Dimensión**: Disponibilidad, Confidencialidad e Integridad

Luego de identificar las amenazas que se pueden presentar en la biblioteca, se presenta un cuadro resumido de las mismas en la siguiente tabla:

Tabla 16 - Catálogo de Amenazas

Ámbito	Amenaza
Desastres naturales	Daño por agua Fuego Terremotos Tormenta eléctrica
De origen industrial	Explosiones Sobrecarga eléctrica Suciedad Condiciones inadecuadas de temperatura o humedad Como consecuencia del paso del tiempo
Errores y fallos no encontrados	Errores de uso Registros incompletos Propagación de virus Alteración accidental de información Pérdida accidental de información Saturación del sistema informático
Ataques intencionales	Suplantación de la identidad de usuario Abuso de privilegios de acceso Propagación intencionada de virus Alteración de datos Acceso no autorizado Análisis de tráfico Interceptación de información

Siguiendo la metodología, se utiliza la Tabla de Valoración de Amenazas, ubicada en el Anexo D de la sección de Anexos de este documento, con el fin de aplicarla sobre la tabla general de amenazas especificada en la Tabla 26. Las escalas de valoración y la probabilidad de ocurrencia se han definido en las siguientes tablas:

Tabla 17 - Escalas de valoración de impactos

Valoración	Detalle
0	Muy bajo
1	Bajo
2	Medio
3	Alto
4	Muy alto

Tabla 18 - Escalas de valoración de probabilidad de ocurrencia

Probabilidad de ocurrencia	Detalle
0	Muy poco frecuente
1	Poco frecuente
2	Frecuente
3	Muy frecuente

El riesgo potencial es una medida del daño probable sobre un sistema. Conociendo el impacto de la amenaza sobre el activo (Valoración), es directo derivar el riesgo potencial sin más que tener en cuenta la probabilidad de ocurrencia, para determinar dicho riesgo se considerará las zonas de impacto vs probabilidad.

Tabla 19 - Valoración de la amenaza (Daño por agua)

Daño por agua					
Tipo de activo	**Activo**	**Valor**	**Probabilidad de ocurrencia**	**Riesgo potencial**	**Justificación**
Equipos informáticos	Impresoras	1	0	Zona 3	Porque el riesgo es muy bajo pero la probabilidad de ocurrencia es muy poco frecuente
	Escáner	1	0	Zona 3	Porque el riesgo es muy bajo pero la probabilidad de ocurrencia es muy poco frecuente
	Router	4	0	Zona 4	Porque el riesgo es muy alto pero la probabilidad de ocurrencia es poco frecuente
	Teléfonos IP	2	0	Zona 2	Porque el riesgo es alto pero la probabilidad de ocurrencia es muy frecuente
	Computadoras personales	4	0	Zona 4	Porque el riesgo es muy alto pero la probabilidad de ocurrencia es poco frecuente
	Laptops	4	0	Zona 4	Porque el riesgo es muy alto pero la probabilidad de ocurrencia es poco frecuente
	Servidor virtual en producción	4	0	Zona 4	Porque el riesgo es muy alto pero la probabilidad de ocurrencia es poco frecuente
Soportes informáticos	CD-ROM	2	0	Zona 2	Porque el riesgo es alto pero la probabilidad de ocurrencia es muy frecuente

La identificación de amenazas para el resto de categorías se encuentra en el Anexo L

3. Identificación de vulnerabilidades

Se procedió a identificar las vulnerabilidades tecnológicas existentes en la biblioteca con la ayuda de la herramienta Microsoft Security Assesment Tool, en la cual se hizo un análisis de infraestructura, aplicaciones, operaciones y personal. De la evaluación, se obtuvieron los resultados detallados en el Anexo G, ubicado en la sección Anexos de este documento en el cual se describe los puntos débilmente protegidos por los que las amenazas podrían materializarse. De dichos resultados se obtendrá la información que se complementen con el presente análisis de riesgo puesto que el informe que emite la herramienta es muy amplio.

4. Selección de Salvaguardas

Tras la identificación de amenazas y vulnerabilidades, es necesario contar con salvaguardas que ayuden a reducir los riesgos identificados en el sistema de bibliotecas, los cuales actualmente no están implantadas, pero al hacerlo se espera una reducción considerable del impacto en caso de materializarse las amenazas. Por tanto, se seleccionaron las salvaguardas necesarias en consonancia de los controles de la ISO 27002:2013 utilizando el Anexo E de la sección de Anexos de este documento.

Tabla 20 - Selección de salvaguardas

Salvaguarda	Amenaza a la que hace frente	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
Copias de seguridad de los datos, protección de equipos informáticos, protección de los soportes informáticos	Daño por agua	X	X			X		X	X				X	X	X
Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Fuego	X	X						X				X	X	X
Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Terremotos	X	X						X				X	X	X
Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Tormenta eléctrica	X	X						X				X	X	X
Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Explosiones	X	X						X				X	X	X
Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Sobrecarga eléctrica	X	X						X				X	X	X
Copias de seguridad de los datos, protección de los equipos informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido	Suciedad	X	X			X			X				X	X	X
Copias de seguridad de los datos, protección de los equipos	Condiciones inadecuadas de	X	X			X		X	X				X	X	X

informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido, climatización	temperatura o humedad														
Copias de seguridad de los datos, reproducción de documentos, limpieza de contenido, aseguramiento de la disponibilidad	Como consecuencia del paso del tiempo	X	X					X	X					X	
Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, uso de herramientas de chequeo de configuración	Errores de uso	X	X			X	X	X					X	X	X
Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad	Registros incompletos	X	X			X	X	X	X					X	X
Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Propagación de virus	X	X			X	X	X	X					X	X
Copias de seguridad de los datos, protección de la información, aseguramiento de la integridad, cifrado de la información, protección criptográfica del contenido de los soportes de información	Alteración accidental de información	X	X			X	X	X	X					X	X

Copias de seguridad de los datos, protección de la información, aseguramiento de la integridad, cifrado de la información, protección criptográfica del contenido de los soportes de información, aseguramiento de la disponibilidad	Pérdida accidental de información	X	X			X	X	X	X					X	X
Copias de seguridad, uso de herramientas de chequeo de configuración, uso de herramientas para análisis de logs, protección de la información, gestión de cambios	Saturación del sistema informático	X	X						X	X				X	X
Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, formación y concienciación al usuario	Suplantación de la identidad de usuario	X	X				X		X	X				X	X
Aplicación de perfiles de seguridad, formación y concienciación, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas	Abuso de privilegios de acceso	X	X				X		X	X				X	X
Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Propagación intencionada de virus	X	X				X		X	X				X	X
Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos	Alteración de datos	X	X						X	X				X	X

informáticos, protección de las aplicaciones informáticas, protección de los soportes de información															
Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas, protección de los soportes de información	Acceso no autorizado	X	X						X	X				X	X
Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad	Análisis de tráfico	X	X				X		X	X				X	X
Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad, autenticación del canal de comunicaciones	Interceptación de información	X	X				X		X	X				X	X

5. Desarrollo de planes de seguridad

Luego de determinar los riesgos potenciales para cada una de las amenazas identificadas, se desarrolla el plan de seguridad para la biblioteca, el cual se encuentra en el Anexo H de la sección Anexos de este documento.

6. Comunicación de resultados

Para comunicar los riesgos a las partes interesadas, se lo realiza mediante una matriz de resultados, utilizando la plantilla del Anexo I de la sección Anexos de este documento.

Tabla 21 – Matriz de resultados

Zona de riesgo	Amenazas	Vulnerabilidades	Salvaguardas	Activo
Zona 1	Condiciones inadecuadas de temperatura o humedad	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, protección de los equipos informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido, climatización	Router Computadoras personales Laptops Servidor virtual en producción CD-ROM
		No existe planes de recuperación de desastres ni de continuidad del negocio		
	Errores de uso	No se han realizado pruebas de la aplicación para evaluar la aplicación informática y las interfaces disponibles para los usuarios por internet	Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, uso de herramientas de chequeo de configuración	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas
	Propagación de virus	No está instalado un software antivirus actualizado en los equipos de la biblioteca	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Sistema de Gestión de Bases de Datos (MySQL)
	Acceso no autorizado	No existe implantado ningún sistema de detección de intrusiones para proteger la infraestructura de la biblioteca de los ataques desde Internet	Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas, protección de los soportes de información	Router Computadoras personales Laptops Servidor virtual en producción Koha
		No se gestiona las contraseñas de manera adecuada		

		Los equipos de trabajo y servidores no se mantienen actualizados a medida que se publican nuevas actualizaciones No se utiliza un protector de pantalla protegido por contraseña en el entorno		Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Suciedad	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, protección de los equipos informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido	Router Computadoras personales Laptops Servidor virtual en producción
	Saturación del sistema informático	No se utilizan equilibradores de carga en el entorno	Copias de seguridad, uso de herramientas de chequeo de configuración y análisis de logs, protección de la información.	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Suplantación de identidad del usuario	No existe ninguna directiva formal para los empleados que dejan de laborar en la empresa	Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas,	Router Teléfonos IP

		No se llevan a cabo comprobaciones del historial personal como parte integral del proceso de contratación	aplicación de perfiles de seguridad, formación y concienciación al usuario	Computadoras personales Laptops Servidor virtual en producción Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Abuso de privilegios de acceso	No existe cortafuegos ni otros controles de acceso de nivel de red en el perímetro de la biblioteca El personal de bibliotecas tiene habilitados accesos administrativos a sus estaciones de trabajo. No existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas	Aplicación de perfiles de seguridad, formación y concienciación, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas	Router Teléfonos IP Computadoras personales Laptops Servidor virtual en producción Koha Sistema de Gestión de Bases de Datos (MySQL)

				Repositorio digital (Dspace)
	Propagación intencionada de virus	No está instalado un software antivirus actualizado en los equipos de la biblioteca	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Router Teléfonos IP Computadoras personales Laptops Servidor virtual en producción Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Interceptación de información	No se utiliza herramientas de pruebas de software de seguridad para la aplicación que se está usando	Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad, autenticación del canal de comunicaciones	Router Teléfonos IP
Zona 2	Suciedad	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, protección de los equipos informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido	Impresoras Escáner Teléfonos IP CD-ROM

	Condiciones inadecuadas de temperatura o humedad	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, protección de los equipos informáticos, protección de los soportes informáticos, reproducción de documentos, limpieza de contenido, climatización	Impresoras Escáner Teléfonos IP
	Daño por agua	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, protección de equipos informáticos, protección de los soportes informáticos	Teléfonos IP CD-ROM
	Fuego	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Teléfonos IP CD-ROM
	Tormenta eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Teléfonos IP CD-ROM
	Terremotos	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Teléfonos IP CD-ROM
	Explosiones	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Teléfonos IP CD-ROM
	Sobrecarga eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Teléfonos IP CD-ROM
	Como consecuencia del paso del tiempo	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, reproducción de documentos, limpieza de contenido, aseguramiento de la disponibilidad	Router Teléfonos IP Computadoras personales Laptops

				Servidor virtual en producción CD-ROM
	Errores de uso	No se han realizado pruebas de la aplicación para evaluar la aplicación informática y las interfaces disponibles para los usuarios por internet	Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, uso de herramientas de chequeo de configuración	Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Registros incompletos	Existe personal que no está capacitado adecuadamente para el manejo de la aplicación informática de bibliotecas	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas
	Propagación de virus	No está instalado un software antivirus actualizado en los equipos de la biblioteca	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas CD-ROM Koha Repositorio digital (Dspace)

	Alteración accidental de la información	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo Existe personal que no está capacitado adecuadamente para el manejo de la aplicación informática de bibliotecas	Copias de seguridad de los datos, protección de la información, aseguramiento de la integridad, cifrado de la información, protección criptográfica del contenido de los soportes de información	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas CD-ROM Koha Repositorio digital (Dspace)
	Propagación intencionada de virus	No está instalado un software antivirus actualizado en los equipos de la biblioteca	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, protección de la información	Impresoras Escáner
	Alteración de datos	No se utiliza ningún software de cifrado de discos en el entorno	Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas, protección de los soportes de información	Router Computadoras personales Laptops Servidor virtual en producción

	Acceso no autorizado	No existe implantado ningún sistema de detección de intrusiones para proteger la infraestructura de la biblioteca de los ataques desde Internet	Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas, protección de los soportes de información	Impresoras Escáner Teléfonos IP
		No se gestiona las contraseñas de manera adecuada		
		Los equipos de trabajo y servidores no se mantienen actualizados a medida que se publican nuevas actualizaciones		
		No se utiliza un protector de pantalla protegido por contraseña en el entorno		
	Análisis de tráfico	No existe cortafuegos ni otros controles de acceso de nivel de red en el perímetro de la biblioteca	Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad	Impresoras Escáner
	Interceptación de información	No se utiliza herramientas de pruebas de software de seguridad para la aplicación que se está usando	Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad, autenticación del canal de comunicaciones	Impresoras Escáner Computadoras personales Laptops Servidor virtual en producción Koha Sistema de Gestión de

				Bases de Datos (MySQL) Repositorio digital (Dspace)
Zona 3	Fuego	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Impresoras Escáner
	Terremotos	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Impresoras Escáner
	Tormenta eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Impresoras Escáner
	Explosiones	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Impresoras Escáner
	Sobrecarga eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Impresoras Escáner
	Daño por agua	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, protección de equipos informáticos, protección de los soportes informáticos	Impresoras Escáner
	Como consecuencia del paso del tiempo	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, reproducción de documentos, limpieza de contenido, aseguramiento de la disponibilidad	Impresoras Escáner

	Registros incompletos	Existe personal que no está capacitado adecuadamente para el manejo de la aplicación informática de bibliotecas	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad	CD-ROM
	Suplantación de identidad del usuario	No existe ninguna directiva formal para los empleados que dejan de laborar en la empresa No se llevan a cabo comprobaciones del historial personal como parte integral del proceso de contratación	Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, formación y concienciación al usuario	Impresoras Escáner
	Abusos de privilegios de acceso	No existe cortafuegos ni otros controles de acceso de nivel de red en el perímetro de la biblioteca El personal de bibliotecas tiene habilitados accesos administrativos a sus estaciones de trabajo. No existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas	Aplicación de perfiles de seguridad, formación y concienciación, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas	Impresoras Escáner
	Alteración de datos	No se utiliza ningún software de cifrado de discos en el entorno	Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones informáticas, protección de los soportes de información	Impresoras Escáner Teléfonos IP
Zona 4	Daño por agua	No existen controles formales para hacer cumplir las directivas de contraseñas en todas las cuentas	Copias de seguridad de los datos, protección de equipos informáticos, protección de los soportes informáticos	Router Computadoras personales Laptops

				Servidor virtual en producción
	Fuego	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Router Computadoras personales Laptops Servidor virtual en producción
	Terremotos	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Router Computadoras personales Laptops Servidor virtual en producción
	Tormenta eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Router Computadoras personales Laptops Servidor virtual en producción
	Explosiones	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos, plan de recuperación de desastres	Router Computadoras personales Laptops Servidor virtual en producción
	Sobrecarga eléctrica	No existe planes de recuperación de desastres ni de continuidad del negocio	Copias de seguridad de los datos, aseguramiento de la disponibilidad, reproducción de documentos	Router Computadoras personales Laptops Servidor virtual en producción

	Análisis de tráfico	No existe cortafuegos ni otros controles de acceso de nivel de red en el perímetro de la biblioteca	Protección de la integridad de los datos intercambiados, protección criptográfica de la confidencialidad de los datos intercambiados, protección de las comunicaciones, aplicación de perfiles de seguridad	Router Teléfonos IP Computadoras personales Laptops Servidor virtual en producción Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Registros incompletos	Existe personal que no está capacitado adecuadamente para el manejo de la aplicación informática de bibliotecas	Identificación y autenticación, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad	Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Alteración accidental de la información	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, protección de la información, aseguramiento de la integridad, cifrado de la información, protección criptográfica del contenido de los soportes de información	Sistema de Gestión de Bases de Datos (MySQL)

		Existe personal que no está capacitado adecuadamente para el manejo de la aplicación informática de bibliotecas		
	Pérdida accidental de información	No se realizan pruebas regulares del proceso de restauración de las copias de seguridad para garantizar la recuperación de datos desde los dispositivos de respaldo	Copias de seguridad de los datos, protección de la información, aseguramiento de la integridad, cifrado de la información, protección criptográfica del contenido de los soportes de información, aseguramiento de la disponibilidad	Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas CD-ROM Koha Sistema de Gestión de Bases de Datos (MySQL) Repositorio digital (Dspace)
	Errores de uso	No se han realizado pruebas de la aplicación para evaluar la aplicación informática y las interfaces disponibles para los usuarios por internet	Identificación y autenticación, aseguramiento de la integridad, gestión de claves criptográficas, aplicación de perfiles de seguridad, copias de seguridad, uso de herramientas de chequeo de configuración	CD-ROM
	Alteración de datos	No se utiliza ningún software de cifrado de discos en el entorno	Identificación y autenticación, aplicación de perfiles de seguridad, aseguramiento de la integridad, protección de los equipos informáticos, protección de las aplicaciones	Koha Sistema de Gestión de Bases de Datos

			informáticas, protección de los soportes de información	(MySQL) Repositorio digital (Dspace) Datos personales de los usuarios Información del material bibliográfico existente en las bibliotecas

En la matriz de la Tabla 21, se refleja los resultados obtenidos tras realizar un análisis de riesgos con la metodología optimizada para bibliotecas, cada tipo de activo cuenta con su respectiva amenaza, además de la vulnerabilidad que podría ser la causa para que la amenaza pueda materializarse y, por último, la zona de riesgo en la que se encuentra cada una, siendo estas:

- Zona 1: Son las amenazas más propensas a materializarse, puesto que si estas se llegaran a materializar producirían un impacto muy alto en el sistema de bibliotecas de la EPN.
- Zona 2: Cubren un alto rango de situaciones improbables o de impacto medio hasta situaciones muy probables, pero de bajo impacto.
- Zona 3: Son riesgos improbables y de bajo impacto.
- Zona 4: Riesgos improbables, pero de muy alto impacto.

Además, se añadió la salvaguarda propuesta para contrarrestar dicha amenaza y de esta manera, reducir el impacto en caso de materializarse.

2. **Ejecutar:** Implementar y utilizar el SGSI

Plan de tratamiento de riesgos

Establecidos los niveles de riesgos para cada amenaza, se analiza el tratamiento de los mismos en función de los controles de la ISO/IEC 27001:2013. Esto permite establecer un plan detallado de acciones a tomar para el tratamiento de riesgos.

Tabla 22 - Tratamiento del riesgo asociado a los controles de la ISO 27001:2013

Riesgo	Tratamiento	Responsable	Resultados esperados	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
Condiciones inadecuadas de temperatura o humedad (Zona 1 y Zona 2)	Aceptarlo	Departamento de Servicios Generales	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia				X			X							
Errores de uso (Zona 1, Zona 2 y Zona 4)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X		X							X				
Propagación de virus (Zona 1 y Zona 2)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X	X	X		X			X						
Alteración de datos (Zona 1, Zona 2, Zona 3 y Zona 4)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X	X	X			X		X	X	X				
Acceso no autorizado (Zona 1 y Zona 2)	Evitarlo	Asistente de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X		X		X	X	X	X	X					X
Saturación del sistema	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la	X						X					X	X	

informático (Zona 1)			probabilidad de ocurrencia														
Suplantación de identidad del usuario (Zona 1, Zona 3)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia			X		X	X						X		
Abusos de privilegio de acceso (Zona 1 y Zona 3)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X	X	X		X			X				X		
Propagación intencionada de virus (Zona 1 y Zona 2)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X	X	X		X			X				X		
Intercepción de información (Zona 1 y Zona 2)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X				X	X		X	X					X
Suciedad (Zona 1 y Zona 2)	Mitigarlo	Departamento de Servicios Generales	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia				X			X						X	
Como consecuencia del	Mitigarlo	Asistente de TICS	Reducirlo disminuyendo el impacto y la	X		X	X		X		X					X	

paso del tiempo (Zona 2 y Zona 3)			probabilidad de ocurrencia														
Daño por agua (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Servicios Generales	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia							X	X						
Fuego (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Seguridad Industrial y Salud ocupacional	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X						X					X	X	
Terremotos (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Seguridad Industrial y Salud ocupacional	Reducirlo disminuyendo el impacto	X						X					X	X	
Tormenta eléctrica (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Seguridad Industrial y Salud ocupacional	Reducirlo disminuyendo el impacto	X						X					X	X	
Explosiones (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Seguridad Industrial y Salud ocupacional	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X						X					X	X	
Sobrecarga eléctrica (Zona 2, Zona 3 y Zona 4)	Mitigarlo	Departamento de Seguridad Industrial y Salud ocupacional	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X						X					X	X	
Registros incompletos (Zona	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la			X		X									

2, Zona 3 y Zona 4)			probabilidad de ocurrencia														
Alteración accidental de la información (Zona 2 y Zona 4)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X				X	X		X		X			X	X
Análisis de tráfico (Zona 2 y Zona 4)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X	X				X			X			X		
Pérdida accidental de información (Zona 4)	Evitarlo	Asistentes de TICS	Reducirlo disminuyendo el impacto y la probabilidad de ocurrencia	X				X		X	X	X				X	

3. **Revisar:** Monitorear y revisar el SGSI

La unión del plan de tratamiento de riesgos junto con un plan de monitoreo permite conocer cuan acertadas son las estrategias implementadas, para así, ejecutar acciones oportunas que permitan anticiparse a los problemas, garantizar la sostenibilidad de los proyectos y retroalimentar los procesos de toma de decisiones. En la siguiente tabla se establecen las medidas para monitorear los riesgos, los responsables a cargo y la frecuencia de ejecución del plan:

Tabla 23 - Plan de monitoreo

Riesgo	Plan de monitoreo	Responsables	Frecuencia
Condiciones inadecuadas de temperatura o humedad (Zona 1 y Zona 2)	Evaluación de los factores ambientales	Departamento de Servicios Generales	Trimestral
Errores de uso (Zona 1, Zona 2 y Zona 4)	Informes de los errores	Asistentes de TICS	Semanal
Propagación de virus (Zona 1 y Zona 2)	Informes de escaneo de antivirus	Asistentes de TICS	Mensual
Alteración de datos (Zona 1, Zona 2, Zona 3 y Zona 4)	Evaluación periódica de la información registrada Revisión de log de ingresos de información al Sistema de Bibliotecas	Asistentes de TICS	Trimestral
Acceso no autorizado (Zona 1 y Zona 2)	Revisión de log de usuarios del Sistema de Bibliotecas	Asistente de TICS	Diario
Saturación del sistema informático (Zona 1)	Chequeo del equilibrio de carga y pruebas de caja negra	Asistentes de TICS	Trimestral
Suplantación de identidad del usuario (Zona 1, Zona 3)	Revisión de log de usuarios del Sistema de Bibliotecas	Asistentes de TICS	Mensual
Abusos de privilegio de acceso	Informes de auditoría internas de	Asistentes de TICS	Mensual

(Zona 1 y Zona 3)	las funciones de los empleados		
Propagación intencionada de virus (Zona 1 y Zona 2)	Informes de escaneo de antivirus	Asistentes de TICS	Mensual
Interceptación de información (Zona 1 y Zona 2)	Evaluación de la configuración de la red y encriptación de la información	Asistentes de TICS	Mensual
Suciedad (Zona 1 y Zona 2)	Informes de mantenimientos preventivos	Departamento de Servicios Generales	Trimestral
Como consecuencia del paso del tiempo (Zona 2 y Zona 3)	Evaluación al proceso de restauración de las copias de seguridades Evaluación y actualización de activos de almacenamiento	Asistente de TICS	Anual
Daño por agua (Zona 2, Zona 3 y Zona 4)	Evaluación de la aplicación del modelo de Análisis de Riesgos de Plagas implementado en la institución Evaluación al proceso de restauración de las copias de seguridades	Departamento de Servicios Generales	Semestral
Fuego (Zona 2, Zona 3 y Zona 4)	Evaluación de la aplicación del modelo de Seguridad Industrial y Salud Ocupacional propuesto por el Departamento Evaluación al proceso de restauración de las copias de seguridades	Departamento de Seguridad Industrial y Salud ocupacional	Semestral

Terremotos (Zona 2, Zona 3 y Zona 4)	Evaluación al proceso de restauración de las copias de seguridades	Departamento de Seguridad Industrial y Salud ocupacional	Semestral
Tormenta eléctrica (Zona 2, Zona 3 y Zona 4)	Evaluación al proceso de restauración de las copias de seguridades	Departamento de Seguridad Industrial y Salud ocupacional	Semestral
Explosiones (Zona 2, Zona 3 y Zona 4)	Evaluación al proceso de restauración de las copias de seguridades	Departamento de Seguridad Industrial y Salud ocupacional	Semestral
Sobrecarga eléctrica (Zona 2, Zona 3 y Zona 4)	Evaluación al proceso de restauración de las copias de seguridades	Departamento de Seguridad Industrial y Salud ocupacional	Semestral
Registros incompletos (Zona 2, Zona 3 y Zona 4)	Evaluación periódica de la información ingresada Seguimiento a capacitaciones sobre responsabilidad en el manejo de la información	Asistentes de TICS	Diario
Alteración accidental de la información (Zona 2 y Zona 4)	Evaluación periódica de la información ingresada Seguimiento a capacitaciones sobre responsabilidad en el manejo de la información	Asistentes de TICS	Diario
Análisis de tráfico (Zona 2 y Zona 4)	Uso de herramientas de análisis de tráfico	Asistentes de TICS	Diario
Pérdida accidental de información (Zona 4)	Evaluación periódica de la información ingresada	Asistentes de TICS	Diario

	Evaluación al proceso de restauración de las copias de seguridades		

Además, se ejecutan auditorías internas para analizar el grado de madurez en la implementación del SGSI respecto a los 14 controles de seguridad de la norma ISO 27002:2013. Para ello se utiliza (CMM) como metodología para dicho análisis puesto que este modelo se enfoca en la mejora continua de los procesos y trata la identificación de elementos actuales y deseables en la organización que permitan evaluar el cumplimiento de los controles definidos para la implementación del SGSI en las bibliotecas de la EPN.

Los niveles de madurez son progresivos y organizados de acuerdo a su importancia y prioridad. Por tanto, para el presente análisis se toman las valoraciones siguientes:

Tabla 24 - Valoraciones criterios de madurez CMM

Valoración	Nivel CMM	Descripción
0	Inexistente	No se ha contemplado por parte de la organización que existe un problema a solucionar.
1	Inicial	Se identifican problemas en la organización que requieren ser solucionados. Sin embargo, no se evidencian procesos estandarizados sino procedimientos empíricos aplicados para cada caso, dichos métodos son desorganizados y no existe documentación formal.
2	Repetible	Se realizan procedimientos rutinarios semejantes en las mismas tareas basadas en procedimientos empíricos y/o estandarizados bajo una documentación formal. No existe capacitación, mostrando un alto grado de confianza en los conocimientos de los empleados, con alta probabilidad de errores.
3	Definido	Se cuenta con procedimientos estandarizados y documentados, notificados por medio de capacitaciones. Sin embargo, el seguimiento de los procesos lo realizan los mismos empleados, lo que causa que no se identifiquen desviaciones. Los procedimientos han formalizado las prácticas existentes en la organización.
4	Gestionado	Se realiza el monitoreo de los procedimientos estandarizados, generando las acciones necesarias en el caso que se identifiquen desviaciones. Las

		herramientas y la automatización se usan de forma limitada.
5	Optimizado	Se han llevado los procesos a la mejor práctica, obteniendo resultados de mejoramiento continuo. Se cuenta con herramientas para la automatización del flujo del trabajo, mejorando así la calidad y rapidez en los procesos de la organización.

Los criterios de madurez fijados anteriormente, permiten medir la situación de las bibliotecas con respecto a los 114 controles pertenecientes a los 14 dominios de la ISO/IEC 27002:2013. Se presenta la evaluación de madurez del SGSI implementado en las bibliotecas de la EPN tras realizar una entrevista (Anexo J) al equipo de proyecto conformado por los Asistentes de TICS la cual se encuentra en el Anexo M.

3. RESULTADOS Y DISCUSIÓN

3.1. Resultados

El presente capítulo proporciona los resultados del proceso de evaluación de la implementación del SGSI como último paso de la metodología Action Research, descrita en el capítulo anterior.

En la siguiente tabla se presenta el análisis de resultados de madurez de cada uno de los controles proporcionados por la ISO/IEC 27002:2013 en las bibliotecas:

Tabla 25 - Resultados evaluación de madurez

Dominio	Controles aplicables	0	1	2	3	4	5
A.5 Políticas de seguridad de la información	2	1	1				
A.6 Organización de la seguridad de la información	7	3	3	1			
A.7 Seguridad de los recursos humanos	6	2	1	2	1		
A.8 Gestión de activos	10	6	2		1	1	
A.9 Control de acceso	14	3	6	3	1	1	
A.10 Criptografía	2	2					
A.11 Seguridad física y del entorno	15	3	9	2	1		
A.12 Seguridad de las operaciones	14		8	3	2	1	
A.13 Seguridad de las comunicaciones	7	2	5				
A.14 Adquisición, desarrollo y mantenimientos de sistemas	13	6	7				
A.15 Relación con los proveedores	5	5					
A.16 Gestión de incidentes de seguridad de la información	7		7				
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	4	1	3				
A.18 Cumplimiento	8	2	6				
Total:	114	36	58	11	6	3	

A partir de los datos obtenidos, se genera el siguiente gráfico que permite observar de forma general el estado actual de las bibliotecas de la EPN con respecto a la implementación del SGSI.

Figura 4 - Resultados de evaluación de madurez

3.2. Discusión

En los resultados de la evaluación de madurez del SGSI en las bibliotecas de la EPN, se destaca que:

- El SGSI implementado se encuentra en un nivel de madurez 1 que corresponde a "Inicial".
- La organización ha dado poca importancia a 36 de los controles de la norma, puesto que, se confía en una muy baja probabilidad de materialización de amenazas relacionados en el nivel de madurez 0 que corresponde a "Inexistente".

  Los controles pertenecientes a esta categoría son:
  - A.5.1.2 Revisión de las políticas para la seguridad de la información
  - A.6.1.4 Contacto con grupos de interés especial
  - A.6.2.1 Política para dispositivos móviles
  - A.6.2.2 Teletrabajo
  - A.7.1.2 Términos y condiciones del empleo
  - A.7.2.3 Proceso disciplinario

- A.8.1.3 Uso aceptable de los activos
- A.8.2.1 Clasificación de la información
- A.8.2.2 Etiquetado de la información
- A.8.2.3 Manejo de activos
- A.8.3.1 Gestión de medios removibles
- A.8.3.2 Disposición de los medios
- A.9.2.5 Revisión de los derechos de acceso de usuarios
- A.9.2.6 Retiro o ajuste de los derechos de acceso
- A.9.4.4 Uso de programas utilitarios privilegiados
- A.10.1.1 Política sobre el uso de controles criptográficos
- A.10.1.2 Gestión de llaves
- A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones
- A.11.2.7 Disposición segura o reutilización de equipos
- A.11.2.9 Política de escritorio limpio y pantalla limpia
- A.13.2.3 Mensajería electrónica
- A.13.2.4 Acuerdos de confidencialidad o de no divulgación
- A.14.1.1 Análisis y especificación de requisitos de seguridad de la información
- A.14.2.1 Política de desarrollo seguro
- A.14.2.2 Procedimientos de control de cambios en sistemas
- A.14.2.6 Ambiente de desarrollo seguro
- A.14.2.8 Pruebas de seguridad de sistemas
- A.14.2.9 Prueba de aceptación de sistemas
- A.15.1.1 Política de seguridad de la información para las relaciones con proveedores
- A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores
- A.15.1.3 Cadena de suministro de tecnología de información y comunicación
- A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
- A.15.2.2 Gestión de cambios en los servicios de proveedores
- A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.
- A.18.1.5 Reglamentación de controles criptográficos
- A.18.2.1 Revisión independiente de la seguridad de la información

- Aunque las bibliotecas de la EPN se encuentran en un nivel bajo de madurez, se observa un avance en varios de los dominios tales como la implementación de políticas de seguridad. Puesto que, la mayor parte del cumplimiento de los controles para la seguridad de la información eran inexistentes antes de implementar el SGSI.
- En un 51% de los controles, pertenecientes a la ISO/IEC 27002:2013, están en una etapa “Inicial”, el 10% de los controles se encuentran en una etapa “Repetible”, el 5% de los controles están en una etapa “Definido” y un 3% de los controles están en una etapa “Gestionado”. Las bibliotecas de la EPN tomarán las medidas correspondientes para mejorar estos indicadores.
- Ninguno de los controles aplica en el nivel de madurez más alto “Optimizado”, lo cual indica, que se carece de herramientas que permitan automatizar los controles para el SGSI.
- La implementación del SGSI ha permitido fortalecer la seguridad de la información con la documentación formal y procedimientos estandarizados. Esto favorecerá la visibilidad de las bibliotecas universitarias públicas en los entornos de investigación en el campo de la gestión de la seguridad.
- Se pone de manifiesto la necesidad de incorporar de forma gradual una gestión de la seguridad en las bibliotecas universitarias públicas que cumpla los objetivos y la misión de las mismas.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

A continuación se presentan las conclusiones obtenidas a lo largo del desarrollo del proyecto.

- La metodología de gestión de riesgos optimizada se adaptó eficientemente al modelo de negocio de las bibliotecas universitarias, además los seis pasos extraídos de Magerit v.3, Octave V.2 y NIST 800-30, son totalmente compatibles con la ISO/IEC 27001:2013.
- Con la implementación del SGSI se logró identificar activos no inventariados, amenazas inminentes y riesgos potenciales, esto permitió alcanzar eficiencia en la administración de los recursos de esta entidad.
- Las políticas de seguridad de la información de las bibliotecas de la EPN no se encontraron legalizadas, gracias al desarrollo de este proyecto se recalcó la necesidad e importancia de su legalización e implementación.
- Las mejoras planteadas le permiten al SGSI alcanzar niveles de madurez más altos y en el futuro tener la posibilidad de obtener la certificación del mismo, mediante la norma ISO/IEC 27001:2013.
- La implementación de un SGSI en el sistema de bibliotecas de la EPN proporcionó mecanismos de protección y optimización de los recursos que se fundamentan en un ciclo de mejora continua que le permitirá a la biblioteca alcanzar objetivos y metas proyectadas.
- La implementación de un SGSI es un proceso que conlleva tiempo, trabajo y costos económicos. Sin embargo, beneficia el crecimiento y alcance de los objetivos de la organización si se gestiona de forma adecuada bajo el ciclo de mejora continua.
- La presentación de este proyecto de desarrollo, al equipo de las bibliotecas de la EPN, generó un impacto positivo y cumplió con los objetivos planteados.

4.2. Recomendaciones

- Se sugiere establecer capacitaciones, monitoreo, automatización de los controles y auditorías internas que permitan incrementar los niveles de madurez del SGSI poniendo en práctica las mejoras descritas.

- Es importante actualizar e implementar políticas de seguridad de la información para el sistema de bibliotecas de la EPN con el fin de proteger la información de la organización.
- El tiempo es un factor escaso para la implementación total de este proyecto, por lo tanto solamente se realiza una vuelta del ciclo de mejora continua y se proponen las mejoras que pueden ser implementadas a futuro en las bibliotecas de la EPN.

Las recomendaciones realizadas para el ciclo de mejora continua se encuentran en el Anexo N.

5. REFERENCIAS BIBLIOGRÁFICAS

Aginsa, A., Matheus Edward, I. Y., & Shalannanda, W. (2016). Enhanced Information Security Management System Framework Design Using ISO 27001 And Zachman Framework A Study Case of XYZ Company . *IEEE*.

Alberts, C. J., Dorofee, A. J., & Allen, J. H. (October de 2001). *OCTAVE Catalog of Practices, Version 2.0 .* Obtenido de https://resources.sei.cmu.edu/asset_files/TechnicalReport/2001_005_001_13883.pdf

Bayona, S., Chauca, W., Lopez, M., & Maldonado, C. (2015). Implementación de la NTP ISO/IEC 27001 en las Instituciones Publicas:Caso de Estudio. *Web of Science*, 6.

Beltran, I. O. (06 de Agosto de 2018). Información General de los Procesos de la Biblioteca General EPN. (M. J. Bravo, Entrevistador)

Bravo, M. J., & Portilla, M. F. (22 de 05 de 2015). *Desarrollo de una interfaz biométrica para el módulo de préstamo del sistema de bibliotecas de la Escuela Politécnica Nacional.* Obtenido de http://bibdigital.epn.edu.ec/handle/15000/10528

Disterer, G. (2017). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 92 - 100.

ED economíaDigital. (2016). *Los diez mayores ataques informáticos de 2016.* Obtenido de https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

Esquema Nacional de Seguridad. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

González Trejo, D. (30 de 08 de 2013). *ISO-27001:2013* . Obtenido de http://www.magazcitum.com.mx/?p=2397#.W2No3VVKjIV

INTERNATIONAL STANDARD ISO/IEC 27001 (Primera ed.). (2013).

INTERNATIONAL STANDARD ISO/IEC 27002 (Primera ed.). (2013).

Livshitz, I. I., & Nikiforova, K. A. (2016). The Evaluation of the Electronic Services with Accordance to IT-security Requirements Based on ISO/IEC 27001 . *IEEE*, 128 - 131.

Narvaez Barreiros, I. R. (07 de 08 de 2018). *Aplicación de la norma ISO 27001 para la implementación de un SGSI en la Fiscalía General del Estado.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/9780/TESIS_SGSI.pdf?sequence=1&isAllowed=y

National Institute of Standards and Technology. (Septiembre de 2012). *NIST Special Publication 800-30.* Obtenido de https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Normas Biblioteca Central EPN. (2014). Normas Biblioteca Central EPN. *Normas Biblioteca Central EPN*, (pág. 20). Quito.

Portal de Administración Electrónica. (2012). *MAGERIT versión 3*. Obtenido de https://administracionelectronica.gob.es/ctt/magerit#.W2N97FVKjIU

Reason, P., & Bradbury, H. (2001). *Handbook of action research : participative inquiry and practice.* London: Thousand Oaks.

Rodal Castro, P. (30 de Diciembre de 2016). *Implementation Plan for an ISMS according to ISO/IEC 27001:2013.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/59325/8/prodalTFM1216mem%C3%B2ria.pdf

Susanto, A., Nurbojatmiko, & Shobariah, E. (2016). Assessment of ISMS Based On Standard ISO/IEC 27001:2013 at DISKOMINFO Depok City . *Web of Science*.

Susanto, H., Nabil Almunawar, M., & Chee Tuan, Y. (2017). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, 23 - 29.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información*.

Vivancos Cerezo, M. E. (06 de Agosto de 2018). *La seguridad en bibliotecas universitarias: normas y auditoría.* Obtenido de http://eprints.rclis.org/16220/1/Seguridad_informacion_en_BU_v1.pdf

6. ANEXOS

La presente sección contiene documentación que explican de manera detallada las plantillas utilizadas en la metodología de análisis de riesgos optimizada para bibliotecas y demás elementos considerados para el desarrollo e implementación del SGSI.

Anexo A – Recopilación de activos
Anexo B - Tabla de valoración del activo
Anexo C - Identificación de amenazas
Anexo D - Tabla de valoración de la amenaza
Anexo E - Selección de salvaguardas
Anexo F - Políticas de seguridad de las bibliotecas
Anexo G - Informe de evaluación de vulnerabilidades
Anexo H - Plan de seguridad de información de la biblioteca
Anexo I- Matriz de resultados
Anexo J - Preguntas de la entrevista realizar al Equipo de Proyecto
Anexo K - Valoración de activos
Anexo L - Valoración de las amenazas
Anexo M - Evaluación de madurez del SGSI
Anexo N - Recomendaciones para la mejora continua