UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA:

PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA

AUTOR/A:

JONATHAN ALEXIS BARRERA ACURIO

TUTOR/A:

ING. TANNIA CECILIA MAYORGA JÁCOME MG.

QUITO, ECUADOR

2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA, ha sido desarrollado por el señor Jonathan Alexis Barrera Acurio con C.C. No. 1721336095 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

JONATHAN ALEXIS BARRERA ACURIO

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **PROPUESTA DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN UTILIZANDO LA NORMA ISO 27001 PARA LA UNIDAD EDUCATIVA NUESTRA SEÑORA DE FÁTIMA**, presentado por Jonathan Alexis Barrera Acurio, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M. 12 de febrero de 2019

TUTOR

Ing. Tannia Cecilia Mayorga Jacome Mg.

AGRADECIMIENTOS

Mi presente trabajo de investigación principalmente lo dedico a mis padres Aníbal y Silvia ya que ellos son los principales promotores de mi sueño gracias por su amor, sacrificio en todos estos años, gracias porque jamás me hicieron faltar nada ni en el apoyo moral ni en la parte económica, y como no agradecer a mis hermanos por estar siempre presentes, acompañándome y por su apoyo moral cuando algún día dije me dijeron dale que tú puedes cumplirás uno de tus sueños.

Como no agradecer a Dios por los magníficos padres que me dio la vida porque él es el único que sabe el sacrificio que ellos han hecho para poderme dar mi educación sin saber que tenían que pasar ellos por no hacerme faltar nada.

Gracias también a Dios por los mejores abuelos que me dio, gracias a ellos porque nunca me dejaron solo cuando mis padres salían a buscar el pan de cada día, gracias a mis abuelos por criarme de la mejor forma, darme los mejores valores de vida y lo más importante la humildad de siempre, sé que mi abuelo desde el cielo está contento por este tan anhelado logro aun que daría lo que sea por tenerle aquí presente conmigo.

Agradezco a mis docentes porque en todos estos años me han compartido sus conocimientos a lo largo de la preparación de mi profesión, de manera especial a la magister Tannia Mayorga principal colaboradora durante mi proceso de titulación, quien me ha guiado con su paciencia, conocimientos, enseñanza y colaboración que permitió el desarrollo de mi trabajo de investigación.

TABLA DE CONTENIDOS

LISTA DE TABLAS

TABLA DE ILUSTRACIONES

RESUMEN

La seguridad de la información puede ser vista desde diferentes ángulos y, en general, este término abarca todo el espectro de una serie de problemas y sus soluciones, relacionados con redes informáticas, seguridad física de la información y a nivel de servidores, cifrado de datos, entre otros. En la Unidad Educativa Nuestra Señora de Fátima no cuentan con un Sistema de Seguridad e la Información por lo que todos sus activos en este respecto se encuentran en peligro. El Objetivo de este trabajo, fue proponer un Sistema para la gestión de la Seguridad de la Información basado en la Norma ISO 27001:2013, para esto, se realizó una caracterización del estado de la institución en base a los elementos requeridos por la ISO 27001:2013, se verifico la factibilidad técnica y operacional para materializar la implementación y se generó la propuesta de implementación. Se observó un 72% de incumplimiento con los requisitos formales de la norma y 78% de incumplimiento de los recaudos asociados al ANEXO A de la misma. Por su parte, la mayoría de los riesgos detectados se ubicaron dentro de la categoría de Alto y muy alto riesgo, así como un elevado índice de vulnerabilidad de los elementos asociados a el mantenimiento y trasferencia de la información, y de falta de documentación para controlar los procesos asociados al tema, por lo cual se terminó proponiendo un SGI apropiado a las condiciones observadas.

Palabras Claves: Seguridad de la Información, ISO 27001:2013, Vulnerabilidad, amenazas, Riesgo, Integridad de la información.

ABSTRACT

The security of information can be viewed from different angles and, in general, this term covers the entire spectrum of a series of problems and their solutions, related to computer networks, physical security of information and server level, data encryption, among others. In the Educational Unit of Our Lady of Fatima, they do not have a Security and Information System, so all their assets in this respect are in danger. The objective of this work was to propose a System for the management of Information Security based on ISO 27001: 2013, for this, a characterization of the state of the institution was made based on the elements required by ISO 27001:2013, the technical and operational feasibility was verified to materialize the implementation and the implementation proposal was generated. A 72% non-compliance with the formal requirements of the standard and 78% non-compliance with the collections associated with ANNEX A of the same was observed. On the other hand, most of the detected risks were placed within the category of High and very high risk, as well as a high vulnerability index of the elements associated with the maintenance and transfer of information, and lack of documentation to control the processes associated to the subject, for which reason it was finished proposing an SGI appropriate to the observed conditions.

Key words: Information Security, ISO 27001: 2013, Vulnerability, threats, Risk, Integrity of information.

INTRODUCCIÓN

Antecedentes de la situación objeto de estudio

De acuerdo al análisis realizado a la Unidad Educativa Nuestra Señora de Fátima se han encontrado varias problemáticas como en este caso el enfoque será la falta de seguridad informática como en el uso de los equipos computacionales del establecimiento, el uso de la web en los que abarca el ingreso a las redes sociales por parte de los estudiantes, la falta de cámaras de seguridad en lugares estratégicos del establecimiento ya que con eso pueden evitar cualquier incidente o comportamiento inadecuado , sospechoso y prevenir por ejemplo el consumo de sustancias, el hurto entre estudiantes, la falta de normas de seguridad para el uso de los laboratorios, como la instalación de antivirus con sus debidas restricciones a redes sociales y el acceso a páginas de pornografía, la vulnerabilidad que sufre la página web ya que para ello se está planteando implementar la norma ISO 27001 para así poder solventar los inconvenientes presentados por la Unidad Educativa.

"Según el blog ISO *Tools Excellence*, para las universidades se ha convertido en un requerimiento primordial la gestión de servicios de tecnología de la información, puesto que quieren que la prestación de sus servicios con la máxima calidad posible"

"Según el blog ISO *Tools Excellence*, Gracias al estándar ISO27001 se lleva a cabo la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) de forma eficiente. Su objetivo es otorgar valor a la información, ya que se trata de un activo clave para las universidades, para garantizar el éxito de las mismas y la continuidad de su negocio en el mercado. Por tanto, el principal objetivo para las universidades es asegurar lo mencionado anteriormente y llevar a cabo los sistemas que procesan esa información."

Tomando en cuenta lo mencionado en el blog ISO *Tools Excellence* se puede aplicar para las instituciones Educativas en este caso para la Unidad Educativa Nuestra Señora de Fátima ya que aquello viene a ser un factor primordial ya que al momento de realizar algún proceso tendrán que realizarlo con mayor y máxima calidad posible para que así la información tenga

un valor y se tenga el cuidado respectivo al momento de usarla, editarla, enviarla, borrarla entre otros.

El análisis de riesgos de la seguridad de la información con lleva a un proceso para el descubrimiento de anomalías, para proceder a una prevención y corrección de los problemas presentados. Este análisis de riesgos es un punto fundamental para así poder implementar niveles adecuados de seguridad.

Los riesgos del establecimiento pueden llegar a ser muchos como, por ejemplo: riesgo de gestión del programa, inversión de riesgo, riesgo de inventario, riesgo de responsabilidad legal, riesgo de seguridad, riesgo presupuestario entre otros.

Todos estos riegos son relacionados con el uso y operatividad de toda la información e infraestructura relacionada con el establecimiento, en base a los riesgos en listados obliga al personal encargado a utilizar información avanzada y actualizada para así cumplir sus misiones y llevar a cabo funciones importantes relacionadas con la Unidad Educativa Nuestra Señora de Fátima.

Planteamiento del problema

La Unidad Educativa Nuestra Señora de Fátima fue creada en 1964, este establecimiento empezó a tener un progreso positivo ya que llegaron a tener educación inicial, educación general básica, y hasta décimo de básica, el establecimiento se encuentra ubicado en la parroquia Chimbacalle, Cantón Quito calles Villonaco s8-99 Carihuairazo, Tipo de educación regular.

Con respecto a las consideraciones o estudios previos sobre la problemática son:

En la Unidad Educativa se ha encontrado varias deficiencias tecnológicas, en este caso el enfoque será la falta de seguridad informática como el uso de los equipos computacionales del establecimiento, el uso de la web en los que abarca el ingreso a las redes sociales por parte de los estudiantes, la falta de cámaras de seguridad en lugares estratégicos del establecimiento ya que con eso pueden evitar cualquier incidente o comportamiento inadecuado, sospechoso y prevenir por ejemplo el consumo de sustancias, el hurto entre estudiantes, la falta de normas de seguridad para el uso de los laboratorios, como la instalación de antivirus con sus debidas restricciones a redes sociales y el acceso a páginas

de pornografía, la vulnerabilidad que sufre la página web; por ello el uso de una norma de seguridad como la ISO 27001 sería la adecuada para el establecimiento educativo ya que "Según la División de Investigación de Alta Tecnología (Divindat) de la Dirincri (31 de julio 2017) la situación se complica en el caso de niños y adolescentes ya que, al ser nativos digitales, manipulan con mayor facilidad los dispositivos con acceso a internet. Sin la supervisión y orientación adecuadas, los menores de edad están más propensos a sufrir de incidentes como pornografía infantil,ciber-acoso, ciberbullyng, sexting, entre otros." ya que por ello sin ninguna norma de seguridad ellos pueden tener acceso a todo lo existente en la web.

"Según la empresa Digiware (31 de julio 2017) recopiló la información que Ecuador es el cuarto país que más recibe ataques cibernéticos en Latinoamérica con un 11,22% de los ataques recibidos. En el mismo informe Digiware revela que el continente recibe el 19% de los ataques a nivel global. De igual manera se revela que el 25% de los grupos activos de cibercriminales, han operado por 6 meses o menos y que el 50% De los grupos cibercriminales tienen 6 o más miembros."

Para Mayorga (2014), el problema de la seguridad de la información en las instituciones Educativas en Ecuador posee el siguiente matiz:

> En general se puede decir que Ecuador tiene una gran debilidad en lo que se refiere a Seguridad Informática en los Centros Educativos de Educación Inicial y Básica, y no existe un modelo general de políticas de seguridades informáticas a aplicarse en los Centros Educativos de Educación Inicial y Básica dejando mucho espacio para que los niños, niñas y adolescentes estén expuestos a los peligros informáticos. (pag. 3)

Formulación del problema

La propuesta de Sistema de gestión de Seguridad de la información utilizando la Norma ISO 27001 ayudará a concientizar sobre seguridades a la comunidad educativa de la Unidad Educativa Nuestra Señora de Fátima.

Por esto la **ISO 27001** ayuda a gestionar la seguridad de la información para ofrecer la mayor protección ante cualquier amenaza que este vulnerable la institución educativa.

Justificación

La finalidad de realizar este proyecto es para ayudar a solventar las necesidades tecnológicas que presenta la Unidad Educativa Nuestra Señora de Fátima, de acuerdo a lo presentado como necesidad se está estudiando la posibilidad de implementar la norma ISO 27001, así se podrá ayudar a solventar los inconvenientes como: la falta de seguridad informática como el uso de los equipos computacionales del establecimiento, el uso de la web en los que abarca el ingreso a las redes sociales, la falta de cámaras de seguridad en lugares estratégicos del establecimiento, la falta de normas de seguridad para el uso de los laboratorios, como la instalación de antivirus con sus debidas restricciones a redes sociales y el acceso a páginas de pornografía, la vulnerabilidad que sufre la página web.

Ayudando a solventar todas estas necesidades se tendrá muchas mejoras en la Unidad Educativa como el evitar el uso excesivo de redes sociales, el bloquear páginas pornográficas para evitar su propagación entre estudiantes, el estudio de instalación de cámaras de seguridad para evitar el hurto entre estudiantes, el consumo de sustancias, el abuso físico y sexual entre estudiantes, y el poner un valor a la información obtenida y guardada del establecimiento para que así puedan tener precaución al momento de editar, eliminar, enviar entre otros.

Objetivo General

Elaborar una propuesta con normas, políticas, estándares de seguridad informática, aplicando la Norma ISO 27001, para la Unidad Educativa Nuestra Señora de Fátima.

Objetivos Específicos

- Evaluar el estado actual del establecimiento respecto a las normas de seguridad informática.
- Identificar en qué sectores del establecimiento hay altos índices de vulnerabilidad.
- Diseñar las políticas, estándares, normas, de seguridad informáticas correctas y adecuadas en beneficio de la Unidad Educativa Nuestra Señora de Fátima.

Resumen

Como parte inicial se realizará estudios de todas las normas para así poder analizar cuál es la adecuada para la Unidad Educativa Nuestra Señora de Fátima tomando en cuenta todas sus necesidades para así poder solucionar los problemas que presentan.

Una de las normas más importantes para esta implementación es la norma ISO 27001 ya que esta ayuda proteger la información, también asegúrese de establecer y alinear su Sistema de Gestión de Seguridad de la Información a las leyes y las normas que se le apliquen. Debe considerar un sistema que le permite a las políticas de referencia cruzadas mediante muchas regulaciones y cumplimiento, usando hiperenlaces, para evitar la duplicación y la repetición.

La aplicación de la norma ISO 27001 es sólo el principio, una entidad viva, que respira para adaptarse al panorama digital en constante cambio. Existe poco valor en el propio certificado, sin embargo, hay mucho más en la estrategia de seguridad de la información y el proceso en sí. Con el conjunto correcto de herramientas que llega a su propio conjunto de políticas y procedimientos de gestión del riesgo asegurará que su Sistema de Gestión de Seguridad de la Información se convierte en una parte integrada e integral de sus procesos de negocio y no un manual burocrático que restringe las actividades comerciales normales.

Sistema de gestión de la seguridad de la información

Un sistema de gestión de la seguridad de la información es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

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. Como cualquier proceso de gestión, un SGSI estará dispuesto a mantener su eficiencia en un siglo prolongado de tiempo, siendo flexible ante los cambios internos de las empresas, así como los movimientos macroeconómicos que circundan el negocio.

Estos son uno de los pasos más importantes para la implementación de una norma ISO

1. Dar a conocer la norma
2. Nombrar encargado de la calidad
3. Realizar análisis de situación actual
4. Diseñar el sistema de calidad
5. Dar participación de los empleados
6. Poner en marcha el sistema de calidad
7. Realizar auditorías internas
8. Elegir organización certificadora
9. Realizar pre-auditoría
10. Realizar auditoría de certificación

1 CAPÍTULO I. FUNDAMENTACIÓN TEÓRICA

1.1.1 Seguridad de la Información

La seguridad de la Información es de interés para las organizaciones, independientemente de que sean lucrativas o no (Perafán, 2015). La información satisface las necesidades de los clientes y permite el reconocimiento de las características de un determinado contexto y apoya los procesos de decisión, lo cual, garantiza ejecutar acciones institucionales en consonancia con los objetivos planteados por la organización (Ramírez, 2014).

Como se desprende de lo anterior, la información en sí misma, junto a los sistemas de información, son una base importante para las empresas. Particularmente, la cada vez mayor transferencia de datos internos y entre empresas además dl empleo de redes abiertas, aumentan los riesgos a los que está expuesta la información y los sistemas de información, por lo cual, con el fin de reducir los riesgos y evitar daños a las empresas, se deben asumir determinadas consideraciones que garanticen adecuadamente la seguridad de la información (Disterer, 2013).

En las últimas décadas ha tenido lugar un proceso de modificación de la sociedad a partir de los continuos avances en las Tecnologías de la Información y la Comunicación–TIC- en cada ámbito de la vida cotidiana, como sugiere Torrent-Sellens, esto se debe a tres factores: primero, el proceso de revolución tecnológica que ha tenido lugar motivado por una alta inversión y uso de las TIC; segundo, la globalización que se ha generado a partir de dichas tecnologías que han ampliado a su vez un mercado demandante de productos y servicios relacionados con la información y la comunicación; y tercero, "*un nuevo patrón de las paulas de demanda de consumo e inversión de familias y empresas*" (Torrent-Sellens, 2008, pág. 36).

Para las empresas y organizaciones en general, la velocidad a la que se puede obtener y procesar información, la capacidad para almacenar y gestionar grandes volúmenes de datos, y la posibilidad de analizar dichos datos para generar información valiosa, han cambiado el panorama competitivo. En la actualidad la información es un recurso o un activo de valor para toda entidad, y al tener valor necesita estar segura.

Según exponen Berumen y Arriaza (2008) el valor de la información radica en que en la actualidad, los paquetes de estos, son susceptible de ser reducidos a mensajes cortos y que

pueden ser retrasmitidos (Berumen & Arriaza, 2008, pág. 10). Al respecto, Prats, Buxarrais, & Tey (2014) indican:

Uno de los cambios sustanciales de las sociedades occidentales actuales es el valor que ha adquirido la información. En una economía industrial, la acumulación de datos era un signo de poder; en una economía informacional, el poder viene marcado por la significación de estos datos. La capacidad técnica de relacionar datos y obtener información es un privilegio del momento actual. El patrimonio colectivo que significa obtener y gestionar los datos no está lo suficientemente ponderado por la mayoría de las personas, que ceden voluntariamente datos personales sin reparar en las consecuencias que ello puede comportar. (pág. 29)

Según se aprecia, una gran cantidad de personas ceden sus datos personales sin considerar las consecuencias de ello, no por un comportamiento inadecuado de las instituciones a quienes confían su información, sino porque esta se vuelve un recurso valioso para terceros, y debido al almacenamiento de grandes cantidades de esta en un solo lugar, pudiera ser sustraída, situación que, paradójicamente, se ha facilitado mediante la digitalización.

En base a lo anterior, Berumen y Arraiza (2008) señalan que, con la digitalización de los datos y la información, se potenció el desarrollo, la transmisión, la difusión, el análisis y la generación de nuevos conocimientos respecto a este cumulo de datos, los cuales en ocasiones podría ser empleados en procedimientos comerciales no consentidos por el dueño de dicha información, como por ejemplo, en el diseño de campañas publicitarias en base a perfiles creados desde información personal.

Ni los profesionales. ni los teóricos sobre el tema, logran ofrecer una definición única del concepto de "*riesgo de seguridad de la información*" (el sinónimo es "riesgo de la información"), por lo tanto, hay varias definiciones en la literatura (Vybornova, 2015; Odegov, 2013; Mikov, 2014):

1. La probabilidad de que ocurra un evento que tendrá un efecto indeseable en la organización y sus sistemas de información;
2. La posibilidad de que una amenaza pueda aprovechar la vulnerabilidad de un activo o grupo de activos y, por lo tanto, pueda dañar a la organización; siendo medido en base a la combinación de la probabilidad de ocurrencia del evento y sus consecuencias;

3. La posibilidad de causar daños asociados con una violación de seguridad de un sistema de información.

En base a lo anterior, se observa que los desafíos de administrar el riesgo de la información, provienen directamente de las dificultades y errores en la evaluación de los factores de riesgo, por lo tanto, es necesario pre-determinar todos los factores que lo afectan.

En la práctica, cuando se gestionan los riesgos de la información, solo se evalúan dos factores: la probabilidad de un evento (la ocurrencia de un incidente) y sus consecuencias (impactos negativos) (García & Salazar, 2005). Sin embargo, este enfoque no tiene en cuenta el hecho de que la probabilidad de un evento, a su vez, también consta de dos componentes: una amenaza para la seguridad de la información y la vulnerabilidad del sistema (CSAE, 2012a).

Una amenaza es una combinación de condiciones y factores que crean un peligro o potencian uno existente para algún sistema informático, por su parte, una amenaza es una situación en la que un intruso potencial detecta la presencia de una cierta vulnerabilidad en el *software* y la utiliza, lo que puede generar un impacto negativo en los activos y la infraestructura. Algo que explota una vulnerabilidad es una fuente de amenaza (Pérez, 2018; Tarazona, 2007).

Por su parte, las vulnerabilidades son debilidades en el *software*, *hardware* o en algún procedimiento, que puede permitir que un atacante acceda a un host virtual o directamente a los recursos informáticos (Tarazona, 2007). Sin una amenaza, la vulnerabilidad por sí sola no puede ser la causa de un incidente, y un ataque informático no puede realizarse sin una debilidad, por lo tanto, es entendible de todo lo anterior, que se debe evaluar no la probabilidad general del evento, sino el poder de la amenaza y el grado de riesgo por separado.

Otro factor importante que afecta el nivel de riesgo de seguridad de la información son las contramedidas, así, la magnitud de los impactos negativos depende de su efectividad (Celi & Díaz, 2017). El impacto es algo que conduce a daños en sobre los recursos informáticos en relación con la acción de una fuente de amenaza, y las contramedidas son medidas cuya implementación reduce las amenazas y vulnerabilidades y, por lo tanto, el nivel de riesgo de la información (Celi & Díaz, 2017).

1.1.2 Importancia de la seguridad de la información

Considerando lo mencionado en los acápites anteriores, la seguridad de la información es evidente que se encuentra encaminada a proteger y a prevenir cualquier riesgo que puedan sufrir los datos almacenados por una organización (Berumen & Arriaza, 2008).

La información es un activo de mucha importancia en la actualidad, las organizaciones trabajan con estos diariamente, también, es un activo muy valioso en determinados contextos, por lo cual, siempre se procura su protección, a través de la implementación de un conjunto de medidas con este fin, en tal sentido, la Organización Internacional para la Normalización / *International Engineering Consortium* - ISO/IEC, creó la norma numero 17799:2005, que luego, en el 2007 pasó a ser la ISO 27002, (ISO, 2005, pág. 2),en la que confirma que los sistemas de información son de suma importancia al describir que, sea cual sea la forma o el medio a través del cual la información es compartida o almacenada, se recomienda que esté siempre protegida adecuadamente (ISO, 2005, pág. 29).

La seguridad de la información hace referencia a la protección de los datos, sistemas y dispositivos (*hardware*) que utiliza una empresa para el almacenamiento y transmisión de la información. Por lo cual, el objetivo de estas conductas de seguridad, es la de proteger de forma adecuada los activos de información y de esta manera, asegurar la continuidad de sus operaciones, minimizando las posibles pérdidas (de estos activos), maximizando a su vez, el retorno de la inversión (Borges, 2016).

Para alcanzar el objetivo antes expuesto, Borges (2016, pág. 5), indica que es necesario preservar tres aspectos críticos de la información, que son: la confidencialidad, la integridad y la disponibilidad. La presentación correcta de estos aspectos de la información, garantiza la credibilidad y la confianza en las organizaciones y los negocios, además, puede lograrse en base a la aplicación de controles, mismos que pueden ser más o menos sofisticados y estructurados en base a una combinación de políticas, procedimientos, estructuras organizativas y mecanismos de medición física o de *hardware* y *software*.

En general, la seguridad de la información es un requisito obligatorio para minimizar los riesgos asociados a una actividad o negocio y asegurar así la conformidad con las disposiciones legales o de carácter regulatorio, como es el caso de reglamentos comunitarios o procedentes de la legislación de algún país (Córdoba, 2015).

1.1.3 Objetivos de la seguridad informática

La seguridad informática tiene como objetivo central la protección de los datos, sin embargo, desde una postura más amplia, también abarca, la protección de los recursos tecnológicos como equipos, servidores, *routers* cables, entre otros (Suárez & Ávila, 2015).

Estos objetivos se encuentran entrelazados a los preceptos indicados por Borges (2016, pág. 5): confidencialidad, integridad y disponibilidad, sin embargo, también se consideran viables los que proponía Areitio (2014, pág. 3), en su trabajo, estos, en esencia son los mismos, solo que adiciona la responsabilidad individual, y la confiabilidad (Ilustración 1).

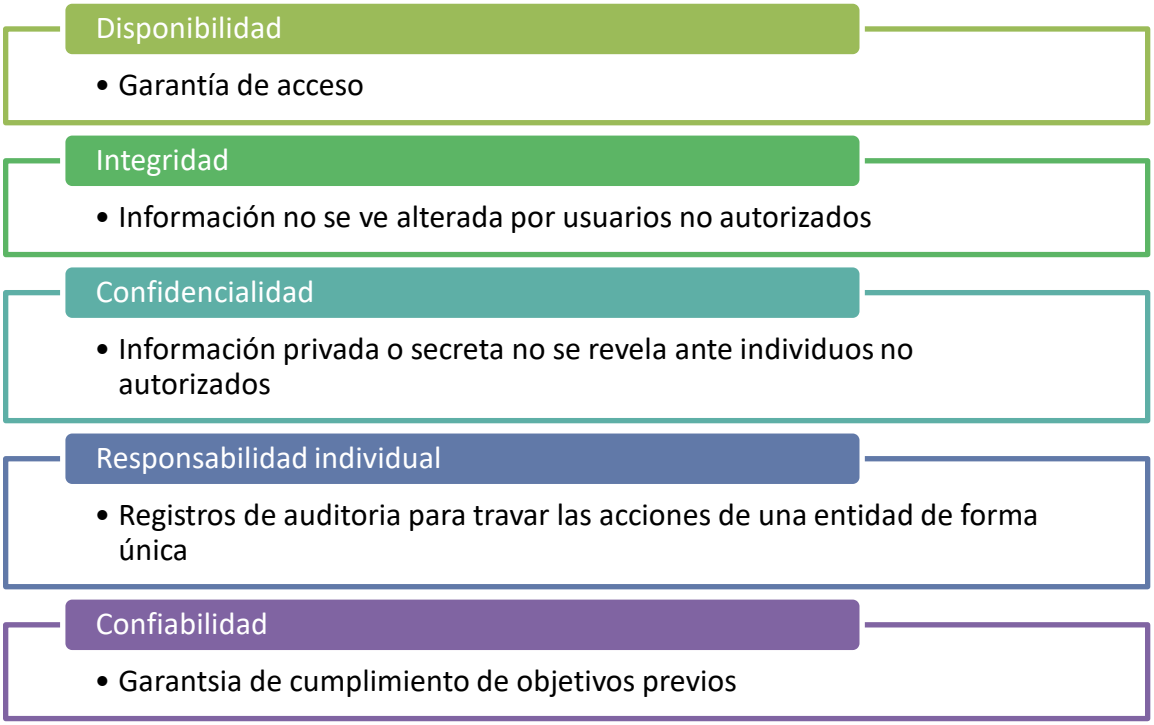


Ilustración 1. Objetivos de la seguridad de información
Fuente: Areitio (2014, pág. 3), Diseñado por el autor.

1.1.3.1 Confidencialidad

La confidencialidad de la información es la calidad o el estado de prevenir la exposición o el acceso no autorizado a la información por parte de individuos o sistemas, debe asegurar que sólo aquellos que poseen derechos y privilegios de acceso a un particular conjunto de

información son los que pueden hacerlo, este acceso legal es a menudo referido por el acceso autorizado y está permitido a las entidades acreditadas a tal efecto (Areitio, 2014).

La protección de la confidencialidad debe prevenir que aquellos que no deben tener acceso a la información no puedan obtener determinado tipo de datos por cualquier forma posible o alternativa. Cuando los individuos o sistemas no autorizados pueden acceder a la información, estamos ante una falla del sistema y puede afirmarse que hubo un compromiso o falla de confidencialidad (Romero, 2014).

1.1.3.2 Integridad de la información

La integridad de la información hace referencia a la calidad o estado de la información, en que ésta constituye un todo y que además, se encuentra completa (García & Alegre, 2011) y no ha sido corrompida (Borges, 2016).

Para Areitio (2014) la integridad de la información, es el segundo objetivo más importante, e indica que puede manejarse en dos vertientes, una es respecto a los datos y el otro es con el sistema.

Este autor, indica que la integridad de datos se refiere, a la necesidad de asegurar que la información del sistema no se vea afectada o alterada durante los procesos de almacenamiento, análisis o trasmisión; por su parte, la integridad del sistema es alcanzada cuando el sistema lógico y físico por donde se maneja el flujo de datos, realizan las actividades deseadas de manera adecuada, (Areitio, 2014). En otras palabras, la integridad pretende asegurar que los datos almacenados puedan ser recuperados de la misma manera: completos, legibles y sin fallas.

1.1.3.3 Disponibilidad de la información

La disponibilidad de la información hace referencia a que la información debe estar accesible a los sistemas y usuarios autorizados, sin interferencias u obstrucciones y en el formato requerido, se asegura de que sólo los usuarios que se hayan comprobado que tienen la

autorización adecuada (credenciales) para la información sean las que puedan acceder a los registros siempre y cuando lo deseen (Borges, 2016).

Sobre este tema, Ramos (2015), coincide en su trabajo, con que la disponibilidad debe asegurar que los usuarios autorizados pueden acceder a la información y sus recursos asociados cuando sea necesario. En términos operativos, cuando un usuario acreditado, logra acceder a los datos a los cuales está autorizado, se puede asegurar que los protocolos asociados a este tema funcionan adecuadamente.

1.1.3.4 Responsabilidad de la información

Según explica (Areitio, 2014), La responsabilidad sugiere que en el sistema puedan seguirse las acciones que ha realizado un usuario de forma específica, y con lo cual, se pueda poder asignar responsabilidades, tanto en caso de usuarios autorizados (conociendo quien llevó a cabo una acción específica como borrado, modificación o trasmisión de datos), o de usuarios no autorizados.

Con respecto al seguimiento de las acciones de los usuarios que manipulan sin autorización un sistema informático, es necesario tener en cuenta este objetivo para poder identificar y asignar sanciones que pueden llegar a ser de tipo legal (García & Alegre, 2011).

1.1.3.5 Confiabilidad de la información

El último objetivo confiabilidad o aseguramiento no suele ser considerado por todos los autores, sin embargo para Areitio (2014) implica que deba garantizarse el cumplimiento de los cuatro objetivos descritos anteriormente.

Según lo estima Areitio (2014), los objetivos antes mencionados, se encuentran relacionados entre sí, e inclusive, existen relaciones de dependencia entre ellos. Los primeros cuatro objetivos solo pueden llevarse a cabo cuando el sistema es funcional completamente, cuando ha sido diseñado de manera correcta y la calidad esperada, es decir, cumpliendo el objetivo de confiabilidad.

En este sentido, el buen funcionamiento de los protocolos de seguridad de la información, depende del *hardware* y del *software* empleado para mantener activo el sistema de flujo y almacenamiento de esta. según Areitio (2014), la confianza es vital, aunque no se cumplan los otros objetivos.

1.1.4 Activos de la información

Según resume el equipo de *ISOTools* (2015), los activos de la información pueden ser comprendidos como un conjunto que involucra a personas, tecnología y procesos, siendo estos responsables de alguna etapa del ciclo de vida de la información. Y en el caso de que se trate de un proceso de manipulación y procesamiento de la información, son los medios en que se almacena, los equipos en los que se manipulan, transportan y descartan dichos paquetes informativos.

La mayoría de las organizaciones suele dar más atención a los activos de mayor valor monetario o los menos comunes. Sin embargo, es importante identificar la participación del activo en el ciclo de vida de la información, o sea, cuanto mayor sea esa participación, mayor será la prioridad con que debe ser considerado en lo que se refiere a la seguridad de la información (Marciano & Marques, 2006).

Para asegurar que la información reciba un nivel adecuado de protección, los activos deben ser mapeados durante la planificación de la seguridad de la información, siendo de extrema relevancia la realización de su clasificación, la cual, determinará el grado de confidencialidad de los datos contenida en ellos (ISOTools, 2017).

De esta manera, la clasificación de los activos está relacionada con su grado de importancia, además, también es muy común la clasificación por el grado de privacidad que pueden tener, en este caso: "públicas" (información que puede ver el público sin mayores consecuencias); "Interna" (información relativa a determinados sectores o unidades de la empresa); y, "confidencial" (información restringida, donde sólo las personas autorizadas puedan acceder) (ISOTools, 2017).

Sin embargo, y a pesar de lo anterior, los activos, independientemente del grado de importancia, están sujetos a vulnerabilidades que pueden comprometer la seguridad de la información.

1.1.5 Vulnerabilidades

Según la norma ISO/IEC 27002 (2005), la vulnerabilidad es una fragilidad de algún activo o un grupo de estos, que puede ser explotado por una o más amenazas, incidiendo en la ruptura de uno o más principios de seguridad. Las vulnerabilidades están presentes en los propios activos, es decir, son inherentes a ellos, y pueden ser de orden tecnológico, humano, procesos y ambientes (Joya & Sacristán, 2017).

Como se aprecia, las vulnerabilidades por sí solas no provocan incidentes, pero estas fallas pueden ser explotadas por un agente causante o condición favorable para un evento negativo, que son las amenazas.

1.1.6 Amenazas

Las amenazas pueden provenir de diferentes formas, ya sean naturales o tecnológicas. La ISO/IEC 27002 (2005) define las amenazas de la seguridad de la información como una causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización. Según esto, las amenazas son agentes o condiciones que causan incidentes que comprometen la información y sus activos a través de la explotación de vulnerabilidades.

A principios de los años 2000 las principales amenazas eran los virus informáticos; en los últimos años, una de las amenazas más comunes son las derivadas del recurso humano o la llamada Ingeniería Social, que es un método de ataque donde alguien hace uso de la persuasión, muchas veces abusando de la ingenuidad o confianza del usuario, para obtener informaciones de manera (Fache, 2016).

Las amenazas siempre existieron y tienen los más diversos orígenes y a medida que la tecnología avanza, surgen nuevas formas a través de las cuales la información puede quedar expuesta, sin embargo, muchas organizaciones no dan el debido reconocimiento de que la seguridad de la información es importante y acaban dejando los activos de información sin las protecciones adecuadas, contribuyendo a la ocurrencia de incidentes de seguridad.

1.1.7 Incidentes de seguridad

De acuerdo con la ISO/IEC 27001:2005 (2007), un incidente de seguridad de la información es reconocido como uno o más eventos no deseados o inesperados, que tengan alguna probabilidad de comprometer las operaciones o los procesos del negocio y amenazar la seguridad de la información. Los incidentes son conceptuados como un acontecimiento que ocurre como consecuencia de la acción de una amenaza que explora una o más vulnerabilidades (Gómez, 2014).

Con esto, se entiende que un incidente de seguridad de la información puede ser entendido como la ocurrencia de un evento que pueda causar interrupciones en los servicios ofrecidos por los sistemas de información, causando perjuicios a los procesos del negocio. Entre una serie de tipos de incidentes presentes en gran parte de las organizaciones, Areitio, en su libro seguridad de la información (2008) indica que se pueden encontrar cuatro categorías:

1. Suplantación o mascarada: ocurre cuando una entidad atacante, simula ser una distinta. Este tipo de incidentes por lo general incluye algún otro tipo de ataque activo
2. Repetición: implica la captura pasiva de unidades de datos de los protocolos y su retransmisión.
3. Modificación de mensajes: implica la alteración de parte o de la totalidad de algún mensaje
4. Denegación de servicio: estas incidencias, normalmente impiden o inhiben el empleo de algún servicio de comunicación.

Un incidente genera impactos a los procesos de negocio de la empresa, pudiendo ser de mayor o menor gravedad y debe ser analizada para que las medidas más adecuadas puedan ser implementadas.

1.1.8 Probabilidad

Konzen (2013), define que en seguridad de la información la probabilidad es la posibilidad de que ocurra un incidente y asocia una escala de 0 a 1 a un evento que puede estar relacionado con una frecuencia de ocurrencia o un grado de confianza de que ocurrirá un evento.

Varios factores contribuyen a la probabilidad de que ocurra un incidente de seguridad, pero la principal relación está en la probabilidad de las amenazas y la gravedad de las vulnerabilidades, entre estos se pueden encontrar a los virus (CSAE, 2012a).

Como se puede percibir, cuanto mayor sea la probabilidad de las amenazas y la gravedad de las vulnerabilidades, mayor será la probabilidad de que se produzca un incidente de seguridad. Además de la probabilidad, se debe tener en cuenta el impacto que un incidente de seguridad pueda causar si ocurre (Konzen, 2013).

1.1.9 Impacto

Sémola (Konzen, 2013) describe el impacto como el alcance de los daños causados por un incidente de seguridad sobre uno o más procesos de negocio, en otras palabras, hace alusión directa a los posibles daños causados al negocio por un incidente de seguridad de la información. Estos perjuicios pueden significar pérdidas financieras, desgaste de la imagen, pérdida en la calidad de los servicios prestados, insatisfacción de los colaboradores y clientes, pérdida de recursos entre otros.

Cada organización tiene estrategias de negocio, procesos y capacidad de respuesta a incidentes diferentes entre sí, por lo que el impacto de un mismo incidente puede no ser igual para diferentes organizaciones, en este sentido, un mismo activo puede tener valor diferente dependiendo de la organización, y cuanto mayor sea la relevancia del activo, mayor será el impacto si sufre un incidente de seguridad. Por lo tanto, es necesario conocer los riesgos que cada eventual incidente de seguridad de la información representa para las organizaciones (Torres, 2015).

1.1.10 Riesgos

La ISO/IEC 27001:2005 (ISO, 2007), define el riesgo como la combinación de la probabilidad de un evento y de sus consecuencias. De esta manera, los riesgos pueden ser una oportunidad, una incertidumbre o una amenaza.

En el caso de que se produzca un cambio en la calidad de la información, se debe tener en cuenta que, el nivel del riesgo, independientemente del tipo de organización o de su segmento, está relacionado directa o indirectamente con diversas variables (ISO, 2007).

1.2 Gestión de Riesgos en la Seguridad de la Información

En base a lo anteriormente descrito, es claro observar que de las organizaciones están a menudo bajo riesgo. La presencia de estos, implica que tales organizaciones deben gestionar los aspectos de la comunicación por sí mismos, identificando, analizando y posteriormente evaluando si dichos riesgos deben ser tratados o no.

Este proceso de identificación, análisis y evaluación resulta en tomas de decisiones estratégicas por parte de la organización que, al detectar un riesgo, evalúa la dimensión del impacto de este y con qué frecuencia se produce.

En un proceso de implementación de Sistemas de Gestión de Seguridad de la Información, la gestión de riesgos es fundamental para el proceso de decisión, pues busca la identificación, evaluación y priorización de riesgos.

En esta fase se definen acciones para la aplicación coordinada y económica de los recursos para minimizar, monitorear y controlar la probabilidad y el impacto de eventos negativos, posibilitando la reducción del riesgo a un nivel aceptable (DAFP, 2006).

De acuerdo con Baccarini, Salm y Love (2004) muchos proyectos del área de Tecnología de la Información y Comunicación pecan por ineficaces y acaban fallando al no priorizar la etapa de gestión de los riesgos, haciendo que el fracaso de muchos proyectos de Gestión de Seguridad esté fuertemente relacionada con la gestión de riesgos.

Según Gerber y von Solms (2005), el proceso de gestión de riesgos se refiere a la planificación, monitoreo y control, basado en la información producida por la actividad de análisis de riesgos, que forma parte del proceso de gestión de riesgos. El *Project Management Institut*e, con su guía llamada PMBOK (2017) explica que la conducción de un análisis de riesgos puede dividirse en seis etapas distintas:

a) Planificación y estrategia: se caracteriza por la planificación de acciones y creaciones de estrategias de evaluación;
b) Identificación: creación de procedimientos para una correcta identificación de los riesgos;
c) Calificación: calificación de las amenazas y vulnerabilidades;

d) Cuantificación: puntuación del nivel de riesgo;
e) Impactos y respuestas: creación de procedimientos que determinen el impacto de un determinado riesgo y la respuesta que debe utilizarse; y
f) Monitoreo y Control: definición de procedimientos para un constante seguimiento de los riesgos y acciones realizadas para minimizarlos.

De acuerdo con Lichtenstein (1996), uno de los factores que son decisivos en la elección de un enfoque o metodología para la gestión de riesgos es el concepto de usabilidad, que está ligado exactamente a la facilidad de uso con que la metodología proporciona en todo proceso de realización de la gestión de riesgos, siendo que cuanto más usual y fácil es menos tiempo se gasta y, consecuentemente, menos costo se gasta para su aprendizaje.

Al comprender los riesgos que involucran los activos de información es posible entonces decidir qué hacer en relación con los riesgos identificados. Las estrategias o respuestas que pueden darse a los riesgos identificados, según Steinberg y col. (2004), se pueden definir cuatro categorías de respuestas para afrontar a los riesgos:

- Evitar: no se adopta tecnología o procesos que ofrezcan riesgos al negocio. La forma de tratar estos riesgos puede generar un nuevo riesgo mayor que el beneficio que puede traer, de esta forma se opta por evitar;
- Transferir: se transfiere el tratamiento de esos riesgos a terceros o a otro sector siendo una alternativa viable cuando su tratamiento aporte el costo de implantación del proyecto;
- Reducir: se adoptan mecanismos o controles que tengan la acción de mitigar el riesgo encontrado;
- Acceder: consiste en no tomar ninguna acción para reducir la probabilidad de ocurrencia o impacto.

Entre estas estrategias, la opción por reducción del riesgo implicará la determinación de un conjunto de medidas a ser implantadas a partir de un nivel de prioridad que es definido por la propia organización. Las acciones o conjunto de acciones que serán elegidos en respuesta al riesgo dependerá de la naturaleza del negocio y sus objetivos (Steinberg, Everson, Martens, & Nottingham, 2004).

Se observa que la definición de medidas contra los riesgos, necesita ser entendida como un proceso dinámico, adaptando los cambios generados en la organización, y siendo alcanzable desde el punto de vista financiero.

Estas discusiones acerca de los aspectos orientadores para la actuación de la seguridad de la información son fuertemente destacados en las normas de gestión de seguridad de la información que promueve ampliamente sus conceptos dentro de la organización a través de la implementación de controles, procesos, políticas y procedimientos, que juntos fortalecen los objetivos del negocio con la minimización de sus riesgos (NTP, 2007).

1.3 Normativas para la gestión de seguridad y riesgos de la información

Debido a la importancia de proteger la información y a los sistemas de eventos que puedan poner en riesgo los negocios de las empresas, se crearon varias normas que guían la implantación de procesos de gestión de seguridad de la información para garantizar las mejores prácticas; la *International Organization for Standartization* (ISO) y la *International Electrotechnical Commission* (IEC) estandarizaron internacionalmente este conjunto de normas y crearon la serie ISO/IEC 27000, la cual es aceptada en todo el mundo para este fin.

Las normas ISO/IEC 27001:2006, ISO/IEC 27002:2005 y ISO/IEC 27005:2008 son las principales normas de esta serie, pues describen los procesos básicos para la implantación de un sistema de gestión de seguridad de la información.

1.3.1 La familia de la norma ISO/IEC 27000

La ISO y la IEC desarrollaron en el año 2009, una familia de normas denominadas ISO/IEC 27000, la cual, sustituyó a la norma BS7799-2, emitida por la *British Standard*, en el año 2002.

Posteriormente, se realizaron cuatro modificaciones a esta en los años 2012, 2014, 2016 y 2018, siendo la ISO/IEC 27000:2018 "*Information Technology – Security Techniques – Information security management systems*" la última de estas modificaciones.

La serie ISO 27000, tiene como objetivo principal, ayudar a las empresas a mantener de manera segura, sus activos de información, tales como, información financiera, intelectual,

datos personales de los trabajadores, clientes, de los usuarios o información que ha sido confiada a terceras entidades. Estas normas, proporcionan directrices en la introducción, implementación y mantenimiento del SGSI que se aplicará a una organización (ISO, 2018).

Estas recomendaciones también tienen el propósito de proporcionar una base común en el desarrollo de prácticas y técnicas orientadas a la seguridad organizacional y establecer la confianza en las relaciones intra e inter organización (ISO, 2018).

De esta familia, forma parte un conjunto de normas que especifican los requisitos necesarios de un sistema de gestión de la seguridad de la información, la gestión de los riesgos, las métricas y las directrices para la aplicación de un sistema de gestión de la seguridad de la información.

En resumen, la familia de normas ISO/IEC 27000, incluye normas para: definir los requisitos para un SGSI; Prestar apoyo directo, orientación y/o interpretación detallada para el proceso global de establecer, implementar, mantener y mejorar un SGSI; proporcionar orientaciones sectoriales y específicas para SGSI; y generar directrices para realizar auditorías y evaluaciones de conformidad en los SGSI. La lista de estándares (ISO, 2018, pág. 19) de la familia ISO/IEC 27000 es la siguiente:

Tabla 1. Familia ISO/IEC 27001

Estándar	Nombre	Alcance:	Propósito:
ISO/IEC 27000	*Information technology — Security techniques — Information security management systems — Overview and vocabulary*	Este documento proporciona a organizaciones e individuos: Una visión general de la familia de normas ISMS; Una introducción a los sistemas de gestión de seguridad de la información; y Términos y definiciones utilizados en toda la familia de normas ISMS.	Este documento describe los fundamentos de los sistemas de gestión de seguridad de la información, que forman el tema de la familia de normas SGSI y definen los términos relacionados.
ISO/IEC 27001	*Information technology — Security techniques — Information security management systems — Requirements*	Este documento especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) formalizados en el contexto de los riesgos comerciales generales de la organización. Especifica los requisitos para la implementación de controles de seguridad de la información personalizados para las necesidades de organizaciones individuales o partes de las mismas. Este documento puede ser utilizado por todas las organizaciones, independientemente de su tipo, tamaño y naturaleza.	ISO/IEC 27001, proporciona requisitos normativos para el desarrollo y la operación de un SGSI, incluido un conjunto de controles para el control y la mitigación de los riesgos asociados con los activos de información que la organización busca proteger al operar su SGSI. Las organizaciones que operan un SGSI pueden tener su conformidad auditada y certificada. Los objetivos de control y los controles de ISO/IEC 27001: 2013, Anexo A se seleccionarán como parte de este proceso SGSI según corresponda para cubrir los requisitos identificados. Los objetivos de control y los controles enumerados en ISO/IEC 27001:2013, Tabla A.1 se derivan y se alinean directamente con los enumerados en ISO/IEC 27002: 2013, Cláusulas 5 a 18.
ISO/IEC 27006	*Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*	Este documento especifica los requisitos y proporciona una guía para los organismos que proporcionan auditoría y certificación ISMS de acuerdo con ISO/IEC 27001, además de los requisitos contenidos en ISO/IEC 17021. Su objetivo principal es respaldar la acreditación de los organismos de certificación que proporcionan la certificación ISMS de acuerdo con ISO/IEC 27001. Los requisitos contenidos en este documento deben ser demostrados en términos de competencia y confiabilidad por cualquiera que proporcione la certificación ISMS, y la guía contenida en este documento proporciona una interpretación adicional de estos requisitos para cualquier persona que proporcione la certificación ISMS.	ISO/IEC 27006 complementa a ISO/IEC 17021 al proporcionar los requisitos según los cuales están acreditadas las organizaciones de certificación, lo que permite a estas organizaciones proporcionar certificaciones de cumplimiento de manera consistente con los requisitos establecidos en ISO/IEC 27001.
ISO/IEC 27009	*Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*	Este documento define los requisitos para el uso de ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado). Explica cómo incluir requisitos adicionales a los de ISO/IEC 27001, cómo refinar cualquiera de los requisitos de ISO/IEC 27001 y cómo incluir controles o conjuntos de control además de ISO/IEC 27001:2013, Anexo A.	ISO/IEC 27009 garantiza que los requisitos adicionales o refinados no entren en conflicto con los requisitos de ISO/IEC 27001.
ISO/IEC 27002	*Information technology — Security techniques — Code of practice for information security controls*	Este documento proporciona una lista de los objetivos de control comúnmente aceptados y los controles de mejores prácticas que se utilizarán como guía de implementación al seleccionar e implementar controles para lograr la seguridad de la información.	ISO/IEC 27002 proporciona orientación sobre la implementación de controles de seguridad de la información. Específicamente, las cláusulas 5 a 18 brindan consejos de implementación específicos y orientación sobre las mejores prácticas para respaldar los controles especificados en ISO/IEC 27001:2013, A.5 a A.18.
ISO/IEC 27003	*Information technology — Security techniques — Information security management —Guidance*	Este documento proporciona una explicación y orientación sobre ISO/IEC 27001:2013.	ISO/IEC 27003 proporciona una base para la implementación exitosa del SGSI de acuerdo con ISO/IEC 27001.
ISO/IEC 27004	*Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*	Este documento proporciona pautas destinadas a ayudar a las organizaciones a evaluar el rendimiento de la seguridad de la información y la eficacia del SGSI para cumplir con los requisitos de ISO/IEC 27001:2013, 9.1. Aborda: El monitoreo y medición del desempeño de seguridad de la información; El monitoreo y la medición de la efectividad de un sistema de gestión de seguridad de la información (SGSI), incluidos sus procesos y controles; El análisis y la evaluación de los resultados de monitoreo y medición.	ISO/IEC 27004 proporciona un marco que permite evaluar y evaluar la efectividad de ISMS de acuerdo con ISO/IEC 27001.
ISO/IEC 27005	*Information technology — Security techniques — Information security risk management*	Este documento proporciona pautas para la gestión de riesgos de seguridad de la información. El enfoque descrito en este documento es compatible con los conceptos generales especificados en ISO/IEC 27001.	ISO/IEC 27005 proporciona orientación sobre la implementación de un enfoque de gestión de riesgos orientado a procesos para ayudar a implementar y cumplir satisfactoriamente los requisitos de gestión de riesgos de seguridad de la información de ISO/IEC 27001.
ISO/IEC 27007	*Information technology — Security techniques — Guidelines for information security management systems auditing*	Este documento proporciona orientación sobre la realización de auditorías de SGSI, así como orientación sobre la competencia de los auditores de sistemas de gestión de seguridad de la información, además de la guía contenida en la norma ISO 19011, que es aplicable a los sistemas de gestión en general.	ISO/IEC 27007 proporcionará orientación a las organizaciones que necesiten realizar auditorías internas o externas de un SGSI o administrar un programa de auditoría de SGSI según los requisitos especificados en ISO/IEC 27001.

Fuente: ISO (2018). Recopilado y diagramado por el Autor. (cont.)

Tabla 1. (Cont). Familia ISO/IEC 27001

Estándar	Nombre	Alcance:	Propósito:
ISO/IEC TR 27008	*Information technology — Security techniques — Guidelines for auditors on information security controls*	Este documento proporciona una guía sobre la revisión de la implementación y operación de los controles, incluida la verificación del cumplimiento técnico de los controles del sistema de información, en cumplimiento con los estándares de seguridad de la información establecidos por la organización.	Este documento proporciona un enfoque en las revisiones de los controles de seguridad de la información, incluida la verificación del cumplimiento técnico, en comparación con un estándar de implementación de seguridad de la información, establecido por la organización. No pretende proporcionar ninguna guía específica sobre la verificación de cumplimiento con respecto a la medición, evaluación de riesgos o auditoría de un SGSI según se especifica en ISO/IEC 27004, ISO/IEC 27005 o ISO/IEC 27007, respectivamente. Este documento no está destinado a auditorías de sistemas de gestión.
ISO/IEC 27013	*Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*	Este documento proporciona una guía sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1 para organizaciones que tienen la intención de: Implementar ISO/IEC 27001 cuando ya se implementó ISO/IEC 20000-1, o viceversa; Implementar ambos ISO/IEC 27001 e ISO/IEC 20000-1 juntos; Integrar los sistemas de gestión existentes basados en ISO/IEC 27001 e ISO/IEC 20000-1. Este documento se enfoca exclusivamente en la implementación integrada de un sistema de gestión de seguridad de la información (SGSI) como se especifica en ISO/IEC 27001 y un sistema de gestión de servicios (SMS) como se especifica en ISO/IEC 20000-1. En la práctica, ISO/IEC 27001 e ISO/IEC 20000-1 también pueden integrarse con otros estándares de sistemas de gestión, como ISO 9001 e ISO 14001.	Proporcionar a las organizaciones una mejor comprensión de las características, similitudes y diferencias de ISO/IEC 27001 e ISO/IEC 20000-1 para ayudar en la planificación de un sistema de gestión integrado que cumpla con ambas Normas Internacionales.
ISO/IEC 27014	*Information technology — Security techniques — Governance of information security*	Este documento proporcionará orientación sobre los principios y procesos para el gobierno de la seguridad de la información, mediante el cual las organizaciones pueden evaluar, dirigir y monitorear la administración de la seguridad de la información.	La seguridad de la información se ha convertido en un tema clave para las organizaciones. No solo hay requisitos reglamentarios crecientes, sino que también el fracaso de las medidas de seguridad de la información de una organización puede tener un impacto directo en la reputación de la organización. Por lo tanto, los órganos rectores, como parte de sus responsabilidades de gobierno, tienen cada vez más la obligación de supervisar la seguridad de la información para garantizar que se logren los objetivos de la organización.
ISO/IEC TR 27016	*Information technology — Security techniques — Information security management — Organizational economics*	Este documento proporciona una metodología que permite a las organizaciones entender mejor económicamente cómo valorar con mayor precisión sus activos de información identificados, valorar los riesgos potenciales para esos activos de información, apreciar el valor que los controles de protección de información entregan a estos activos de información y determinar el nivel óptimo de recursos Para ser aplicado en la obtención de estos activos de información.	Este documento complementa la familia de estándares ISMS al sobreponer una perspectiva económica en la protección de los activos de información de una organización en el contexto del entorno social más amplio en el que opera una organización y proporcionar orientación sobre cómo aplicar la economía organizacional de la seguridad de la información mediante el uso de Modelos y ejemplos.
ISO/IEC 27021	*Information technology — Security techniques — Information security management — Competence requirements for information security management systems professionals*	Este documento especifica los requisitos de competencia para los profesionales de ISMS que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del sistema de gestión de seguridad de la información que cumplen con la norma ISO/IEC 27001:2013.	Este documento está destinado a ser utilizado por: Las personas que deseen demostrar su competencia como profesionales del sistema de gestión de la seguridad de la información (SGSI), o que deseen comprender y cumplir la competencia requerida para trabajar en esta área, y que deseen ampliar sus conocimientos, Organizaciones que buscan posibles candidatos profesionales del SGSI para definir la competencia requerida para los puestos en roles relacionados con el SGSI, Organismos para desarrollar la certificación para profesionales de SGSI que necesitan un cuerpo de conocimiento (BOK) para las fuentes de examen, y Organizaciones de educación y capacitación, como universidades e instituciones vocacionales, para alinear sus programas de estudio y cursos con los requisitos de competencia para los profesionales de SGSI.
ISO/IEC 27010	*Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*	Este documento proporciona directrices además de la orientación proporcionada en la familia de normas ISO/IEC 27000 para implementar la gestión de la seguridad de la información dentro de las comunidades que comparten información. Este documento proporciona controles y orientación específicamente relacionados con el inicio, la implementación, el mantenimiento y la mejora de la seguridad de la información en las comunicaciones entre organizaciones y entre sectores.	Este documento es aplicable a todas las formas de intercambio e intercambio de información sensible, tanto pública como privada, nacional e internacionalmente, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a intercambios de información y compartir información relacionada con la provisión, el mantenimiento y la protección de la infraestructura crítica de una organización o estado.
ISO/IEC 27011	*Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations*	Este documento proporciona directrices que respaldan la implementación de controles de seguridad de la información en las organizaciones de telecomunicaciones.	ISO/IEC 27011 permite a las organizaciones de telecomunicaciones cumplir con los requisitos básicos de gestión de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.

Fuente: ISO (2018). Recopilado y diagramado por el Autor (cont.)

Tabla 1. (Cont). Familia ISO/IEC 27001

Estándar	Nombre	Alcance:	Propósito:
ISO/IEC 27017	*Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*	ISO/IEC 27017 proporciona pautas para los controles de seguridad de la información aplicables a la provisión y el uso de servicios en la nube al proporcionar: Guía de implementación adicional para los controles relevantes especificados en ISO/IEC 27002; Controles adicionales con guías de implementación que se relacionan específicamente con los servicios en la nube.	Este documento proporciona controles y guía de implementación para los proveedores de servicios en la nube y los clientes de servicios en la nube.
ISO/IEC 27018	*Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*	ISO/IEC 27018 establece objetivos de control, controles y pautas comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad de ISO/IEC 29100 para el entorno de computación en la nube pública.	Este documento es aplicable a organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que proporcionan servicios de procesamiento de información como procesadores de PII a través de la computación en la nube bajo contrato con otras organizaciones. Las pautas en este documento también pueden ser relevantes para las organizaciones que actúan como controladores de PII. Sin embargo, es posible que los controladores de la PII estén sujetos a leyes, regulaciones y obligaciones de protección de la PII adicionales, que no se apliquen a los procesadores de la PII, y estos no están cubiertos en este documento.
ISO/IEC 27019	*Information technology — Security techniques —* Information security controls for the energy utility industry	Este documento proporciona una guía basada en ISO/IEC 27002:2013 aplicada a los sistemas de control de procesos utilizados por la industria de energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor, y para el Control de los procesos de soporte asociados. Esto incluye en particular lo siguiente: Control centralizado y distribuido de procesos, tecnología de control y automatización, así como sistemas de información utilizados para su funcionamiento, como dispositivos de programación y parametrización; Controladores digitales y componentes de automatización, como dispositivos de control y de campo o controladores lógicos programables (PLC), incluidos sensores digitales y elementos de actuador; Todos los sistemas de información de soporte adicionales utilizados en el dominio de control de procesos, p. Ej. para tareas complementarias de visualización de datos y para fines de control, monitoreo, archivo de datos, registro de historiadores, informes y documentación; Tecnología de comunicación utilizada en el dominio de control de proceso, p. Ej. redes, telemetría, aplicaciones de telecontrol y tecnología de control remoto; Componentes de infraestructura de medición avanzada (AMI), por ejemplo, contadores inteligentes; Dispositivos de medición, por ejemplo, para valores de emisión; Protección digital y sistemas de seguridad, por ej. relés de protección, PLC de seguridad, mecanismos de control de emergencia; Sistemas de gestión de energía, por ej. de recursos energéticos distribuidos (DER), infraestructuras de carga eléctrica, en hogares privados, edificios residenciales o instalaciones industriales de clientes; Componentes distribuidos de entornos de redes inteligentes, por ejemplo, en redes de energía, en hogares privados, edificios residenciales o instalaciones industriales de clientes; Todo el *software*, el firmware y las aplicaciones instaladas en los sistemas mencionados anteriormente, por ejemplo, Aplicaciones DMS (sistema de gestión de distribución) u OMS (sistema de gestión de interrupciones); Cualquier local que contenga los equipos y sistemas mencionados anteriormente; Sistemas de mantenimiento remoto para los sistemas mencionados. Este documento no se aplica al dominio de control de procesos de las instalaciones nucleares. Este dominio está cubierto por IEC 62645. Este documento también incluye un requisito para adaptar la evaluación de riesgos y los procesos de tratamiento descritos en ISO/IEC 27001:2013 a la orientación específica del sector de la industria de energía eléctrica que se proporciona en este documento.	Además de los objetivos y medidas de seguridad que se establecen en ISO/IEC 27002, este documento proporciona pautas para los sistemas utilizados por las empresas de energía y los proveedores de energía en los controles de seguridad de la información que abordan otros requisitos especiales.
ISO 27799	*Health informatics — Information security management in health using ISO/IEC 27002*	Este documento proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de administración de la seguridad de la información, incluida la selección, implementación y administración de los controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización. Este documento proporciona una guía de implementación para los controles descritos en ISO/IEC 27002 y los complementa cuando es necesario, para que puedan ser utilizados de manera efectiva para administrar la seguridad de la información de salud.	ISO 27799 proporciona a las organizaciones de salud una adaptación de las directrices ISO/IEC 27002 únicas para su sector industrial, que son adicionales a la guía proporcionada para cumplir con los requisitos de ISO/IEC 27001:2013, Anexo A.

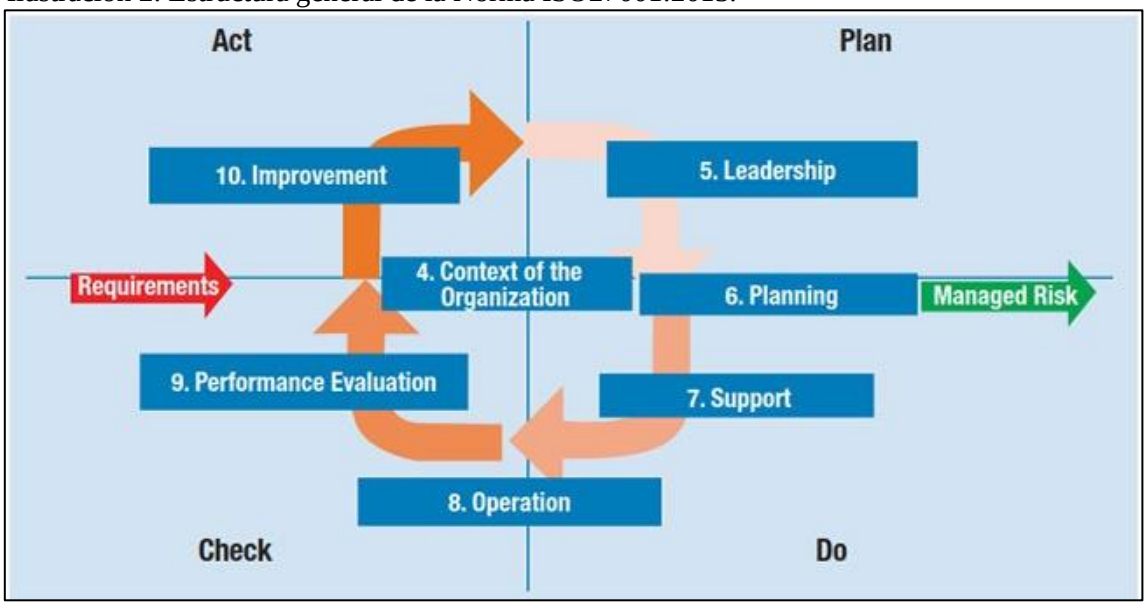
Fuente: ISO (2018). Recopilado y diagramado por el Autor (cont.)

1.4 Entorno del estándar ISO/IEC 27001:2013

La ISO/IEC 27001:2013 especifica los requisitos relativos a un sistema de gestión de seguridad de la información que permite a las organizaciones evaluar sus riesgos e implementar los procedimientos necesarios para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como principal objetivo impedir que la información sea utilizada por terceros no deseados o perdida de forma irremediable (Gaona, 2013).

Además de la interconexión existente entre esta norma y otras de la serie 27000, posee una alineación explícita con la norma ISO 31000:2013, en la cual se incluyen, los requisitos para la evaluación y el tratamiento de riesgos de seguridad información a la medida de las necesidades de la organización (ISO, 2014, pág. 10). Los requisitos establecidos en la norma ISO/IEC 27001 "*son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza*." (ISO, 2014, pág. 10). La estructura global de la norma ISO/IEC 27001 puede presentarse de la siguiente manera:

Ilustración 2. Estructura general de la Norma ISO27001:2013.



Fuente: Mataracioglu. *Proposal for the Next Version of the ISO/IEC 27001 Standard* (2017).

La norma ISO/IEC 27001, se compone de dos módulos relativamente distintos, en el primero de estos, se definen las reglas y los requisitos que deben ser aplicables. "Excluir cualquiera de los requisitos especificados en las Cláusulas 4 a 10 no es aceptable cuando una

organización declara conformidad con esta Norma." (ISO, 2014, pág. 10), El segundo componente de la norma, es el referente al de los controles, designados como los puntos A.5 a A.18 y " son directamente derivados desde y alineados con los listados en ISO/IEC 27002:2013, Cláusulas 5 a 18" (ISO, 2014, pág. 27).

Estos objetivos de control enumerados en el Anexo A no son exhaustivos y pueden ser necesarios objetivos de control adicionales, es decir, "las organizaciones pueden diseñar controles o identificarlos de cualquier fuente.” (ISO, 2014, pág. 16).

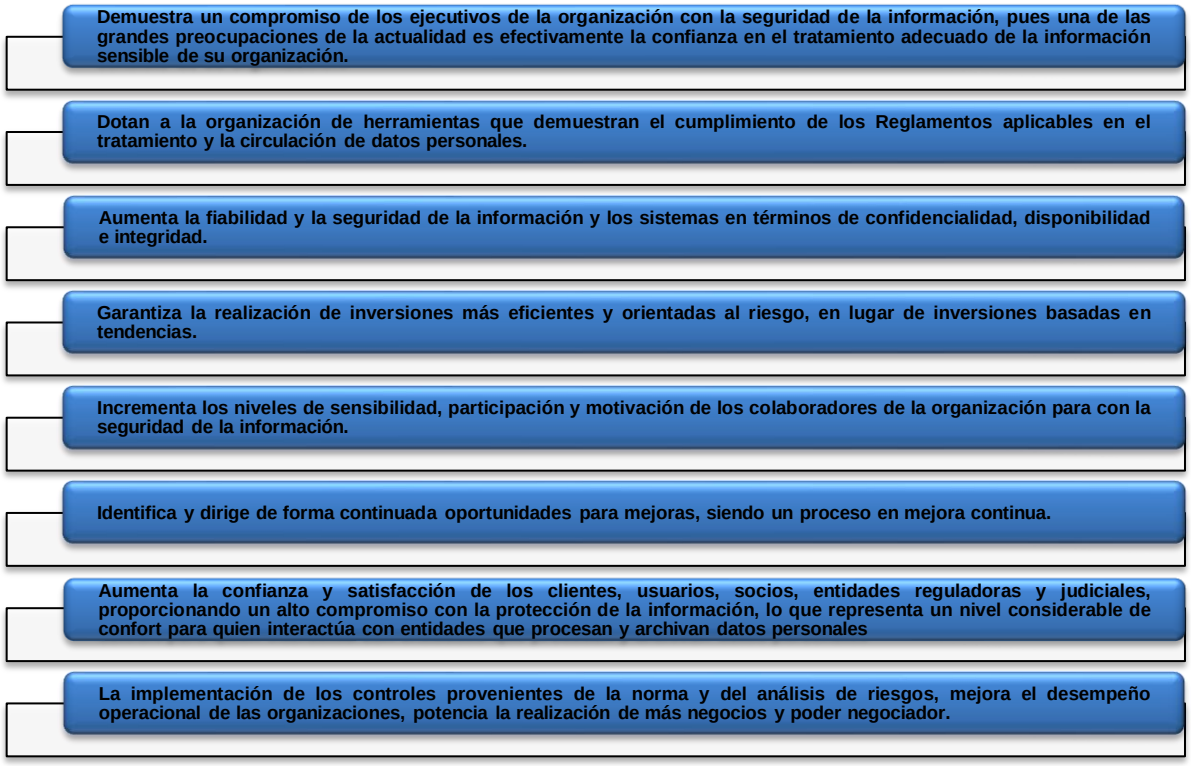
1.5 Beneficios de la aplicabilidad de la norma ISO/IEC 27001

La norma ISO IEC 27001 es universal para todos los tipos de organizaciones, ya sean comerciales, gubernamentales, con o sin fines de lucro, pero transmite flexibilidad en la especificación de los requisitos para la implementación de controles de seguridad que se pueden personalizar según las necesidades de determinadas empresas.

Como otras normas del sistema de gestión ISO, la certificación ISO/ IEC 27001 es posible, pero no obligatoria. Algunas organizaciones sólo optan por implementar estos estándares internacionales para beneficiarse de las mejores prácticas que estas normas especifican, Cada vez más responsables de Sistemas y Tecnologías de la Información, reconocen que la adopción de puntos de referencia de buenas prácticas y normas universales son de gran valor para el éxito de sus proyectos (itSMF, 2015).

Independientemente de que las organizaciones aseguren o no, la inclusión de todas las prácticas de gestión documentadas en la norma, siempre representa un conjunto de beneficios tras su adopción, en particular:

Ilustración 3. Beneficios de la aplicación de la Norma ISO 27001.



Fuente: *ISOTools* (2015). Diagramado por el autor

1.6 Implementación de un sistema de gestión de la seguridad de la información

La implementación de un SGSI resulta de la estandarización de buenas prácticas que incluye la producción de documentación, procedimientos, instrucciones, herramientas y técnicas, además de la creación de indicadores, registros y en la definición de un proceso educativo de concienciación en la organización (Córdoba, 2015).

El éxito de un SGSI comienza con la garantía de la aplicabilidad de una de las recomendaciones más importantes de la norma ISO/IEC 27001:2013 en que "*La alta dirección debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información*." (ISO, 2014, pág. 12). Según se expone en la normativa anteriormente citada, este liderazgo y compromiso se debe demostrar:

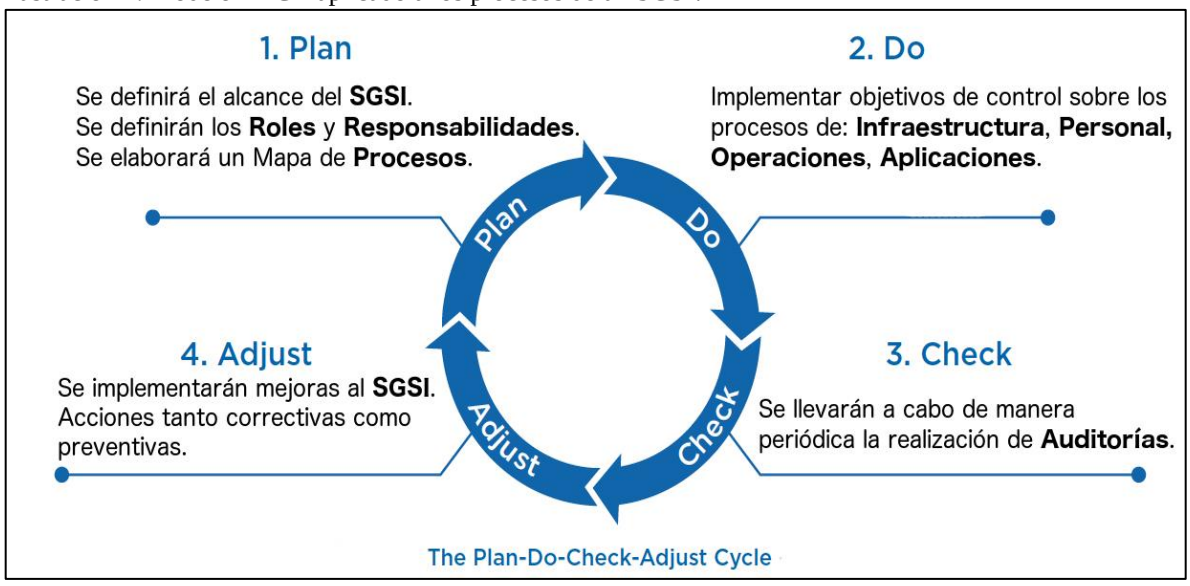
- Asegurando que la política de seguridad de la información y los objetivos de seguridad de la información, están establecidos y son compatibles con la orientación estratégica de la organización;

- Asegurando la integración de los requisitos del sistema de gestión de la información en los procesos de la organización;
- Asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información están disponibles
- Comunicando la importancia de una gestión de la seguridad de la información eficaz y de conformidad con los requisitos del SGSI
- Asegurando que el sistema de gestión de la seguridad de la información alcanza los resultados deseados;
- Orientando y apoyando a las personas para contribuir a la eficacia del sistema de gestión de la seguridad de la información;
- Promoviendo la mejora continua;
- Apoyando otras funciones de gestión relevantes a demostrar su liderazgo, según sea aplicable a sus áreas de responsabilidad.

Teniendo en cuenta que la organización debe establecer, aplicar, mantener y mejorar de forma continua un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de la norma ISO/IEC 27001:2013, se debe aplicar un modelo de gestión que satisfaga este propósito (Córdoba, 2015).

El modelo PDCA (*Plan-Do-Check-Act* o ciclo de mejora continua de Deming), es una de las herramientas de gestión que favorece ese propósito, pues este modelo de gestión está basado en el ciclo de mejora continua. El modelo PDCA (Ilustración 3), prioriza un ciclo de actividades que, en su conjunto, define la forma de establecimiento de un Sistema de Gestión de Seguridad de la Información, que integra: su implementación y operación, su monitorización y revisión y, finalmente, su optimización en función de los resultados obtenidos en cada interacción del proceso (VHGroup, 2018).

Ilustración 4. Modelo PDCA aplicado a los procesos de un SGSI.



Fuente: VHGroup (2018).

Las fases 1 y 2 del ciclo PDCA mostrado en la ilustración 4, corresponden a las etapas de construcción del SGSI, y se corresponden con el diseño y definición del contexto de acción, el análisis de riesgos, la formalización estratégica de gestiones de riesgo, la documentación y la selección de los controles aplicables para reducir los riesgos cuando sea necesario. Así, la implementación del SGSI se da efectivamente en las dos primeras fases del ciclo PDCA.

Las fases tres y cuatro del ciclo de PDCA, están relacionadas con la verificación y la medición del desempeño de los procesos en comparación con las políticas del SGSI. El objetivo que la norma pretende obtener con este modelo, es la correcta gestión de los sistemas de seguridad de la información, teniendo como base las expectativas y necesidades específicas de la organización.

El sistema de gestión de seguridad de la información debe realizarse teniendo en cuenta no sólo el proceso de análisis/evaluación y tratamiento de riesgos, sino que también, las medidas de control sugeridas en normas de la familia ISO/IEC 27000 y el modelo de proceso PDCA.

1.7 Factores críticos para el éxito de la implementación de un SGSI

La implementación de un sistema de seguridad de la información en una organización, es un proceso transversal que influye en todas las áreas orgánicas de la empresa debido a que, como se resume de los acápites anteriores, al aplicar este programa, se estará transmitiendo una imagen de preocupación en esta materia a todos los sectores de la institución, cada vez más importante y con mayor visibilidad, logrando al mismo tiempo gestionar el riesgo al que está sujeta la empresa.

El programa de seguridad de este modo, cumple con los objetivos de la creación de una base de protección y confianza sobre la cual se desarrolla una actividad; señal clara e inequívoca de que la organización tiene preocupaciones fundamentales con la integridad y preservación de sus activos (ya sean procesos, servicios, información u otros); además de afirmar por esta vía al entorno externo a la institución, la dedicación y el cuidado particular de los intereses de socios, ciudadanos, usuarios o proveedores.

De esta manera, se puede resumir en base a los aportes encontrados en una amplia variedad de informes, y trabajos basados en la experiencia de los autores o grupos de consultores expertos en el tema (GMV, 2007; Condori, 2012; Seclén, 2016; Mendoza, 2017), que algunos factores críticos para el éxito de la implementación del sistema de seguridad de la información, dentro de la organización, en particular son:

a) Una política de seguridad cuyos objetivos y actividades reflejen los objetivos estratégicos y la misión de la organización;
b) Compromiso y apoyo visible del consejo directivo;
c) Una aplicación de la seguridad de la información consistente con la cultura organizativa;
d) Un claro entendimiento de los requisitos de seguridad, evaluación y gestión de riesgos;
e) Una divulgación compartida de las directrices sobre las normas y políticas de seguridad de la información para todos los colaboradores, proveedores de servicios y socios.

1.8 Caracterización de la organización

1.8.1 Reseña de la institución

El Colegio Particular Nuestra Señora de Fátima, es una institución privada de doctrina católica creado el 14 de diciembre de 1964 bajo el amparo del con el Acuerdo Ministerial 4083. La fundación del instituto educativo fue realizada por la Congregación de Hermanas Misioneras de Santa Teresita del Niño Jesús, el mismo pertenece a la Arquidiócesis de Quito, Teniendo una trayectoria de 49 años, y en la actualidad trabaja con seis grados de instrucción primaria. Su Funcionamiento se da en jornadas matutinas del régimen sierra (Colegio N.SRA. Fatima, S.F).

En el año 2005, se aprueba bajo Acuerdo Nº 4526 y Resolución 1200 del 12 de julio de ese mismo año, el funcionamiento del octavo año, y el 12 de febrero de 2007 se autoriza el funcionamiento del Noveno y el Décimo Año de la educación básica (Colegio N.SRA. Fatima, S.F).

1.8.2 Actividad y Entorno

La institución objeto de estudio, enmarca sus actividades en el área de la formación académica de niños y jóvenes, con lo cual, además de contar con las aulas de clases convencionales, posee una sala de computación donde todos los estudiantes realizan las actividades de la materia de computación, así como también de otras materias que requieran el uso de las salas informáticas.

Adicionalmente, el entorno administrativo, cuenta con una serie de ordenadores en los que se realizan principalmente tareas administrativas, entre las que se encuentran el control de las notas.

1.8.3 Estructura Organizacional

1.8.4 Plan estratégico

La planeación estratégica de la institución, esta expresada en su página *web* (Colegio N.SRA. Fatima, S.F), la misma está compuesta por Misión, Visión y Valores, los cuales se muestran textualmente a continuación

- **Misión:**

  "Somos una Institución Educativa Católica Diocesana con experiencia, calidad y calidez; brindamos a nuestros estudiantes una educación integral que forma seres humanos responsables, participativos y capaces de responder críticamente a los retos que la sociedad exige; Empleando nuevas técnicas, metodologías alternativas y profesionales, para fortalecer la identidad ecuatoriana, el sentido de la Iglesia y la excelencia académica en los niños y jóvenes, teniendo un Cristo como hermano, amigo y maestro. A partir de las transformaciones científicas, tecnológicas, culturales, sociales y ambientales, desarrollamos un Proyecto Institucional coherente, dinámico y pertinente, que facilitan el desarrollo del pensamiento crítico y el alcance de los estándares, para ello se apoyan en talento humano altamente calificado, recursos Técnicos y tecnológicos" (Colegio N.SRA. Fatima, S.F).

- **Visión**:

  "Nuestra Institución Educativa Nuestra Señora de la Fátima como parte de la Arquidiócesis de Quito, para el año 2017, será reconocida como la institución de la excelencia en el marco de los servicios propuestos por el Ministerio de Educación, a través de la formación integral, humanista, Incluyendo e innovadora, basada en los valores cristianos y la verdad evangélica" (Colegio N.SRA. Fatima, S.F).

- **Valores** (Colegio N.SRA. Fatima, S.F):

Fe.	Amor	Verdad.
Libertad.	Solidaridad.	Respeto.
Calidad	Eclesialidad	Trascendencia

2 CAPÍTULO II. PROPUESTA

2.1. Diagnóstico de la situación actual

Esta etapa se realizará con la finalidad de dar respuesta a los objetivos específicos uno y dos de la presente investigación, en cuyo caso, se requiere de una evaluación de las condiciones actuales de vulnerabilidad informática en la institución y de la identificación de los elementos más vulnerables.

2.1.1. Recopilación de información

Se realizó para esto un inventario de activos de la información, con dichos datos, se verificó el estado actual de cumplimiento de los elementos de seguridad de la información, los cuales pueden ser vulnerables y que deben ser considerados en la propuesta de implementación de un SGSI.

Tabla 2. Inventarios de equipos tecnológicos de la Institución Educativa "Nuestra Señora de la Fátima"

Tipo	Equipos	Marca/ Modelo	Procesador	Velocidad	Capacidad RAM	Capac_ Disco Duro	Equipos ACTIVOS	GARANTIA	SO	Version
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	128 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	256 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	256 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	256 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	128 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	1,7 GHZ	256 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	2.56 GHZ	256 MB	80 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	2,53 GHZ	256 MB	80 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	PENTIUM IV	1,8 GHZ	256 MB	60 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	PENTIUM III		64 MB	40 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	2.8 GHZ	256 MB	80 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	2.8 GHZ	256 MB	80 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
COMPUTADOR_DE ESCRITOIO	**1**	CLON	INTEL CELERON	2.8 GHZ	256 MB	80 GB	**1**	FINALIZADA	WIN-XP	OFF PRO 2003
TOTAL	**13**						**13**			

Datos Aportados por la institución y verificados visualmente por Autor.

Tabla 3. Identificación de activos y nivel de vulnerabilidad

	Descripción del activo	Tipo	Electrónica	Dueño del activo	Acceso	Responsable	AUTENTICACIÓN	INTEGRIDAD	CONFIDENCIALIDAD	Puntos	Valor
INSTALACIONES	Lab. de Computación	TANGIBLE		Institución	RLBC	RLBC	Alta	Crítica	Restringuida	11	Alta
	Oficina Rectorado	TANGIBLE		Institución	REC	REC	Alta	Crítica	Restringuida	11	Alta
	Oficina Vice rectorado	TANGIBLE		Institución	VIC	VIC	Alta	Crítica	Restringuida	12	Alta
	Oficinas Administrativas	TANGIBLE		Institución	ADM	ADM	Alta	Crítica	Restringuida	11	Alta
	Sala de Profesores	TANGIBLE		Institución	DOCENTES	DOCENTES	Alta	Alta	Restringuida	10	Normal
	Oficinas DOBE	TANGIBLE		Institución	DECE	DECE	Normal	Crítica	Restringuida	10	Normal
	Oficina Inspección	TANGIBLE		Institución	INS	INS	Normal	Crítica	Restringuida	10	Normal
	Aulas Secundaria	TANGIBLE		Institución			Normal	Crítica	Restringuida	9	Normal
	Aulas Primaria	TANGIBLE		Institución			Normal	Crítica	Restringuida	9	Normal
HARDWARE	Desktop pc de uso institucional.	TANGIBLE	Equipo de computo	Institución	EOF	DOC. INFOR.	Normal	Alta	Restringuida	11	Alta
	Impresoras	TANGIBLE	Equipos de impresión	Institución	EOF	DOC. INFOR.	Baja	Baja	Libre	5	Baja
	Router principal de la Institución	TANGIBLE		CNT	RLBC	DOC. INFOR.	Baja	Alta	Protegida	8	Normal
	Router principal de Administración	TANGIBLE		CNT	ADM	ADM	Normal	Alta	Protegida	9	Normal
	Puntos de Acceso Inalámbricos	TANGIBLE		CNT	RLBC	RLBC	Normal	Baja	Restringuida	8	Normal
	Proyectores	TANGIBLE		Institución	DOC	DOC	Baja	Baja	Libre	5	Baja
	Dispositivos móviles personales	TANGIBLE	Dispositivos móviles	DOCENTES	DOC	DOC	Normal	Baja	Restringuida	8	Normal
APLICACIONES	Sistemas Operativos	INTANGIBLE	Equipo de computo	Microsoft	RLBC	COMPUTACION	Alta	Crítica	Confidencialidad	15	Alta
	Ofimática	INTANGIBLE	Equipo de computo	Microsoft	RLBC	COMPUTACION	Alta	Alta	Restringuida	11	Alta
DATOS/INFORMACION	Facturación	INTANGIBLE	Equipo de computo	SEC	ADM-CON	ADM	Crítica	Normal	Restringuida	11	Alta
	Roles de pago	INTANGIBLE	Archivador	SEC	ADM-CON	ADM	Crítica	Alta	Protegida	12	Alta
	Contratos	INTANGIBLE	Archivador	SEC	ADM-SCA	ADM	Normal	Alta	Restringuida	9	Normal
	Notas Académico	INTANGIBLE	Archivador	DOC	DOC	DOC	Crítica	Alta	Confidencialidad	14	Alta
	Notas académicas	INTANGIBLE	Equipo de computo	DOC	DOC	DOC	Crítica	Alta	Protegida	12	Alta
	DOBE	TANGIBLE	Equipo de computo	DOBE	DOBE	PSICOLOGA	Normal	Crítica	Protegida	11	Alta
	Matriculación	TANGIBLE	Equipo de computo	SEC	SEC	SEC	Normal	Alta	Restringuida	12	Alta
REDES /COMUNICACI	Internet	INTANGIBLE		CNT	RLBC	DOC. INFOR.	Crítica	Alta	Restringuida	12	Alta
	Red de Área Local	INTANGIBLE		Institución	RLBC	DOC. INFOR.	Alta	Normal	Restringuida	9	Normal
	Coneccion Inalámbrica	INTANGIBLE		CNT	RLBC	DOC. INFOR.	Normal	Baja	Libre	5	Baja
PERSONAL	Administrativo de la Institución	TANGIBLE		Institución	Administrativo	Administrativo	Crítica	Crítica	Protegida	14	Alta
	Personal Docente	TANGIBLE		Institución	Administrativo	Administrativo	Alta	Alta	Protegida	13	Alta
	Personal de conserjería	TANGIBLE		Institución	Administrativo	Administrativo	Normal	Baja	Restringuida	7	Normal
	Estudiantes	TANGIBLE		Institución	Estudiantes	Institución	Alta	Alta	Protegida	12	Alta

Elaborado por el Autor

Tabla 4. Caracterización de las posibles amenazas detectados con influencia sobre los activos

ACTIVO	AMENAZA		VULNERABILIDADES
DATOS / INFORMACIÓN	Errores de utilización ocurridos durante la recogida y transmisión de datos.	Información errónea	Falta de control en el manejo de datos
	Errores de ruta, secuencia o entrega de la información durante el tránsito.	Acceso a los archivos	Los archivos no son administrados con permiso de usuario
	Acceso físico con inutilización.	Acceso a las oficinas	Manipulación de equipos fuera de hora de trabajo
	Acceso lógico con modificación de información en tránsito.	Acceso lógico	Modificación de la información
SOFTWARE	Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.	Daños a equipos	Las computadoras de los laboratorios son usadas por los estudiantes sin ningún control de los docentes.
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Daño de *software* de los equipos de cómputo.
	Errores de ruta, secuencia o entrega de la información durante el tránsito.	Acceso a los archivos	Los archivos no son manejados con una administración por grado de confidencialidad.
	Acceso físico con inutilización.	Acceso a las computadoras	Perdida o hurto de información de los computadores de los docentes
	Acceso lógico con modificación de información en tránsito.	Acceso lógico	El uso de las computadoras por parte de los alumnos sin ninguna supervisión puede causar el uso inadecuado.
HARDWARE	Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.	Inundaciones	Debido a los cambios climáticos la información y las aulas se encuentran en riesgo
	Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.	Daños a equipos	Las computadoras del establecimiento no tienen un grado de privacidad, por ello sufren una de daño físico o lógico.
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Cableado eléctrico descubierto, falta de protección
	Acceso físico con inutilización.	Acceso a las computadoras	Mal uso de los equipos informáticos por parte de los estudiantes.
COMUNICACIONES	Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.	Inundaciones	Por el mal estado del techo de las aulas, se pone en riesgo la parte interna
	Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.	Daños a equipos	El uso de las computadoras por parte de los alumnos sin ninguna supervisión puede causar el uso inadecuado.
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Conexiones eléctricas descubiertas
	Acceso físico con inutilización.	Acceso a los dispositivos de red	Configuración de los equipos en la red inexistente
	Acceso lógico con intercepción pasiva simple de la información.	Acceso lógico de forma pasiva	No existe controles de acceso lógico.
	Acceso lógico con modificación de información en tránsito.	Acceso con modificación	Por no contar con servidores en la institución, no se puede verificar el acceso

Elaborado por el Autor

Tabla 4. (Cont). Caracterización de las posibles amenazas detectados con influencia sobre los activos

ACTIVO	AMENAZA		VULNERABILIDADES
INSTALACIONES	Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.	Incendios e inundaciones	Mal estado de las conexiones eléctricas puede provocar accidentes de gravedad.
	Accidente físico de origen natural, riada, fenómeno sísmico o volcánico.	Daños físicos	Mal estado de tuberías puede provocar inundaciones
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Cables al intemperie puede provocar la pérdida de energía eléctrica
PERSONAL	Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.	Incendios e inundaciones	Mal estado de conexiones eléctricas y tuberías puede poner en riesgo la integridad del personal de la institución
	Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.	Daños	Riesgos que puede sufrir la institución
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Falta de personal
	Acceso físico con inutilización.	Acceso a las instalaciones	El personal de limpieza desconecta cables al momento de hacer la limpieza.
	Repudio del origen o de la recepción de información en tránsito.	Repudio del origen de la recepción de la información.	Falta de control al personal
SISTEMAS DE SEGURIDAD Y CONTROL DE ACCESO	Accidente físico de origen industrial, incendios, explosiones, inundaciones, contaminación.	Incendios e inundaciones	Mal estado de techo, conexiones eléctricas, tuberías, puede causar incendios, inundaciones.
	Averías que pueden ser de origen físico o lógico, se debe al el efecto de origen.	Daños y averías de cables	Cables eléctricos expuestos a la intemperie
	Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicaciones, fluidos y suministros.	Interrupción de servicios	Instalaciones eléctricas y tuberías en mal estado
	Acceso físico con inutilización.	Acceso a las instalaciones	Al salir de la institución el personal desconecta

Elaborado por el Autor

Tabla 5. Medición del nivel de riesgo detectado en la institución educativa

ACTIVO	AMENAZAS		VULNERABILIDAD	FRECUENCIA O PROBABILIDAD	CRITERIO	IMPACTO	CRITERIO	VALOR	NIVEL DE RIESGO
	TIPO	AMENAZA							
DATOS / INFORMACIÓN	Daño físico	Destrucción del equipo o los medios	Falta de esquemas de reemplazo periódico.	2	Algunas veces	3	Medio	6	Normal
		Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	2	Algunas veces	1	Muy Bajo	2	Normal
	Eventos naturales	Inundación	Ubicación en una área susceptible de inundación.	1	Casi nunca	1	Muy Bajo	1	Normal
	Pérdida de los servicios esenciales	Pérdida del suministro de energía	Red energética con toma corrientes susceptibles a manipulación y fallas eléctricas.	1	Casi nunca	4	Alta	4	Normal
		Falla en el equipo de comunicaciones	Conexión de cables accesibles a manipulación.	3	A menudo	4	Alta	12	Alta
	Perturbación debida a la radiación	Radiación electromagnética	Sensibilidad a la radiación electromagnética.	3	A menudo	2	Bajo	6	Normal
	Compromiso de la información	Hurto de medios de documentos	Almacenamiento sin protección.	1	Casi nunca	4	Alta	4	Normal
		Hurto de equipo	Falta de política formal sobre la utilización de computadores portátiles.	4	Casi siempre	3	Medio	12	Alta
	Fallas técnicas	Fallas del equipo	Falta de planes de continuidad.	3	A menudo	4	Alta	12	Alta
		Incumplimiento en el mantenimiento	Mantenimiento insuficiente.	3	A menudo	3	Medio	9	Normal
	Acciones no autorizadas	Uso no autorizado del equipo	Falla en la producción de informes de gestión.	5	Siempre	5	Muy alto	25	Crítico
		Abuso de derechos	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	5	Siempre	4	Alta	20	Alta
			Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.	5	Siempre	4	Alta	20	Alta
		Falsificación de derechos	Falta de mecanismos de identificación y autenticación, como la autenticación de usuario.	4	Casi siempre	5	Muy alto	20	Alta
SOFTWARE	Daño físico	Destrucción del equipo o los medios	Falta de esquemas de reemplazo periódico.	1	Casi nunca	3	Medio	3	Normal
		Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	1	Casi nunca	1	Muy Bajo	1	Normal
	Pérdida de los servicios esenciales	Pérdida del suministro de energía	Falta de protección a los equipos tecnológicos en caso de pérdida de la energía eléctrica.	5	Siempre	5	Muy alto	25	Crítico
	Compromiso con la información	Manipulación del *software*	Descarga y uso no controlados de *software*	3	A menudo	3	Medio	9	Normal
	Acciones no autorizadas	Uso no autorizado del equipo	Falla en la producción de informes de gestión.	3	A menudo	3	Medio	9	Normal
		Procesamiento ilegal de datos	Habilitación de servicios innecesarios	3	A menudo	4	Alta	12	Alta
	Compromiso de las funciones	Error de uso	Falta de documentación	3	A menudo	3	Medio	9	Normal
		Abuso de derechos	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.	5	Siempre	5	Muy alto	25	Crítico
			Distribución errada de los derechos de acceso.	5	Siempre	5	Muy alto	25	Crítico
		Falsificación de derechos	Falta de mecanismos de identificación y autenticación, como la autenticación de usuario.	5	Siempre	5	Muy alto	25	Crítico
			Gestión deficiente de las contraseñas.	4	Casi siempre	4	Alta	16	Alta
		Incumplimiento en el mantenimiento	Mantenimiento insuficiente.	3	A menudo	2	Bajo	6	Normal
HARDWARE	Daño físico	Destrucción del equipo o los medios	Falta de esquemas de reemplazo periódico.	2	Algunas veces	3	Medio	6	Normal
		Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	1	Casi nunca	1	Muy Bajo	1	Normal

Elaborado por el autor (Cont).

Tabla 5 (Cont.). Medición del nivel de riesgo detectado en la institución educativa

ACTIVO	AMENAZAS		VULNERABILIDAD	FRECUENCIA O PROBABILIDAD	CRITERIO	IMPACTO	CRITERIO	VALOR	NIVEL DE RIESGO
	TIPO	AMENAZA							
	Pérdida de los servicios esenciales	Pérdida del suministro de energía	Susceptibilidad a las variaciones de tensión.	1	Casi nunca	1	Muy Bajo	1	Normal
		Falla en el equipo de comunicaciones	Conexión de cables accesibles a manipulación.	5	Siempre	5	Muy alto	25	Crítico
	Compromiso de la información	Manipulación con el *hardware*	Acceso sin restricción a las computadoras por parte del personal.	5	Siempre	4	Alta	20	Alta
			Intercambio de dispositivos extraíbles	5	Siempre	4	Alta	20	Alta
	Fallas técnicas	Incumplimiento en el mantenimiento	Mantenimiento insuficiente.	3	A menudo	2	Bajo	6	Normal
		Uso no autorizado del equipo	Falla en la producción de informes de gestión.	4	Casi siempre	3	Medio	12	Alta
	Compromiso de las funciones	Error de uso	Falta de control de cambio con configuración eficiente.	3	A menudo	3	Medio	9	Normal
		Falsificación de derechos	Falta de mecanismos de identificación y autenticación, como la autenticación de usuario.	5	Siempre	4	Alta	20	Alta
COMUNICACIONES	Daño físico	Destrucción del equipo o los medios	Falta de esquemas de reemplazo periódico.	2	Algunas veces	2	Bajo	4	Normal
		Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad.	1	Casi nunca	1	Muy Bajo	1	Normal
	Pérdida de los servicios esenciales	Pérdida del suministro de energía	Susceptibilidad a las variaciones de tensión.	1	Casi nunca	1	Muy Bajo	1	Normal
		Fallas del equipo de telecomunicaciones	Conexión de cables accesibles a manipulación.	4	Casi siempre	4	Alta	16	Alta
	Compromiso de la información	Manipulación con el *hardware*	Acceso sin restricción a las computadoras por parte del personal.	4	Casi siempre	4	Alta	16	Alta
	Fallas técnicas	Falla del equipo	Poca protección de los equipos ante la suspensión de la energía eléctrica.	4	Casi siempre	4	Alta	16	Alta
		Incumplimiento en el mantenimiento	Mantenimiento insuficiente.	3	A menudo	2	Bajo	6	Normal
	Acciones no autorizadas	Uso no autorizado del equipo	Falta de seguridad en los equipos por estar expuestas a manipulación.	4	Casi siempre	4	Alta	16	Alta
INSTALACIONES	Eventos naturales	Inundación	Ubicación en una área susceptible de inundación.	4	Casi siempre	5	Muy alto	20	Alta
	Pérdida de los servicios esenciales	Pérdida del suministro de energía	Susceptibilidad a las variaciones de tensión.	1	Casi nunca	5	Muy alto	5	Normal
	Acciones no autorizadas	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones.	4	Casi siempre	5	Muy alto	20	Alta
	Fallas técnicas	Incumplimiento en el mantenimiento	Susceptibilidad a las variaciones de tensión.	1	Casi nunca	1	Muy Bajo	1	Normal
	Compromiso de las funciones	Abuso de derechos	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso.	4	Casi siempre	4	Alta	16	Alta
		Incumplimiento en el mantenimiento	Mantenimiento insuficiente.			2	Bajo	0	Normal
		Negación de servicios	Falta de asignación adecuada de responsabilidades en la seguridad de la información.	4	Casi siempre	4	Alta	16	Alta

Elaborado por el autor (Cont).

En primer lugar, se puede observar que la institución no cuenta con un amplio stock de equipos computacionales activos, todos los equipos indicados en la tabla 2, son los que en la actualidad se encuentran operativos y los cuales se distribuyen tanto en el área administrativa como en la sala de computación.

Los equipos que se encuentran activos, en su totalidad, son de vieja data, y las prestaciones de cada uno no son las más óptimas de entre los equipos actuales. Así mismo, no se observó la presencia de ningún servidor informático, y la conexión a internet, se realiza principalmente desde el Router de la compañía que suministra el servicio de internet.

Los elementos observados, de antemano, denotan las condiciones en las que se encuentra la implementación completa de un SGSI en la institución, la cual, dada las características de los equipos, las condiciones de las conexiones y el desconocimiento por parte de la institución de los estándares mínimos de seguridad informática a aplicar, implican que la implementación de dicho sistema de gestión requiere de la reestructuración total de las condiciones antes señaladas en la institución.

En la tabla 3 de identificación de activos y nivel de vulnerabilidad, observamos que, en casi todos los activos detectados, existe una alta proporción de elementos con un nivel de vulnerabilidad, alto. La mayoría de los activos, en las condiciones actuales, y si no se toman las políticas de seguridad de la información adecuada, pueden ser objeto de ataques, intencionados o no, que atenten contra la continuidad de la existencia de los datos o que favorezcan la manipulación inadecuada de los mismos

Por su parte, en la tabla 4 y 5, se aprecia que las vulnerabilidades divisadas tras una inspección de las instalaciones equipos y rutinas de trabajo, que generan una serie de amenazas particulares que afectan la integridad de los activos, prácticamente representan a la gran mayoría de las infecciones o ataques posibles, esto se debe a que en la institución no se ha implementado en ningún momento algún tipo de control sobre la gestión de la información, y los recursos, a través del tiempo, han sido manejados sin atender las mínimas previsiones al respecto.

2.1.2. Factibilidad Técnica

En base a los datos aportados por la institución, se aprecia que la factibilidad de la implementación de un SGSI en las condiciones de equipos actuales (Tabla 2), es poco viable. Como se verifico en la **Tabla 2 de inventario de equipos tecnológicos**, los equipos son obsoletos, que funcionan con sistemas operativos, a los que incluso ya el fabricante (*Microsoft*®) dejó de dar soporte técnico y de ofrecer parches de seguridad actualizados.

En este sentido, se requiere de la inversión en nuevos equipos con sistemas operativos más actualizados, así como la adquisición de las respectivas licencias para sistemas antivirus, esto como parte de una inversión mínima,

Además, deben considerar la adquisición de un *ruter* con mejores prestaciones técnicas, con el cual, se administre adecuadamente el acceso a la red, esto implica adicionalmente la inversión mínima necesaria para la implementación del sistema de cableado requerido.

Como se aprecia, son varias las acciones que se deben implementar para que la institución pueda asegurarse comenzar de manera adecuada la implementación de un SGSI, todas estas, requieren de una considerable inversión inicial, que, si bien pudiera no resultar tan elevada como la que pudiera requerir una empresa de mayor envergadura, si representa un costo que la institución debe considerar asumir.

2.1.3. Factibilidad Operacional

A pesar de la necesidad de inversión antes mencionada, la implementación del SGSI, es viable en términos operativos, siempre que la institución decida realizar la inversión en los activos computacionales y su enlazado adecuado a una red interna.

La situación determinada por la adquisición de nuevos equipos, ofrece la ventaja de una configuración desde cero del sistema de gestión de la información, lo cual garantizaría la implementación de los estándares y los procesos asociados a este. Los equipos actuales pueden ser empleados igualmente para la implementación del sistema de gestión, principalmente si previo a esto, se realiza una actualización de los mismos, principalmente en lo que respecta el sistema operativo, sin embargo, esta opción, evidentemente es de segunda preferencia ante el planteamiento de la renovación de los activos.

2.1.4. Modelo o estándar a aplicar

Se aplicará la norma ISO 27001 ya que ayuda a gestionar la seguridad de la información para así obtener una mayor protección ante cualquier amenaza, también para evitar el peligro de pérdida o daño de los activos de la información al que puede estar expuesto la Unidad Educativa Nuestra Señora de Fátima.

3. CAPÍTULO III. IMPLEMENTACIÓN

3.1. Desarrollo del Proyecto. Soporte de la Dirección.

3.1.1. Propósito de la propuesta

El propósito de este documento es establecer una propuesta de un Sistema de Gestión de la Seguridad de la Información mediante la aplicación del estándar ISO/IEC 27001:2013.

3.1.2. Razones.

La principal motivación para la realización de la presente propuesta de implementación, es la adecuación de la situación actual de la Unidad Educativa Nuestra Señora de Fátima, con respecto a los elementos de los sistemas de seguridad de la información, a las directrices técnicas operativas y de control dispuestas en la norma iniciales de esta propuesta mediante el estándar ISO/IEC 27001:2013, los cuales son:

> Establecer un punto de partida para la implementación de un Sistema de Gestión de la Seguridad de la Información que garantice la confidencialidad, integridad y disponibilidad de la información, asumiendo niveles de riesgos aceptables (ISO27000.es, 2015).
>
> Comprender la importancia y beneficios que ofrece un Sistema de Gestión de la Seguridad de la Información en la optimización de los procesos institucionales (ESAN, 2016).

3.1.3. Objetivos de la propuesta

Los objetivos de la propuesta se enumeran a continuación:

1. Evaluar el estado actual del establecimiento respecto a las normas de seguridad informática.
2. Identificar en qué sectores del establecimiento hay altos índices de vulnerabilidad.
3. Diseñar las políticas, estándares, normas, de seguridad informáticas correctas y adecuadas en beneficio de la Unidad Educativa Nuestra Señora de Fátima
4. Facilitar las herramientas para generar un plan de abordaje de los riesgos detectados en la institución educativa en el cual se logren definir adecuadamente

las medidas de control mínimas recomendadas que logren subsanar la situación de riesgo actualmente presente.

5. Conocer cuáles son los elementos de seguridad más críticos en la unidad educativa, con lo cual se pueda generar un plan específico de acción para su control y mitigación.

3.1.4. Duración y Estructura del Proyecto

La presente propuesta de implementación, únicamente se corresponde con la etapa de planificación del SGSI, por lo tanto, no existe una planificación especifica en el tiempo para su aplicación, debido a que la implementación de estos controles responderá a las posibilidades de inversión de la institución, la cual, podrá emplear el presente documento como guía, y en efecto, planificar en torno a sus posibilidades la implementación del mismo.

3.1.5. Responsabilidades

La implementación de la presente propuesta, estará a cargo de la dirección ejecutiva del plantel, la cual, designará en su respectivo momento una comisión técnica con las credenciales adecuadas para lograr la implementación definitiva del mismo, esta comisión, repartirá oportunamente entre sus miembros las responsabilidades pertinentes para la ejecución de la implementación.

3.1.6. Recursos

Los recursos incluidos para la planeación del Sistema de Gestión de la Seguridad de la Información están catalogados en Humanos y Técnicos (Tabla 6).

Tabla 6. Empleo de recursos en la implementación del SGSI en la unidad educativa

Recursos	Descripción
Humanos	Personal Docente y administrativo de la institución
Técnicos	Herramientas de ofimática (procesador de texto, hojas de cálculo, *software*s de SGSI).
Otros	Normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 y otros documentación empleados comúnmente en el análisis y evaluación de riesgos

Elaborado por el autor.

3.2. Alcance del SGSI propuesto

3.2.1. Propósito, Alcance y Usuarios

La presente propuesta, es aplicable a toda la documentación, actividades y procesos desarrolladas en la Unidad Educativa Nuestra Señora de Fátima referentes a la planificación y desarrollo del Sistema de Gestión de la Seguridad de la Información propuesto, en el mismo, se espera su aplicación por parte de todo el personal administrativo docente y alumnado de la institución en la medida que para cada usuario se aplique alguno de los aspectos que en el sistema propuesto se detallan.

3.2.2. Grado real de ajuste a la norma

Previo a la implementación del plan propuesto, se sugiere que la comisión conformada por la institución educativa Nuestra Señora de Fátima, realice una evaluación actualizada del cumplimiento de los requerimientos del estándar ISO/IEC 27001:2013.

Para esto, se debe realizar un análisis diferencial de los aspectos obligatorios del punto 4 al 10 de la norma (requisitos obligatorios) y del Anexo A (ISO, 2014).

Esta evaluación previa a la implementación es necesaria debido a que, con ella, la institución puede comparar las condiciones actuales al momento previa a la ejecución con respecto a lo que requiere la normativa.

3.2.3. Requisitos de la Norma ISO/IEC 27001:2013

Para que una organización este acorde al estándar no se deben excluir ninguno de los requisitos especificados en los temas obligatorios del 4 al 10.

A continuación, se pueden observar los resultados del nivel actual de conformidad y cumplimiento de estos requisitos por parte de la Unidad Educativa Nuestra Señora de Fátima:

Tabla 7. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto al contexto de la Organización.

Req	Contexto de la Organización	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar

4.1	Comprender a la organización yde su contexto	SI	Se conoce adecuadamente a la organización, su contexto, misión, visión y objetivos estratégicos.	Implementar políticas relacionadas con la TI ajustado con los requerimientos de la institución acorde con los objetivos estratégicos, las capacidades,recursos, y estructura organizacional.
4.2	Comprender las necesidades y expectativas de las partes interesadas	SI	Se conoce adecuadamente a las partes interesadas en la implementación del SGSI.	Vincular a todas las unidades administrativas y la gerencia de la institución en la implementación del Sistema de Gestión de Seguridad de la Información.
4.3	Determinación del alcance del sistema de gestión de la seguridad de la información	SI	El sistema de gestión de seguridad de la información propuesto, se aplicará en la Unidad Educativa Nuestra Señora de Fátima abarcando tanto a la parte administrativa como operativa de la institución.	Comunicar a los docentes, y personal administrativo, la relevancia de la aplicación de la propuesta del sistema de gestión en la institución, así como, conseguir un nivel adecuado de compromiso y concientización con las políticas que por esta causa se adopten.
4.4	Sistema de Gestión de Seguridad de la Información	NO	En la actualidad no existe ningún tipo de sistema de gestión aplicado.	Implementar la propuesta de sistema de gestión generada, a través de un proceso organizado y sistemático de mejora continua, con el cual se disminuyan los niveles de riesgo presentes

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 8. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto al Liderazgo.

Req	Liderazgo	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar
5.1	Liderazgo y Compromiso	SI	La directiva de la institución, se encuentra consiente de la necesidad de la implementación de un sistema de gestión de la información, y en tal sentido, se encuentran al tanto de la generación de la presente propuesta , y así mismo, están dispuestos a prestar toda la colaboración necesaria para su culminación y la generación de las condiciones necesarias para su posterior aplicación.	Reforzar el apoyo a la propuesta, ya hacer extensiva a todo el personal las orientaciones pertinentes para concientizar sobre la relevancia de la aplicación de la misma.
5.2	Política	NO	Es manifiesto por parte de la gerencia, la no existencia en la actualidad de políticas orientadas a mantener un entorno seguro relacionado con la seguridad de la información..	Reestructurar las políticas operativas internas de la institución para adaptarlas a las estrategias y mecanismos establecidos en el SGSI que se propone. Estas políticas deben ser públicas y de total conocimiento y comprensión por parte de todo el personal de la institución
5.3	Roles, Responsabilidades y Autoridades organizacionales	SI	Todo el personal tiene claro su rol y responsabilidad dentro de la institución, sin embargo no existe un manual que documente los cargos y sus responsabilidades	Debe generarse un manual de cargo, en el cual se recopile la información de cada uno y las responsabilidades exactas de cada empleado.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 9. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto a la Planificación.

Req	Planificación	Cumple	¿Qué se Tiene?	Recomendaciones aImplementar
6.1.1	Acciones para tratar los riesgos y oportunidades	SI	En la actualidad existen la disposición por parte del personal directivo de la institución para la implementación de un	N/A.

	(Generalidades)		SGSI, a lo cual, se encuentran avocados a ofrecer las herramientas y dar los pasos necesarios para su aplicación.	
6.1.2	Valoración de riesgos de la seguridad de la información	NO	En la actualidad, la institución no posee un método para medir y clasificar los riesgos de la seguridad de la información.	Seleccionar una metodología de evaluación de riesgo de entre las existentes, que se adapte a los recursos y posibilidades de la institución, esta debe ser documentada e implementada en las etapas que así lo requieran en el SGSI.
6.1.3	Tratamiento de los riesgos de la seguridad de la información	NO	No existe en la institución una matriz donde se puedan identificar los riesgos y con el cual se puedan direccionar las acciones necesarias para disminuirlos o eliminarlos.	Generar una matriz para el análisis de riesgo y asumir los correctivos pertinentes
6.2	Objetivos de la seguridad de la Información y planes para lograrlo	NO	No están documentados los objetivos de la seguridad de la información.	Definir los objetivos de la seguridad de la información y definir de qué manera se alcanzaran.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 10. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto a las Soportes.

Req	Soporte	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar
7.1	Recursos	SI	Los recursos para esta fase de diseño y planeación están asignados.	Debe planificarse la asignación de recursos para la implementación completa y definitiva del SGSI.
7.2	Competencia	SI	La institución dispone del apoyo del personal con la experiencia necesaria para el desarrollo de la presente propuesta de implementación, así mismo, está dispuesto a formar las comisiones necesarias para su implementación y mantenimiento en el tiempo.	Contratar a personas certificadas en implementar un SGSI con la norma ISO 27001:2013.
7.3	Concientización	NO	No existen campañas ni procesos de concientización de los empleados en torno a la importancia de la seguridad de la información, las acciones emprendidas por los empleados en este tema, son básicas y no están asociadas a que están conscientes de la importancias de institucionalizar las políticas de seguridad en la información.	Adiestrar a todo el personal, tanto administrativo como docente, sobre la importancia del resguardo de la información.
7.4	Comunicación	NO	Los métodos de comunicación institucionales no son empleados para difundir lineamientos ni estrategias relacionadas con el tema puntual de la seguridad de la información	Emplear los medios de comunicación institucional para la difusión de datos sobre seguridad de la información
7.5.1	Información Documentada (Generalidades)	NO	No se tiene la información documentada sobre los SGSI ni de la normativa internacional relacionada	Recabar y documentar, toda la información relacionada sobre los sistemas de gestión de la información y sobre los estándares ISO a los que estos están asociados
7.5.2	Información Documentada (Creación y Actualización)	NO	No existen documentos asociados a un SGSI que se puedan actualizar	Asumir políticas de actualización periódica de los documentos y la información asociada al sistema de gestión cuando estos sean creados e implementados
7.5.3	Información Documentada (Control de la información documentada)	NO	No existe un control de documentos del SGSI que se pueda controlar	Mantener un control de los documentos del SGSI.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 11. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto a las operaciones.

Req	Operación	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar
8.1	Planificación y	NO	No existe un control de los procesos	Establecer los procesos necesarios todos

	Control Operacional		requeridos para alcanzar los objetivos de la seguridad de la información.	los aspectos relacionados con la implementación y seguimiento de un SGSI.
8.2	Evaluación de Riesgos de Seguridad de la Información	NO	No existe una valoración de riesgos.	Establecer un esquema de clasificación de riesgos informáticos
8.3	Tratamiento de los Riegos de Seguridad de la Información	NO	No existe una planificación ni metodologías para corregir riesgos informáticos.	Documentar el tratamiento de riesgos informáticos.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 12. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto a las Evaluaciones del Desempeño.

Req	Evaluación del Desempeño	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar
9.1	Monitoreo, Medición, Análisis y Evaluación	NO	No existen procesos de seguridad de la información implementados y que puedan ser medidos o monitoreados.	Establecer los procesos de Monitoreo, Medición, Análisis y Evaluación de los procesos y controles del SGSI.
9.2	Auditoría Interna	NO	No está definido un plan de auditorías internas, así como tampoco los formatos para llevarla a cabo este proceso	Planear, implementar y mantener un plan de auditoría interna en base al estándar ISO 27001:2013.
9.3	Revisión por la Dirección	NO	No está documentado un plan de la revisión del SGSI por parte de la dirección.	Documentar y planear la ejecución periódica de procesos de revisión del SGSI.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 13. Requisitos y cumplimiento de la Norma ISO/IEC 27001:2013 con respecto a las Mejoras.

Req	Mejora	Cumple	¿Qué se Tiene?	Recomendaciones a Implementar
10.1	No Conformidades y Acciones Correctivas	NO	No está documentada la forma de cómo tratar a las no conformidades con el SGSI.	Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.
10.2	Mejora Continua	NO	No se tiene el SGSI implementado.	Proponer un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

En base a las tablas anteriores, es posible observar el estado real de cumplimiento de las disposiciones que se encuentran en la norma ISO 27001:2013, en la Tabla 14, se muestra un resumen de la ponderación de cumplimiento por ítem y de manera general.

Tabla 14. Nivel de cumplimiento de los requisitos de la Norma ISO/IEC 27001:2013

Requisito	Cumple (%)	No Cumple (%)
Contexto de la organización	75	25
Liderazgo	67	33
Planificación	25	75
Soporte	29	71
Operación	0	100
Evaluación del desempeño	0	100
Mejora	0	100
Proporción total de cumplimiento/no cumplimiento de la norma	**28**	**72**

Diseñado por el Autor.

3.3. Dominios, Objetivos de Control y Controles de Seguridad.

Siguiendo la línea de las recomendaciones para la implementación del SGSI propuesto, también se aconseja al consejo directivo de la institución realizar un Análisis Diferencial con respecto a los temas normativos abordados en al Anexo A del estándar ISO/IEC:27001:2013(2014) para verificar el cumplimiento de la respectiva normativa al momento de implementar de manera definitiva el sistema de gestión.

A continuación, se presenta el análisis diferencial del Anexo A del estándar ISO/IEC:27001:2013(2014), mismo que es realizado en la actualidad previo a la implementación de la propuesta, y que sirve de modelo para los que posteriormente requiera aplicar la institución.

Tabla 15. Análisis diferencial del Anexo A.5 de la Norma ISO/IEC 27001:2013. Políticas de la Seguridad de la Información

<table>
<tr><td>A.5</td><td colspan="3">POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="3">Dirección de la gerencia para la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.</td></tr>
<tr><td rowspan="5">A.5.1.1</td><td rowspan="5">Políticas para la seguridad de la información</td><td rowspan="5">Control: Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas asociadas al SGSI aseguran un direccionamiento estratégico acoplado a los objetivos de la Unidad Educativa, además que garantizan el cumplimiento de las leyes y regulaciones. Esta documentación es de carácter obligatorio en la norma ISO:27001:2013.</td></tr>
<tr><td>SE IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe un SGSI ni documento que normen las políticas de seguridad de la información</td></tr>
<tr><td rowspan="5">A.5.1.2</td><td rowspan="5">Revisión de las políticas para la seguridad de la información</td><td rowspan="5">Control: Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas asociadas al SGSI deberían ser evaluadas con el fin de garantizar que se asocien a los objetivos de la organización.</td></tr>
<tr><td>SE IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado</td></tr>
</table>

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 16. Análisis diferencial del Anexo A.6 de la Norma ISO/IEC 27001:2013. Organización de la seguridad de la información

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	Organización Interna		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	APLICA SI / NO Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas SE IMPLEMENTA SI / NO No se tiene implementado un SGSI.
A.6.1.2	Segregación de funciones	Control: Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	APLICA SI / NO Ningún empleado debería tener acceso a modificar los activos informáticos sin autorización previa SE IMPLEMENTA SI / NO No existe un manual de cargo donde se delimiten las funciones del personal
A.6.1.3	Contacto con autoridades	Control: Contactos apropiados con autoridades relevantes deben ser mantenidos.	APLICA SI / NO Deberían existir procedimientos para contactar a las autoridades pertinentes y reportar las incidencias relativas a la seguridad de la información SE IMPLEMENTA SI / NO Hasta el momento, las incidencias relacionadas a la seguridad de la información, son resueltas internamente
A.6.1.4	Contacto con grupos especiales de interés	Control: Contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales deben ser mantenidos.	APLICA SI / NO Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información. SE IMPLEMENTA SI / NO No se mantienen contactos con grupos de interés.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información debe ser tratada en la gestión de proyectos, sin importar el tipo de proyecto.	APLICA SI / NO Es una metodología de análisis de riesgos puede adaptarse a diversos proyectos y debería implementarse en el proceso de ejecución de un proyecto de TI. SE IMPLEMENTA SI / NO Nunca se ha implementado previo a este trabajo, un análisis de riesgo de la información
A.6.2	Dispositivos móviles y trabajo a distancia		
Objetivo: Garantizar la seguridad del trabajo a distancia y el uso de dispositivos móviles			
A.6.2.1	Políticas de dispositivos móviles	Control: Una política y medidas de seguridad de soporte deben ser adoptadas para gestionar los riesgos introducidos por el uso de dispositivos móviles.	APLICA SI / NO Los dispositivos móviles representan potencialmente un riesgo para la seguridad de la información. SE IMPLEMENTA SI / NO No existe una política de seguridad para estos dispositivos
A.6.2.2	Trabajo a distancia	Control: Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo	APLICA SI / NO El trabajo remoto debería tener una política de seguridad sobre las condiciones y restricciones SE IMPLEMENTA SI / NO En la institución no se aplica el trabajo a distancia.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 17. Análisis diferencial del Anexo A.7 de la Norma ISO/IEC 27001:2013. Seguridad de los Recursos Humanos

A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.1	**Antes de asumir el empleo**		
***Objetivo**: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.*			
A.7.1.1	Selección	***Control***: Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos..	**APLICA** **SI** / **NO** Se requiere que el personal contratado reúna las pericias técnicas adecuadas a sus funciones, además de poseer una determinada condición ética favorable a la encomienda de responsabilidades de confidencialidad SE IMPLEMENTA **SI** / **NO** No se posee conocimiento del nivel de confiabilidad de los empleados ya que este no es un factor fuerte a evaluar en los procesos de contratación
A.7.1.2	Términos y condiciones del empleo	**Control:** Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	**APLICA** **SI** / **NO** Deben existir cláusulas contractuales que condicionen las normas internas de confidencialidad de la información. SE IMPLEMENTA **SI** / **NO** Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**		
***Objetivo**: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan*			
A.7.2.1	Responsabilidades de la gerencia	***Control***: La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	**APLICA** **SI** / **NO** Debe reforzarse periódicamente las exigencias de seguridad. SE IMPLEMENTA **SI** / **NO** No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	**Control:** Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	**APLICA** **SI** / **NO** Es necesario y oportuno la formación en cuanto a resguardo de la información SE IMPLEMENTA **SI** / **NO** No se tiene implementado un SGSI ni un plan de concientización con respecto a la seguridad de la información
A.7.2.3	Proceso Disciplinario	**Control:** Debe haber un proceso disciplinario formal y comunicado para tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.	**APLICA** **SI** / **NO** Toda organización debe tener un proceso disciplinario establecido. SE IMPLEMENTA **SI** / **NO** No existe un proceso disciplinario
A.7.3	**Terminación y cambio de empleo**		
***Objetivo**: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo*			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**Control**: Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar su cumplimiento.	**APLICA** **SI** / **NO** Los acuerdos contractuales deberían plasmar el compromiso sobre la confidencialidad de la información aún después de culminada la relación contractual. SE IMPLEMENTA **SI** / **NO** No se aplican reco0rdfatorios sobre la responsabilidad de confidencialidad luego de terminada la relación laboral

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 18. Análisis diferencial del Anexo A.8 de la Norma ISO/IEC 27001:2013. Gestión de Activos.

A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	**Responsabilidad por los activos**		
***Objetivo**: Identificar los activos organizacionales y definir las responsabilidades apropiadas*			
A.8.1.1	Inventario de activos	***Control***: Información, Otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	**APLICA** **SI** / **NO** Los inventarios de activos son de carácter obligatorio en la norma ISO 27001:2013 **IMPLEMENTA** **SI** / **NO** No existe un inventario formal donde se detalle que tan crítico es alguno de los activos
A.8.1.2	Propiedad de los activos	***Control:** Los activos mantenidos en el inventario deben ser propios*	**APLICA** **SI** / **NO** Los activos deben tener asignados un deño y estos deben ser reconocidos de manera general. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** / **NO** No se especifican los propietarios de los activos informáticos inventariados
A.8.1.3	Uso aceptable de los activos	***Control***: Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	**APLICA** **SI** / **NO** Los empleados son los responsables del uso que les dan a los activos informáticos. **IMPLEMENTA** **SI** / **NO** No se especifican las reglas para el uso aceptable de los activos
A.8.1.4	Retorno de activos	***Control:** Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo*	**APLICA** **SI** / **NO** La devolución de activos debe ser formalizada y la información almacenada en dispositivos personales transferida a la organización. **IMPLEMENTA** **SI** / **NO** No se mantienen registros de la devolución de activos informáticos suministrados a los empleados.
A.8.2	**Clasificación de la Información**		
***Objetivo**: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización*			
A.8.2.1	Clasificación de la Información	***Control***: La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	**APLICA** **SI** / **NO** Esta documentación es de carácter obligatorio en la norma ISO27001:2013. **IMPLEMENTA** **SI** / **NO** Actualmente no existe un documento que clasifique información y los activos.
A.8.2.2	Etiquetado de la información	***Control:** Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.*	**APLICA** **SI** / **NO** El etiquetado de la información debe reflejar en el esquema de clasificación adoptador por la organización. **IMPLEMENTA** **SI** / **NO** Actualmente no existe algún etiquetado y/o clasificación de la información
A.8.2.3	Manejo de activos	***Control***: Los procedimientos para el manejo de activos deben ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	**APLICA** **SI** / **NO** Los accesos a los activos deberían restringirse de acuerdo a su esquema de clasificación **IMPLEMENTA** **SI** / **NO** Actualmente una clasificación de la información por lo que no se manejan procedimientos relacionados con la manipulación de esta.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 18. (cont.). Análisis diferencial del Anexo A.8 de la Norma ISO/IEC 27001:2013. Gestión de Activos.

<table>
<tr><td>A.8.3</td><td colspan="3">Manejo de medios</td></tr>
<tr><td colspan="4">Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios</td></tr>
<tr><td rowspan="6">A.8.3.1</td><td rowspan="6">Gestión de medios removibles</td><td rowspan="6">Control: Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los medios removibles podrían almacenar información confidencial y deberían tener el mismo tratamiento y esquema de clasificación que cualquier otro activo informático</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los medios removibles analizados contra virus de manera ocasional, sin embargo, no existe un protocolo de clasificación de la información que en estos se almacena</td></tr>
<tr><td rowspan="6">A.8.3.2</td><td rowspan="6">Disposición de medios</td><td rowspan="6">Control: Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los medios removibles podrían almacenar información confidencial y deberían ser respaldados y resguardados en lugares seguros.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los medios removibles no son dispuestos en lugares seguros.</td></tr>
<tr><td rowspan="6">A.8.3.3</td><td rowspan="6">Transferencia de medios físicos</td><td rowspan="6">Control: Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Los medios transportados podrían tener información sensible por lo que se debería identificar para asegurar un uso correcto de los mismos.</td></tr>
<tr><td colspan="2">IMPLEMENTA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se transportan activos informáticos fuera de la institución</td></tr>
</table>

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(conti.)*

Tabla 19. Análisis diferencial del Anexo A.9 de la Norma ISO/IEC 27001:2013. Control de Acceso.

A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos del negocio para control de acceso**			
***Objetivo**: Limitar el acceso a información y a instalaciones de procesamiento de información.*				
A.9.1.1	Política de control de acceso	***Control***: Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información	**APLICA** **SI** / **NO** El control de acceso físico y lógico permiten tener un control sobre los riesgos de diseminación de información o acceso físico a los activos por parte de personas no autorizadas **IMPLEMENTA** **SI** / **NO** Se poseen una serie de controles para el acceso a las activos pero estos no se encuentran documentados	
A.9.1.2	Acceso a redes y a servicios de red	***Control:*** Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	**APLICA** **SI** / **NO** Las redes y servicios de red deben mantener un acceso restringido al personal autorizado. **IMPLEMENTA** **SI** / **NO** La conexión es cableada y solo están conectadas las computadoras autorizadas, el wifi posee contraseñas y solo es de uso del personal directivo y administrativo gerencial.	
A.9.2	**Gestión de acceso de usuarios**			
***Objetivo**: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios*				
A.9.2.1	Registro y baja de usuarios	***Control***: Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	**APLICA** **SI** / **NO** Se mantiene un control del suministro de acceso a las redes y a determinado tipo de datos **IMPLEMENTA** **SI** / **NO** A los empleados se les asigna una clave de acceso a la red inalámbrica con cierto tiempo de duración, luego esta clave es cambiada y se mantiene un registro de estas autorizaciones, aunque no se ha documentado este proceso.	
A.9.2.2	Aprovisionamiento de acceso a usuario	***Control:*** Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios..	**APLICA** **SI** / **NO** Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso de solicitud formal. **IMPLEMENTA** **SI** / **NO** A los empleados se les asigna una clave de acceso a la red que dura determinado tiempo, el proceso no se encuentra formalmente documentado, aunque si se realiza seguimiento.	
A.9.2.3	Gestión de los derechos de acceso privilegiado	***Control***: La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	**APLICA** **SI** / **NO** Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso. **IMPLEMENTA** **SI** / **NO** A los empleados se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo.	
A.9.2.4	Gestión de información de autenticación secreta de usuarios	***Control:*** *La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal*	**APLICA** **SI** / **NO** La autenticación de los empleados en los sistemas debería mantenerse confidencial y secreta. **IMPLEMENTA** **SI** / **NO** La entrega de claves de acceso se realiza de forma personal y no se fuerza a que sea cambiada inmediatamente en su primer acceso.	
A.9.2.5	Revisión de los derechos de acceso de usuarios	***Control***: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares	**APLICA** **SI** / **NO** Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas. **IMPLEMENTA** **SI** / **NO** No se realizan verificaciones regulares de los derechos de acceso a los sistemas.	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 19. (Cont.). Análisis diferencial del Anexo A.9 de la Norma ISO/IEC 27001:2013. Control de Acceso.

A.9.2.6	Remoción o ajuste de derechos de acceso	***Control:*** Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes externas deben removerse al término de su empleo, contrato o acuerdo, o ajustarse según el cambio.	**APLICA** **SI** / **NO** La remoción de los derechos de acceso asegura que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminada la relación laboral. **IMPLEMENTA** **SI** / **NO** No existe un proceso y/o documentación formal de remoción de privilegios de acceso al terminar la relación laboral
A.9.3	**Responsabilidades de los usuarios**		
***Objetivo**: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación*			
A.9.3.1	Uso de información de autenticación secreta	***Control***: Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.	**APLICA** **SI** / **NO** La información confidencial debería ser accedida sólo por las personas autorizadas y para fines de la organización. **IMPLEMENTA** **SI** / **NO** La información de autenticación del empleado en los sistemas y acceso a información es confidencial y de carácter institucional
A.9.4	**Responsabilidades de los usuarios**		
***Objetivo**: Evitar el acceso no autorizado a sistemas y aplicaciones*			
A.9.4.1	Restricción de acceso a la información	***Control***: El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	**APLICA** **SI** / **NO** El acceso a la información debe ser restringida a extraños **IMPLEMENTA** **SI** / **NO** Los derechos de acceso a los sistemas e información son restringidos al personal de la institución.
A.9.4.2	Procedimiento de ingreso seguro	***Control:*** Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	**APLICA** **SI** / **NO** El acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro **IMPLEMENTA** **SI** / **NO** Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	***Control:*** Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	**APLICA** **SI** / **NO** Los dispositivos poseen mecanismos de asignación de contraseñas. **IMPLEMENTA** **SI** / **NO** Los sistemas de gestión de contraseñas no son interactivos ya que es otorgada de forma manual.
A.9.4.4	Uso de programas utilitarios privilegiados	***Control:*** El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.	**APLICA** **SI** / **NO** Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente **IMPLEMENTA** **SI** / **NO** Los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y con licencias válidas.
A.9.4.5	Control de acceso a códigos fuente de los programas	***Control:*** El acceso al código fuente de los programas debe ser restringido..	**APLICA** **SI** / **NO** El acceso al código fuente de los programas debe ser restringido. **IMPLEMENTA** **SI** / **NO** El código fuente sólo es accedido por las personas autorizadas y con la capacidad técnica para operarlos

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 20. Análisis diferencial del Anexo A.10 de la Norma ISO/IEC 27001:2013. Criptografía.

A.10.1	**Criptografía**		
	Controles Criptográficos		
***Objetivo**: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.*			
A.10.1.1	Política sobre el uso de controles criptográficos	***Control***: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	**APLICA** **SI** / **NO** Es necesaria la encriptación de los mensajes y de la información para garantizar una transferencia segura de los datos. **IMPLEMENTA** **SI** / **NO** No existen controles criptográficos de la transferencia de la información
A.10.1.2	Gestión de claves	***Control:*** Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	**APLICA** **SI** / **NO** La gestión de claves criptográficas asegura la seguridad, mantenimiento, renovación, distribución y destrucción de la información. **IMPLEMENTA** **SI** / **NO** No existe una política sobre el uso y distribución de claves criptográficas

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 21. Análisis diferencial del Anexo A.11 de la Norma ISO/IEC 27001:2013. Seguridad Física del entorno.

A.11	**SEGURIDAD FISICA Y DEL ENTORNO**		
A.11.1	**Áreas seguras**		
***Objetivo**: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización*			
A.11.1.1	Perímetro de seguridad física	***Control***: Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información	**APLICA** **SI** / **NO** Se deben establecer áreas de acceso restringido a personas sin las suficientes credenciales **IMPLEMENTA** **SI** / **NO** Existen áreas delimitadas como de acceso restringido
A.11.1.2	Controles de ingreso físicos	Control: Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	**APLICA** **SI** / **NO** Deben existir controles físicos de accesos a las áreas **IMPLEMENTA** **SI** / **NO** Se controla el acceso físico a las áreas
A.11.1.3	Asegurar oficinas, áreas e instalaciones	***Control:*** Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada	**APLICA** **SI** / **NO** Debe haber controles que identifiquen los movimientos dentro de las áreas restringida o que eviten el acceso de cualquier persona **IMPLEMENTA** **SI** / **NO** Las oficinas y lugares de trabajo están protegidas por cámaras de seguridad y existe personal de seguridad que controla el acceso a las mismas
A.11.1.4	Protección contra amenazas externas y ambientales	***Control:*** Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	**APLICA** **SI** / **NO** Protección física contra los desastres naturales y/o humanos. **IMPLEMENTA** **SI** / **NO** No existe una protección física contra los desastres naturales y/o humanos.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014) *(Cont.).*

Tabla 21. (Cont.). Análisis diferencial del Anexo A.11 de la Norma ISO/IEC 27001:2013. Seguridad Física del entorno

A.11.1.5	Trabajo en áreas seguras	***Control:*** Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado	**APLICA**	
			SI	**NO**
			Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente	
			IMPLEMENTA	
			SI	**NO**
			No se tienen áreas seguras para ser aseguradas físicamente.	
A.11.1.6	Áreas de despacho y carga	***Control:*** Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado..	**APLICA**	
			SI	**NO**
			Los lugares de entrega de equipos y otros dispositivos deben estar controlados y separados de las área donde se maneja información	
			IMPLEMENTA	
			SI	**NO**
			Las áreas de despacho de equipos o mercancías es en las mismas oficinas administrativas de la unidad educativa	
A.11.2	**Equipos**			
***Objetivo**: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización*				
A.11.2.1	Emplazamiento y protección de los equipos	***Control***: Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	**APLICA**	
			SI	**NO**
			Los equipos deberían estar protegidos físicamente de amenazas ambientales y humanas así como evitar el acceso no autorizado.	
			IMPLEMENTA	
			SI	**NO**
			Los equipos están protegidos físicamente contra amenazas ambientales y se restringe su uso a personas ajenas a la institución.	
A.11.2.2	Servicios de suministro	***Control:*** Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	**APLICA**	
			SI	**NO**
			Los suministros eléctricos, agua y gas no deben afectar a los equipos..	
			IMPLEMENTA	
			SI	**NO**
			Los servicios básicos son los requeridos para el	
A.11.2.3	Seguridad del cableado	***Control:*** El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	**APLICA**	
			SI	**NO**
			El cableado provee la transmisión de datos o energía a los dispositivos	
			IMPLEMENTA	
			SI	**NO**
			El cableado eléctrico está separado del cableado de datos.	
A.11.2.4	Mantenimiento de equipos	***Control:*** Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	**APLICA**	
			SI	**NO**
			Se requiere un mantenimiento periódico de los equipos.	
			IMPLEMENTA	
			SI	**NO**
			Los equipos son mantenidos sólo por el personal autorizado sin embargo los tiempos de actualización son muy largos.	
A.11.2.5	Remoción de activos	***Control*** Los equipos, la información o el *software* no deben ser retirados de su lugar sin autorización previa.	**APLICA**	
			SI	**NO**
			El retiro de los equipos, eliminación de *software* e información sólo debería ser realizada por el personal autorizado y bajo autorización de la directiva.	
			IMPLEMENTA	
			SI	**NO**
			El retiro de los equipos, eliminación de *software* e información sólo es realizada por el personal autorizado y bajo autorización.	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014) *(Cont.)*

Tabla 21. (Cont.). Análisis diferencial del Anexo A.11 de la Norma ISO/IEC 27001:2013. Seguridad Física del entorno

A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	***Control:*** La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	**APLICA**	
			SI	**NO**
			Los equipos y/o dispositivos que pertenecen a la institución solo deberían usarse en las instalaciones de la misma.	
			IMPLEMENTA	
			SI	**NO**
			Los equipos no son utilizados fuera de la Unidad Educativa	
A.11.2.7	Disposición o reutilización segura de equipos	***Control:*** Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y *software* con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización	**APLICA**	
			SI	**NO**
			Se debe garantizar que los equipos está libre de información sensible cada vez que sean reasignados	
			IMPLEMENTA	
			SI	**NO**
			Se realiza un procedimiento seguro para la disposición o reutilización de equipos	
A.11.2.8	Equipos de usuario desatendido	***Control:*** Los usuarios deben asegurarse de que los equipos desatendidos tenga la protección apropiada	**APLICA**	
			SI	**NO**
			Los usuarios deberían cerrar sesiones y proteger el equipo con contraseñas cuando no lo estén utilizando.	
			IMPLEMENTA	
			SI	**NO**
			Aunque no exista una política documentada, los usuarios emplean el uso de contraseñas de manera adecuada para el manejo de las sesiones abiertas en los equipos	
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	***Control:*** Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.	**APLICA**	
			SI	**NO**
			El almacenamiento de información confidencial no debería ser visible al público	
			IMPLEMENTA	
			SI	**NO**
			La información confidencial es almacenada adecuadamente y se mantiene fuera de la vista del personal no autorizado.	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014) *(Cont.)*

Tabla 22. Análisis diferencial del Anexo A.12 de la Norma ISO/IEC 27001:2013. Seguridad de las operaciones.

A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	**Procedimientos operacionales y responsabilidades**			
***Objetivo**: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de Información*				
A.12.1.1	Procedimientos de operativos documentados	***Control***: Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que los necesitan	**APLICA**	
			SI	**NO**
			Los procedimientos operacionales deberían estar documentados y disponibles para todos los usuarios. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013	
			IMPLEMENTA	
			SI	**NO**
			Los procedimientos operacionales no están documentados.	
A.12.1.2	Gestión de Cambios	***Control***: Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deben ser controlados.	**APLICA**	
			SI	**NO**
			Los cambios en los equipos que afectan la seguridad de la información deberían ser controlados y planificados	
			IMPLEMENTA	
			SI	**NO**
			Los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 22. (Cont.). Análisis diferencial del Anexo A.12 de la Norma ISO/IEC 27001:2013. Seguridad de las operaciones.

A.12.1.3	Gestión de Capacidad	***Control***: El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	**APLICA** **SI** / **NO** Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento. **IMPLEMENTA** **SI** / **NO** Se les realiza un monitoreo continuo a los recursos y la adquisición de nuevos se proyecta de acuerdo a las necesidades críticas de la unidad educativa
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	***Control***: Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	**APLICA** **SI** / **NO** La separación de ambientes de desarrollo y pruebas reduce el riesgo de operaciones no autorizadas **IMPLEMENTA** **SI** / **NO** No existe la necesidad de poseer áreas de desarrollo o pruebas.
A.12.2	**Protección contra códigos maliciosos**		
***Objetivo**: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos*			
A.12.2.1	Controles contra códigos maliciosos	***Control***: Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios	**APLICA** **SI** / **NO** El malware o *software* malicioso es un riesgo potencial para los sistemas y equipos. **IMPLEMENTA** **SI** / **NO** Aunque no existe una política claramente definida contra el malware, os equipos posen protección anti virus
A.12.3	**Respaldo**		
***Objetivo**: Proteger contra la pérdida de datos*			
A.12.3.1	Respaldo de la información	***Control***: Copias de respaldo de la información, del *software* y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	**APLICA** **SI** / **NO** Las copias de seguridad (backups) e imágenes de los sistemas garantizan que la información esencial e instalación de *software* podría ser recuperada después de fallas o desastres. **IMPLEMENTA** **SI** / **NO** Las copias de seguridad se realizan a intervalos programados y de forma automática
A.12.4	**Copias de respaldo**		
***Objetivo**: Registrar eventos y generar evidencia*			
A.12.4.1	Registro de eventos	***Control***: Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	**APLICA** **SI** / **NO** Los registros (logs) almacenan información relevante sobre los eventos ocurridos en la operación de un sistema **IMPLEMENTA** **SI** / **NO** No se mantienen los registros de los eventos ocurridos en los sistemas
A.12.4.2	Protección de información de registro	***Control:*** Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	**APLICA** **SI** / **NO** Los registros de eventos deberían ser custodiados para prevenir modificación no autorizada. **IMPLEMENTA** **SI** / **NO** No se generan de manera sistemática, ni se almacenan registros de eventos de los sistemas
A.12.4.3	Registros del administrado y del operador	***Control:*** Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.	**APLICA** **SI** / **NO** Los administradores tienen accesos a los sistemas, generando también registros de eventos **IMPLEMENTA** **SI** / **NO** No se generan de manera sistemática, ni se almacenan registros de eventos de los sistemas

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 22. (Cont.). Análisis diferencial del Anexo A.12 de la Norma ISO/IEC 27001:2013. Seguridad de las operaciones.

A.12.4.4	Sincronización de reloj	***Control:*** Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.	**APLICA**	
			SI	**NO**
			Los relojes de los sistemas deben mantener una referencia única de tiempo y zona horaria	
			IMPLEMENTA	
			SI	**NO**
			Aunque no existe una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.	
A.12.5	**Control de *software* operacional**			
***Objetivo**: Asegurarse de la integridad de los sistemas operacionales*				
A.12.5.1	Instalación de *software* en sistemas operacionales	***Control***: Procedimientos deben ser implementados s para controlar la instalación de *software* en sistemas operacionales.	**APLICA**	
			SI	**NO**
			Se debería controlar las instalaciones de *software* en los sistemas operativos	
			IMPLEMENTA	
			SI	**NO**
			No existe una política documentada o procedimientos sobre la instalación de *software*.	
A.12.6	**Gestión de la vulnerabilidad técnica**			
***Objetivo**: Prevenir el aprovechamiento de las vulnerabilidades técnicas.*				
A.12.6.1	Gestión de las vulnerabilidades técnicas	***Control***: Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado	**APLICA**	
			SI	**NO**
			El inventario de los activos se debería mantener actualizado.	
			IMPLEMENTA	
			SI	**NO**
			Aunque existe un inventario de los activos físicos y del *software* operacional, no se tiene una metodología de evaluación de riesgos	
A.12.6.2	Restricciones sobre la instalación de *software*	***Control:*** Reglas que gobiernen la instalación de *software* por parte de los usuarios deben ser establecidas e implementadas.	**APLICA**	
			SI	**NO**
			Cualquier persona con elevados privilegios de acceso podría instalar cualquier *software* en un equipo y/o dispositivo.	
			IMPLEMENTA	
			SI	**NO**
			La instalación de *software* es realizada sólo por el personal autorizado y con *software* probado y licenciado,	
A.12.7	**Consideraciones sobre auditorías de sistemas de información**			
***Objetivo**: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos*				
A.12.7.1	Controles de auditorías de sistemas de información	***Control***: Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	**APLICA**	
			SI	**NO**
			Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos	
			IMPLEMENTA	
			SI	**NO**
			No se tiene un plan de auditoría para la verificación de los sistemas operativos	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 23. Análisis diferencial del Anexo A.13 de la Norma ISO/IEC 27001:2013. Seguridad de las comunicaciones.

A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	**Gestión de seguridad de la red Objetivo: Asegurar la protección de la**		
***Objetivo**: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.*			
A.13.1.1	Controles de redes	***Control***: Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	**APLICA** **SI** / **NO** Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de clave Pública (PKI) implementada
A.13.1.2	Seguridad de los servicios de red	***Control:*** Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	**APLICA** **SI** / **NO** El acceso a la red de los proveedores de servicios de red debería ser controlado y monitoreado **IMPLEMENTA** **SI** / **NO** Se monitorea el acceso a la red
A.13.1.3	Segregación de redes	***Control:*** Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	**APLICA** **SI** / **NO** Los usuarios y servicios deberían estar separados lógicamente en unidades organizacionales o dominios. **IMPLEMENTA** **SI** / **NO** Los usuarios y servicios están separados a través de dominios
A.13.2	**Transferencia de información**		
***Objetivo**: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa*			
A.13.2.1	Políticas y procedimientos de transferencia de información	***Control***: Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	**APLICA** **SI** / **NO** Los procedimientos y controles ayudan a mantener la seguridad de la información cuando es transferida. **IMPLEMENTA** **SI** / **NO** No existe un documento que establezca los procedimientos y controles a implementar para la transferencia de información.
A.13.2.2	Acuerdos sobre la transferencia de información	***Control:*** Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	**APLICA** **SI** / **NO** Se deberían tener acuerdos sobre procedimientos para transferencia de información **IMPLEMENTA** **SI** / **NO** No se han implementado controles que garanticen la seguridad en la transmisión de información
A.13.2.3	Mensajería electrónica	***Control:*** La información involucrada en mensajería electrónica debe ser protegida apropiadamente	**APLICA** **SI** / **NO** Se deberían proteger los mensajes enviados internamente de los empleados de la institución **IMPLEMENTA** **SI** / **NO** No se realizan protección de los mensajes enviados
A.13.2.4	Acuerdos de confidencialidad o no divulgación	***Control:*** Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.	**APLICA** **SI** / **NO** deberían tener acuerdos de confidencialidad de la información **IMPLEMENTA** **SI** / **NO** En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 24. Análisis diferencial del Anexo A.14 de la Norma ISO/IEC 27001:2013. Adquisición, desarrollo y mantenimiento de sistemas.

A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
***Objetivo**: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas*			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	***Control***: Requisitos relacionados a la seguridad de la información deben ser incluidos dentro de los requisitos para nuevos sistemas de información o mejoras a los sistemas de información existentes	**APLICA** **SI** / **NO** Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de información
A.14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	***Control:*** La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debe ser protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.	**APLICA** **SI** / **NO** La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de clave Pública (PKI) implementada .
A.14.1.3	Protección de transacciones de los servicios de aplicaciones	***Control:*** La información involucrada en las transacciones de servicios de aplicación debe ser protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.	**APLICA** **SI** / **NO** La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de clave Pública (PKI) implementada
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
***Objetivo**: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información*			
A.14.2.1	Política de desarrollo seguro	***Control***: Reglas para el desarrollo de *software* y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.	**APLICA** **SI** / **NO** Las políticas y controles de seguridad deberían ser aplicados en el desarrollo de *software* **IMPLEMENTA** **SI** / **NO** No se desarrolla *software*
A.14.2.2	Procedimientos de control de cambio del sistema	***Control:*** Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	**APLICA** **SI** / **NO** El procedimiento formal de los cambios en el desarrollo de *software* debería ser documentado. **IMPLEMENTA** **SI** / **NO** No se desarrolla *software*
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	***Control:*** Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	**APLICA** **SI** / **NO** Los cambios en las aplicaciones deberían ser revisados y probados antes de implementarlas **IMPLEMENTA** **SI** / **NO** Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse
A.14.2.4	Restricciones sobre cambios a los paquetes de *software*	***Control:*** Modificaciones a los paquetes de *software* deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	**APLICA** **SI** / **NO** Limitar las modificaciones de *software* sólo a lo estrictamente necesario **IMPLEMENTA** **SI** / **NO** No se desarrolla *softwares*

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont.)*

Tabla 24. (Cont.). Análisis diferencial del Anexo A.14 de la Norma ISO/IEC 27001:2013. Adquisición, desarrollo y mantenimiento de sistemas.

A.14.2.5	Principios de ingeniería de sistemas seguros	***Control:*** Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información	**APLICA**	
			SI	**NO**
			Se deberían establecer y documentar los principios de desarrollo de *software* seguro	
			IMPLEMENTA	
			SI	**NO**
			No se desarrolla *software*	
A.14.2.6	Ambiente de desarrollo seguro	***Control*** Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.	**APLICA**	
			SI	**NO**
			Los ambientes de desarrollo de *software* deberían estar protegidos de acceso no autorizado o de ejecución de *software* malicioso	
			IMPLEMENTA	
			SI	**NO**
			No se desarrolla *software*	
A.14.2.7	Desarrollo contratado externamente	**Control**: La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	**APLICA**	
			SI	**NO**
			El *software* desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros.	
			IMPLEMENTA	
			SI	**NO**
			Se asegura la adquisición de *software* externo validado adecuadamente	
A.14.2.8	Pruebas de seguridad de sistemas	**Control**: Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	**APLICA**	
			SI	**NO**
			Se deberían realizar pruebas de seguridad al *software* que se está desarrollando	
			IMPLEMENTA	
			SI	**NO**
			No se desarrolla *software*	
A.14.2.9	Pruebas de aceptación de sistemas	**Control**: Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.	**APLICA**	
			SI	**NO**
			Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización	
			IMPLEMENTA	
			SI	**NO**
			No existen lineamientos o políticas de la seguridad de la información	
A.14.3	**Datos de prueba**			
***Objetivo**: Asegurar la protección de los datos usados para pruebas*				
A.14.3.1	Protección de datos de prueba	***Control***: Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	**APLICA**	
			SI	**NO**
			Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial	
			IMPLEMENTA	
			SI	**NO**
			Cuando se aplica, los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014). *(Cont)*

Tabla 25. Análisis diferencial del Anexo A.15 de la Norma ISO/IEC 27001:2013. Relaciones con los proveedores.

A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		
***Objetivo**: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores*			
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	***Control***: Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	**APLICA** **SI** / **NO** Se deben emplear controles y procedimientos de seguridad para el acceso a los activos por parte de los proveedores. **IMPLEMENTA** **SI** / **NO** No se tiene una política de seguridad definida.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	***Control:*** Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	**APLICA** **SI** / **NO** Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos. **IMPLEMENTA** **SI** / **NO** Este proceso no se realiza
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	***Control:*** Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	**APLICA** **SI** / **NO** Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información. **IMPLEMENTA** **SI** / **NO** No existe una clasificación de seguridad de la información, ni políticas y procedimientos relacionados
A.15.2	**Gestión de la prestación de servicios de proveedores**		
***Objetivo**: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores*			
A.15.2.1	Monitoreo y revisión de servicios de los proveedores	***Control***: Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores	**APLICA** **SI** / **NO** El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos
A.15.2.2	Gestión de cambios en los servicios de los proveedores	***Control:*** Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	**APLICA** **SI** / **NO** Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 26. Análisis diferencial del Anexo A.16 de la Norma ISO/IEC 27001:2013. Gestión de Incidentes de Seguridad de la Información

A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
***Objetivo**: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.*			
A.16.1.1	Responsabilidades y procedimientos	***Control***: Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	**APLICA** **SI** / **NO** Los planes y procedimientos para gestionar los incidentes relacionados a la seguridad de la información deben estar documentados **IMPLEMENTA** **SI** / **NO** No existen procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información
A.16.1.2	Reporte de eventos de seguridad de la información	***Control:*** Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible	**APLICA** **SI** / **NO** Todos los empleados deben estar pendientes de los eventos y reportar las incidencias de seguridad de la información **IMPLEMENTA** **SI** / **NO** Los empleados alertan de los eventos e incidentes relacionados a la seguridad de la información.
A.16.1.3	Reporte de debilidades de seguridad de la información	***Control:*** Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	**APLICA** **SI** / **NO** Se deben implementar mecanismos de reportes de incidentes de seguridad de la información. **IMPLEMENTA** **SI** / **NO** Aunque los empleados reportan los incidentes este proceso no se encuentra documentado
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	***Control:*** Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información	**APLICA** **SI** / **NO** La clasificación y priorización de los incidentes de seguridad ayudan a identificar el impacto en la organización **IMPLEMENTA** **SI** / **NO** Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos
A.16.1.5	Respuesta a incidentes de seguridad de la información	***Control:*** Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados	**APLICA** **SI** / **NO** Deben existir procedimientos documentados para dar respuesta a los incidentes de seguridad aceptable lo más pronto posible **IMPLEMENTA** **SI** / **NO** Aunque los empleados reportan los incidentes este proceso no se encuentra documentado
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	***Control:*** El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros	**APLICA** **SI** / **NO** Se debería recolectar información delos incidentes ocurridos con el fin de prevenirlos en el futuro **IMPLEMENTA** **SI** / **NO** No se recolecta la información de los incidentes y se aplican los controles necesarios para prevenirlos
A.16.1.7	Recolección de evidencia	**Control**: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**APLICA** **SI** / **NO** Se deberían recolectar las evidencias y registros para tomar acciones legales **IMPLEMENTA** **SI** / **NO** Las evidencias son recolectadas formalmente para emprender las acciones legales.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 27. Análisis diferencial del Anexo A.17 de la Norma ISO/IEC 27001:2013. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**			
A.17.1	**Continuidad de seguridad de la información**			
***Objetivo**: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización*				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	***Control***: La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	**APLICA**	
			SI	**NO**
			Los BCP y los DRP deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.	
			IMPLEMENTA	
			SI	**NO**
			No existe la documentación o los procedimientos para los BCP y DRP	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	***Control:*** La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	**APLICA**	
			SI	**NO**
			Los Planes de Continuidad del Negocio (BCP) y los Planes de Recuperación de Desastres (DRP) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.	
			IMPLEMENTA	
			SI	**NO**
			No existe la documentación o los procedimientos para los BCP y DRP	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	***Control:*** La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	**APLICA**	
			SI	**NO**
			Los procedimientos y controles para la restablecer los servicios se deben revisar periódicamente.	
			IMPLEMENTA	
			SI	**NO**
			No existe la documentación o los procedimientos para los BCP y DRP	
A.17.2	**Redundancias**			
***Objetivo**: Asegurar la disponibilidad de instalaciones de procesamiento de información.*				
A.17.2.1	Instalaciones de procesamiento de la información	***Control***: Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	**APLICA**	
			SI	**NO**
			La información debería ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares	
			IMPLEMENTA	
			SI	**NO**
			La organización no dispone de redundancia de la información	

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

Tabla 28. Análisis diferencial del Anexo A.17 de la Norma ISO/IEC 27001:2013. Cumplimiento.

A.18	**CUMPLIMIENTO**		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		
***Objetivo**: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.*			
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	***Control***: Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	**APLICA** **SI** / **NO** Los administradores deberían identificar toda la información legislativa aplicable a la Institución. **IMPLEMENTA** **SI** / **NO** Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley
A.18.1.2	Derechos de propiedad intelectual	***Control:*** Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de *software* propietario.	**APLICA** **SI** / **NO** Se deben definir las políticas y procedimientos para controlar la propiedad intelectual. **IMPLEMENTA** **SI** / **NO** No se desarrolla y/o patenta *software*
A.18.1.3	Protección de registros	***Control:*** Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	**APLICA** **SI** / **NO** Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización y nivel de confidencialidad **IMPLEMENTA** **SI** / **NO** No existe un nivel de clasificación formal de confidencialidad de los registros.
A.18.1.4	Privacidad y protección de información de datos personales	***Control:*** La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	**APLICA** **SI** / **NO** Se debería documentar y definir políticas relativas a la protección de datos personales de acuerdo a las reglamentaciones que la ley exige. **IMPLEMENTA** **SI** / **NO** Existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley
A.18.1.5	Regulación de controles criptográficos	***Control:*** Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes	**APLICA** **SI** / **NO** Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de clave Pública (PKI).
A.18.2	**Revisiones de seguridad de la Información**		
***Objetivo**: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos..*			
A.18.2.1	Revisión independiente de la seguridad de la información	***Control***: El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	**APLICA** **SI** / **NO** Se deberían realizar auditorías de los procesos, procedimientos y sistemas por medio de entidades externas. **IMPLEMENTA** **SI** / **NO** No se realizan estas auditorías.
A.18.2.2	Cumplimiento de políticas y normas de seguridad	***Control:*** Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	**APLICA** **SI** / **NO** Se deberían realizar revisiones de las políticas de seguridad con el fin de verificar su cumplimiento. **IMPLEMENTA** **SI** / **NO** No existen políticas de la seguridad de la información
A.18.2.3	Revisión del cumplimiento técnico	***Control:*** Los sistemas de información deben ser revisados regularmente respecto a cumplimiento de las políticas y normas de seguridad de la información de la organización.	**APLICA** **SI** / **NO** Se debe realizar un control de los dispositivos periódicamente para asegurar que cumplen con las políticas institucionales **IMPLEMENTA** **SI** / **NO** No hay políticas de seguridad o metodología de riesgo que permita comparar los resultados.

Diseñado por el Autor. Referencia: ISO 27001:2013 (2014).

En las tablas anteriores se observa el nivel de cumplimiento de la Unidad Educativa Nuestra Señora de Fátima, a los requerimientos de la Norma ISO 27001:2013. Con lo cual, es posible emitir un resumen global de cumplimiento de la misma:

Tabla 29. Nivel de Cumplimiento de los Controles de la Norma ISO/IEC 27001:2013.

Dominio de Control	Cumple (%)	No Cumple (%)
A5. Políticas de la Seguridad de la Información	0	**100**
A6. Organización de la Seguridad de la Información	0	**100**
A7. Seguridad de los Recursos Humanos	16,7	**83,3**
A8. Gestión de Activos	0	**100**
A9. Control de Acceso	64,2	**35,8**
A10. Criptografía	0	**100**
A11. Seguridad Física y del Entorno	66,6	**33,4**
A12. Seguridad de las Operaciones	42,9	**57,1**
A13. Seguridad de las Comunicaciones	42,8	**57,2**
A14. Adquisición, Desarrollo y Mantenimiento de Sistemas	23,1	**76,9**
A15. Relaciones con los Proveedores	0	**100**
A16. Gestión de Incidentes de Seguridad de la Información	14,3	**85,7**
A17. Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio	0	**100**
A18. Cumplimiento	25	**75**
Total Cumplimiento/No Cumplimiento	**21,1**	**78,9**

Elaborado por el Autor.

Tras la anterior evaluación, se puede apreciar que la Unidad Educativa Nuestra Señora del Fátima, se encuentra con un gran déficit en el nivel de adaptación de procesos, dominios, objetivos de control y controles de seguridad que se requieren en el estándar ISO/IEC 27001:2013.

Como se observa, no existe una documentación del estándar dentro de la institución, es decir, muchas de estas faltas, se deben a desconocimiento de la norma, y por tanto de la necesidad de su aplicación, en muchos casos los requerimientos que faltan están asociados con el desarrollo de la documentación pertinente al punto que corresponda la evaluación. Esta situación puede ser subsanada al asumir la implementación formal de la normativa estándar ISO/IEC 27001:2013.

3.4. Políticas de Seguridad de la Información.

3.4.1. Propósito, Alcance y Usuarios

En base a los resultados preliminares y a la intención expedita de la directiva de Institucion de aplicar un SGSI, se establezca un compromiso formal para proteger los activos de la información que maneja, y se generen a partir de estos, las bases para asegurar los elementos de Confidencialidad, Integridad y Disponibilidad de la información, que maneja, además, de garantizar el cumplimiento de los preceptos de control establecidos en la normativa ISO/IEC 27001:2013.

3.4.2. Estrategia de Seguridad de la Información

Los lineamientos por los cuales se establecerá el control de los activos de la información dentro de la institución educativa, se sustentan en la aplicación y control de estrategias definidas en la propuesta de la norma ISO/IEC 27001:2013, el cual, principalmente incluyen la implementación de la documentación adecuada para normar los respectivos procesos, a su vez, garantizando un adecuado control de los mismos tras su aplicación con el fin de seguir detectando carencias en los mecanismos de resguardo que puedan ser posteriormente resueltos.

3.4.3. Objetivos de las Políticas de Seguridad

Los objetivos a seguir con la propuesta de un plan de gestión de la seguridad de la información en la Unidad Educativa Nuestra Señora De Fátima son los siguientes:

- Asegurar mejoras en los mecanismos de protección de la Confidencialidad, Integridad y Disponibilidad de la información de los estudiantes, docentes, personal administrativo y obrero que hacen vida dentro de la institución, así como también, de la información que puedan recabar en el transcurso de sus actividades sobre los representantes de los alumnos y las de otros proveedores.
- Tras la implementación de un SGSI, lograr garantizar el normal funcionamiento de la institución tras un eventual incidente de seguridad informática.
- Generar conciencia colectiva al respecto del tema de la seguridad de la información, entre todas las personas que se relacionan directamente con la institución, esto, como

mecanismo adicional de aseguramiento de las garantías de resguardo y control de los activos de la información.

3.4.4. Definiciones

Para alcanzar el mayor entendimiento posible entre las personas que de alguna manera se involucran con la implementación, seguimiento y evaluación del SGSI se emplean los términos y definiciones contemplados en la norma ISO/IEC 2700 (ISO, 2018):

Tabla 30. Tabla de definiciones

Numeral	Concepto	Definición
A	Acción correctiva	(Inglés: *Corrective action*). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.
	Acción preventiva	(Inglés: *Preventive action*). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades
	Aceptación del riesgo	(Inglés: *Risk acceptance*). Decisión informada de asumir un riesgo concreto.
	Activo	(Inglés: *Asset*). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
	Alcance	(Inglés: *Scope*). Ámbito de la organización que queda sometido al SGSI.
	Amenaza	(Inglés: *Threat*). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
	Análisis de riesgos	(Inglés: *Risk analysis*). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
	Análisis de riesgos cualitativo	(Inglés: *Qualitative risk analysis*). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
	Análisis de riesgos cuantitativo	(Inglés: *Quantitative risk analysis*). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
	Auditor	(Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
	Auditor de primera parte	(Inglés: *First party auditor*). Auditor interno que audita la organización en nombre de ella misma.
	Auditor de segunda parte	(Inglés: *Second party auditor*). Auditor que audita una organización en nombre de otra. Por ejemplo, cuando una empresa audita a su proveedor de outsourcing, o cuando una administración pública ordena una auditoriía de una empresa.
	Auditor de tercera parte	(Inglés: *Third party auditor*). Auditor que audita una organización en nombre de una tercera parte independiente que emite un certificado de cumplimiento.
	Auditor jefe	(Inglés: *Lead auditor*). Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría acordado.
	Auditoría	(Inglés: *Audit*). Proceso sistemático, independiente y documentado para obtener evidencias de auditoriía y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
	Autenticación	(Inglés: *Authentication*). Provisión de una garantía de que una característica afirmada por una entidad es correcta.
	Autenticidad	(Inglés: *Authenticity*). Propiedad de que una entidad es lo que afirma ser.

Fuente: (iso27000.es, s.f), ISO (2018). Diagramado por el Autor. (Cont.).

Tabla 30. Definiciones (Cont.).

C	**CID**	**(Inglés: *CIA*). Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.**
	CISA	*Certified Information Systems Auditor*. Es una acreditación ofrecida por ISACA.
	Checklist	Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.
	CobiT	Control *Objectives for Information and related Technology*. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.
	Compromiso de la Dirección	(Inglés*: Management commitment*). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
	Confidencialidad	(Inglés: *Confidentiality*). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados
	Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
	Control correctivo	(Inglés: *Corrective control*). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
	Control detectivo	(Inglés: *Detective control*). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
	Control disuasorio	(Inglés: *Deterrent control*). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
	Control preventivo	(Inglés: *Preventive control*). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse
	Corrección	(Inglés: *Correction*). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
D	Declaración de aplicabilidad	(Inglés*: Statement of Applicability*; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
	Desastre	(Inglés: *Disaster*). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa
	Directiva o directriz	(Inglés: *Guideline*). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
	Disponibilidad	(Inglés: *Availability*). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
E	Entidad de acreditación	(Inglés: *Accreditation body*). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país.
	Entidad de certificación	(Inglés: *Certification body*). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.
	Entidad de normalización	(Inglés: *Standards body*). Un organismo oficial que genera y publica normas.
	Estimación de riesgos	(Inglés*: Risk evaluation*). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
	Evaluación de riesgos	(Inglés: *Risk assessment*). Proceso global de identificación, análisis y estimación de riesgos.
	Evidencia objetiva	(Inglés: *Objective evidence*). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Fuente: (iso27000.es, s.f), ISO (2018). Diagramado por el Autor. (Cont.).

Tabla 30. Definiciones (Cont.).

F	**Fase 1 de auditoría**	**(Inglés: *Stage 1 Audit*). Etapa de la auditoría de primera certificación en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.**
	Fase 2 de auditoría	(Inglés: *Stage 2 Audit*). Etapa de la auditoría de primera certificación en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo eficaz.
G	Gestión de claves	(Inglés: *Key management*). Controles referidos a la gestión de claves criptográficas.
	Gestión de incidentes de seguridad de la información	(Inglés: *Information security incident management*). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
	Gestión de riesgos	(Inglés: *Risk management*). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
H	Humphreys, Ted	Experto en seguridad de la información y gestión del riesgo, considerado "padre" de las normas BS 7799 e ISO 17799 y, por tanto, de ISO 27001 e ISO 27002
I	Identificación de riesgos	(Inglés: *Risk identification*). Proceso de encontrar, reconocer y describir riesgos.
	Impacto	(Inglés: *Impact*). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.
	Incidente de seguridad de la información	(Inglés: *Information security incident*). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
	Integridad	(Inglés: *Integrity*). Propiedad de la información relativa a su exactitud y completitud.
	Inventario de activos	(Inglés: *Assets inventory*). Lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
	ISO	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
	ISO/IEC 27001	Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
	ISO/IEC 27002	Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.
	ITIL	IT *Infrastructure Library*. Un marco de gestión de los servicios de tecnologías de la información.
N	No conformidad	(Inglés: *Nonconformity*). Incumplimiento de un requisito.
	No repudio	Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
O	Objetivo	(Inglés: *Objetive*). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Fuente: (iso27000.es, s.f), ISO (2018). Diagramado por el Autor. (Cont.).

Tabla 30. Definiciones (Cont.).

	Parte interesada	**(Inglés: *Interested party / Stakeholder*). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.**
P	PDCA	*Plan-Do-Check-Act*. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.
	Plan de continuidad del negocio	(Inglés: *Bussines Continuity Plan*). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
	Plan de tratamiento de riesgos	(Inglés: *Risk treatment plan*). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
	Política de escritorio despejado	(Inglés: *Clear desk policy*). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.
	Proceso	(Inglés: *Process*). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
	Propietario del riesgo	(Inglés: *Risk owner*). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
R	Recursos de tratamiento de información	(Inglés: *Information processing facilities*). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
	Riesgo	(Inglés: *Risk*). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
	Riesgo residual	(Inglés: *Residual risk*). El riesgo que permanece tras el tratamiento del riesgo.
S	Segregación de tareas	(Inglés: *Segregation of duties*). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
	Seguridad de la información	(Inglés: *Information security*). Preservación de la confidencialidad, integridad y disponibilidad de la información.
	Selección de controles	(Inglés: *Control selection*). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
	SGSI	(Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.
	Sistema de Gestión de la Seguridad de la Información	(Inglés: *Information Security Management System*). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
T	Tratamiento de riesgos	(Inglés: *Risk treatment*). Proceso de modificar el riesgo, mediante la implementación de controles.
	Trazabilidad	(Inglés: *Accountability*). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
V	Vulnerabilidad	(Inglés: *Vulnerability*). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Fuente: (iso27000.es, s.f), ISO (2018). Diagramado por el Autor. (Cont.).

3.4.5. Políticas de Seguridad de los Activos de la Información

En el marco de la implementación de la presente propuesta, se sugiere asumir los siguientes preceptos e indicaciones, dentro del contexto de la aplicación de la Normativa ISO/IEC 27001:2013 dentro de la Unidad Educativa Nuestra Señora de Fátima:

Tabla 31. Delimitación de las políticas propuestas para la seguridad de los activos de la información.

Política	Indicación
Política de seguridad general	Todo el personal directivo, administrativo, obrero y docente, además de alumnado y los representantes de estos, se comprometerán a mantener los activos informativos relacionados con cada una de las partes mencionadas y de la institución en general, lo más resguardados posibles. Con esto, queda expresa la total prohibición de la reproducción total o parcial de la información que pudiera considerar la institución como de índole confidencial. Esto solo podrá ocurrir, con la debida autorización o consentimiento del ente competente. También queda prohibido el maltrato y/o destrucción bajo cualquier motivo, de los dispositivos (Activos informáticos) con los que cuenta la institución.
Política de la seguridad de la información general	Se aplicarán procesos y directrices de seguridad que obliguen a mantener la información de estudiantes, docentes y administrativos en un entorno seguro. Dichas directrices se orientan en el objetivo de asegurar el cumplimiento de los principios de la Seguridad Informática como lo son la Confidencialidad, Integridad y Disponibilidad, además de los Planes de Continuidad del Negocio y Recuperación de Desastres
Política de la gestión del riesgo	Se Aplicaran controles y métodos de manejo de riesgos para conservar el normal funcionamiento de los procesos
Política de la protección de datos	Se aplicaran controles según el tipo de usuario de la información
Política de auditoría	Se implementaran auditorías programadas en cada una de las áreas y procesos críticos de la institución
Política de calidad	La dirección de la Unidad Educativa Nuestra Señora de Fátima, se comprometerá a ejecutar controles y cambios en beneficio de mejorar continuamente sus procesos. Estas políticas deben estar acompañadas de controles periódicos con los cuales se monitoree el nivel de calidad de cada proceso crítico. En este sentido, la meta fundamental de esta política es alcanzar una certificación ISO/IEC 27001:2013 y mantenerla actualizada en el tiempo.
Política de los dispositivos traídos por el usuario	Todo el personal administrativo y docente, que desee usar sus dispositivos propios para la ejecución de las actividades relacionadas con sus funciones, deben contar con la autorización previa de la dirección para hacer esto. En tal sentido, el equipo (Principalmente computadores personales) deberá ser configurado para que el equipo posea las mismas condiciones de configuración de acceso a la red que los equipos de la institución, para que no se propaguen dentro de la red *software*s maliciosos que comprometan la integridad de la información. Entre las acciones a tomar, se incluye la exhaustiva revisión de los mismos con los servicios de antivirus actualizados con los que cuenta la institución
Política de la instalación de *software* y *hardware*	La instalación de *software* y *hardware*, serán exclusivamente realizado por el personal técnico capacitado que designe la institución para tal fin. Cada unidad computacional, debe poseer un inventario de *hardware* y *software* instalados. Se realizará un chequeo de este en cada oportunidad que se haga revisión de los equipos para determinar que elemento ha sido instalado sin consentimiento de la directiva, y el cual servirá de soporte para las reparaciones y sanciones pertinentes que tengan lugar.
Política de la comunicación institucional	La información y comunicación institucional será única y exclusivamente informada por medio de los correos electrónicos institucionales. Se debe escanear con un programa antivirus actualizado, todos los documentos subidos o bajados de la plataforma de correo electrónico.
Responsabilidad	Cada individuo que forma parte de la comunidad de la Unidad Educativa Nuestra Señora de Fátima, en cualquiera de sus niveles de responsabilidad con la información, deberá garantizar la seguridad de los activos informáticos que están a su disposición, así mismo, se comprometerá a acatar los lineamientos que para tal fin, y en el marco de la implementación del SGSI se implementen. El no cumplimiento de este requerimiento, autoriza expresamente a la dirección de la unidad educativa a que tome las medidas correctivas o sancionatorias más pertinentes.
Procedimientos en incidentes de seguridad	Si se detecta alguna violación de las disposiciones emanadas para el control de la información establecidas en este documento, deberá generarse un reporte donde se detalle el incidente, posibles causas y fallas que podrían haberlo generado, además de las recomendaciones y/o controles para mitigarlo.

Diseñado por el Autor.

3.5. Métodos de análisis y evaluación y reporte de riesgos.

3.5.1. Propósito, Alcance y Usuarios.

El propósito de esta declaración, es verificar los métodos que se emplearan en el análisis y la evaluación de los riesgos a los que pudieran estar expuestos los activos de la información pertenecientes a la Unidad Educativa Nuestra Señora de Fátima.

El análisis de los riesgos, se sustentará en las mediciones de impacto solicitadas en la norma ISO/IEC 2001:2013. Y se pretende que involucre todos los aspectos de la implementación y monitoreo del SGSI, así como, a todos los activos de la institución (incluyendo a el personal relacionado con la Unidad Educativa).

3.5.2. Metodología de Análisis Evaluación de Riegos y Reporte de Evaluación de Riesgos.

Se propone la aplicación de la metodología MAGERIT (*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)* creado por el CSAE (*Consejo Superior de Administración Electrónica*) (2012a), la cual se fundamenta en la obtención de beneficios por el empleo de TI por medio de la gestión de los riesgos implícitos en el empleo de dichas tecnologías.

Con esto se pretenderá aportar herramientas adecuadas y suficientes para la protección de los activos informáticos, con los cuales, se facilite el alcance de los objetivos institucionales de quien la aplique.

Esta es una metodología de gestión de riesgos basada en la generación de elementos para la toma oportuna de decisiones que posee los siguientes objetivos:

Tabla 32. Objetivos del método MAGERIT de Control De Riesgos

Tipo	Objetivo
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

Fuente: CSAE (2012a, pág. 8). Diagramado por el Autor.

Esta metodología, contempla la implementación de dos tareas principales, el análisis de los riesgos y el tratamiento de estos. El Análisis de los Riesgos, intenta calificar los riesgos al cuantificar sus consecuencias o al determinar su importancia relativa. A su vez, el Tratamiento de Riesgos abarca la definición de las acciones requeridas para subsanar los riesgos detectados.

3.5.2.1.Paso 1: Activos

3.5.2.1.1. Inventario de Activos

El primer proceso a aplicarse en esta metodología, particularmente en la primera etapa, correspondiente al análisis de los riesgos, es el de "*determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación*" (2012a, pág. 22).

3.5.2.1.2. Valoración de activos

El método MAGERIT indica que existen dos clases de valoraciones: La Cualitativa y la Cuantitativa. La primera, permite calcular el valor de un activo en base al impacto que pueda tener en la organización, mientras que la cuantitativa, estima el costo del activo.

3.5.2.2. Paso 2: Amenazas

3.5.2.2.1. Identificación de amenazas

Las amenazas son eventos que ocurren y que potencialmente pueden causar daño a los activos de la institución (CSAE, 2012a, pág. 27). La metodología MAGERIT posee un catálogo de amenazas posibles sobre los activos de un sistema de información (CSAE, 2012b), en el cual, se clasifican las amenazas de la forma que se presenta en la tabla siguiente:

Tabla 33. Categorización de las Amenazas según la metodología MAGERIT

Tipo de Amenaza	Nomenclatura	Definición
Desastres Naturales	[N]	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	[I]	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Esta amenaza puede darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	[E]	Fallos no intencionales causados por las personas.
Ataques Intencionados	[A]	Fallos deliberados causados por las personas.

Fuente: CSAE*:* (2012b). Diagramado por el Autor.

3.5.2.2.2. Valoración de amenazas:

Según el método MAGERIT, para lograr obtener una valoración adecuada de las amenazas, se requiere determinar la frecuencia de ocurrencia de los eventos (CSAE, 2012a, pág. 28), para esto, establecen una escala con su respectiva valoración (Tabla 34).

Tabla 34. Escala de valoración de frecuencia de la ocurrencia de amenazas según el método MAGERIT de estimación y caracterización de riesgos.

Probabilidad o Frecuencia	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: CSAE: (2012a, pág. 28). Diagramado por el Autor.

Seguidamente, se aplica la evaluación del Riesgo potencial de la amenaza, esta se corresponde con el nivel probable de daño sobre un sistema. Esta valoración, se corresponde con el cálculo siguiente: ***Riesgo = Probabilidad x Impacto.*** En esta valoración, se estima que el riesgo aumenta con el impacto y con la probabilidad alta de que este ocurra (Ilustración 5).

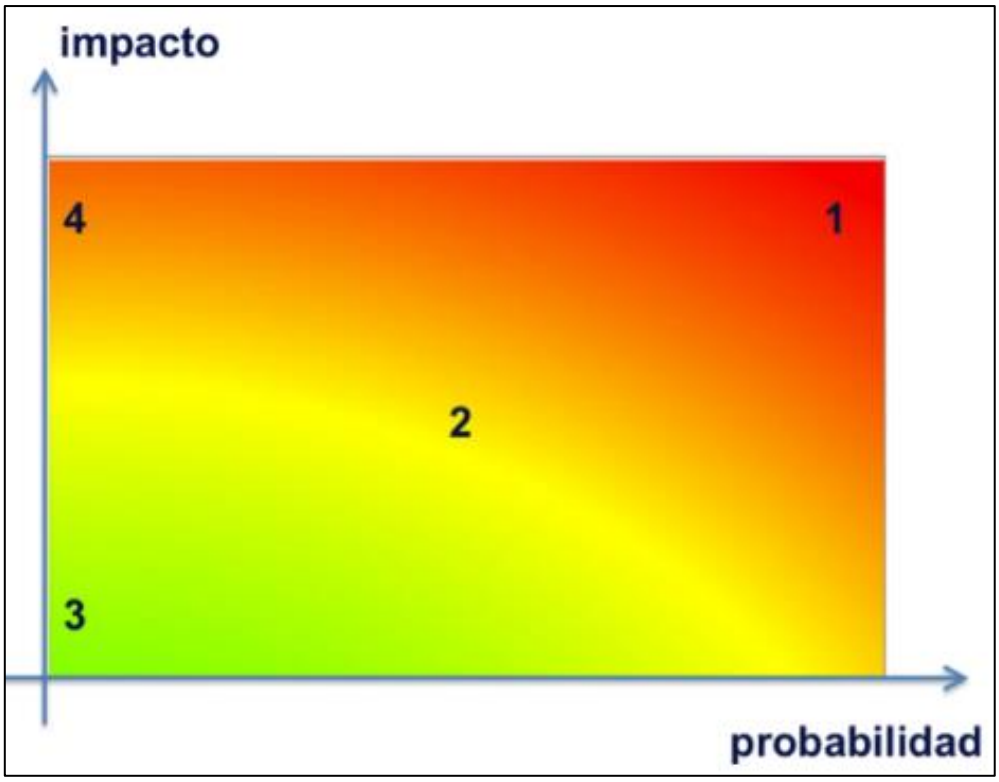


Ilustración 5. Riesgo en función del impacto y la probabilidad según el método MAGERIT. Fuente: CSAE: (2012a, pág. 28).

En el método MAGERIT, las cuatro zonas principales en el gráfico de valoración de riesgo se corresponden a la clasificación siguiente (2012a, pág. 28):

- **Zona 1**: Riesgos muy probables y de muy alto impacto (**MA: Críticos**)
- **Zona 2**: Riesgos que varían desde situaciones improbables y con impacto medio hasta situaciones muy probables, pero de impacto bajo o muy bajo (**M: Apreciables**)
- **Zona 3**: Riesgos improbables y de bajo impacto (**MB, B: Despreciables o bajos**).
- **Zona 4**: Riesgos improbables, pero de muy alto impacto (**A: Importantes**).
- En base a lo anterior, es posible generar la siguiente matriz de valoración de los impactos:

Tabla 35. Estimación cualitativa del riesgo

Riesgo		Probabilidad				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: CSAE: (2012a) y CTIC (2017). Diagramado por el Autor.

3.5.2.3. Paso 3: Salvaguardas

Los Controles de Seguridad, o salvaguardas, son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo (2012a), Los controles propuestos en MAGERIT se clasifican en los siguientes (CSAE, 2012b):

Tabla 36. Resumen de Salvaguardas definidos en el método MAGERIT

Control	Nomenclatura
Protecciones generales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (*software*)	SW
Protección de los equipos (*hardware*)	HW
Protección de las comunicaciones	COM
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Protecciones relativas al personal	PS
Protecciones de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E
Adquisición y desarrollo	NEW

Fuente: CSAE (2012b). Diagramado por el Autor.

3.6. Inventario y clasificación de activos informáticos

Luego de definidos los aspectos metodológicos de la evaluación de riesgo según el método MAGERIT, se empleó el mismo para la evaluación de los activos de la información de la institución, los elementos que se muestran a continuación son el resultado de esta evaluación.

El mismo procedimiento es el que se recomienda aplicar en la implementación definitiva del SGSI propuesto.

En todo caso, un activo o recurso informático está constituido por los objetos físicos, objetos e intangibles como: (software, bases de datos, sistemas operativos, cpu, disco duro entre otros) y el personal de trabajo y las instalaciones físicas, en la Unidad Educativa Nuestra Señora de Fátima se encuentran los siguientes:

Tabla 37. Activos informáticos identificados y empleados en la clasificación de riesgo por medio del método MAGERIT

Tipo	Elementos que lo conforman
Copias de Seguridad de los Sistemas de Información	**Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.**
Registros de Actividad	**Archivos de registros de actividad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.**
Códigos Fuentes	**Archivos de códigos fuentes de los diferentes Sistemas de Información.**
Gestión de Identidades	**Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras institucionales.**
Servicios Internos	**Servicios de uso interno para docentes, estudiantes y administrativos que cuentan con datos de acceso institucionales. *Software* académico, Bases de Datos de Biblioteca, Gestión Documental y Atención al usuario.**
Páginas web de acceso público	**Páginas, portales, ambientes virtuales de aprendizaje, sitios y aplicativos que son disponibles para el acceso público.**
Gestores de Bases de Datos	**Administran y gestionan las bases de datos que se utilizan para soportar todo el *software* académico, administrativo, educativo y demás que apoyan a los demás procesos institucionales.**
Software de Antivirus	***Software* para prevenir y eliminar el *malware*.**
Sistemas Operativos	***Software* que administra los recursos de las computadoras de uso institucional.**
Dispositivos de Respaldo	**Dispositivos que almacenan la información y son útiles para la recuperación de desastres.**
Firewall	**Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.**
Computadoras Portátiles de Uso Institucional	**Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.**
Computadoras de Escritorio de Uso Institucional	**Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.**
Escáner	**Dispositivos para transformar la información en formato digital.**
Impresoras	**Dispositivos para la impresión en papel.**
Router	**Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).**
Switches	**Administra las VLANS el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.**
Puntos de Acceso Inalámbricos	**Amplían la cobertura de la red por medio de conexiones inalámbricas.**
Red de Área Local	**Permite la interconexión de las computadoras institucionales, así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.**
Rack	**Aloja los servidores, *router*, *switches* y *firewall* protegiéndolos de la humedad, golpes o uso malintencionado.**
Fuente de Alimentación	**Provee y regula la energía a los Servidores.**
Sistema de Alimentación Ininterrumpida	**Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.**
Cableado Eléctrico	**Provee energía eléctrica a las instalaciones y dispositivos**

Diagramado por el Autor.

Según el método MAGERIT, los elementos listados en la tabla 37 se clasifican de la siguiente manera (CSAE, 2012b, págs. 8-13):

- [D] Datos/Información:

Tabla 38. Clasificación de los activos identificados dentro del grupo de "Datos/Información", según la metodología MAGERIT.

CODIGO	SUBTIPO	DESCRIPCION	CONTENIDO
D_BCK	[backup]	Copias de Seguridad de los Sistemas de Información	**Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.**
D_CNT	[files]	Contratos	**Contratos del personal administrativo y académico.**
D_HAC	[files]	Historial Académico	**Historial académico de los estudiantes**
D_HLB	[files]	Historial Laboral	**Historial del tiempo laborado por el personal administrativo y de contratación.**
D_PUB	[files]	Publicaciones	**Publicaciones y comunicaciones oficiales institucionales.**
D_LOG	[log]	Registros de Actividad	**Archivos de registros de actividad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.**
D_SRC	[source]	Códigos Fuentes	**Archivos de códigos fuentes de los diferentes Sistemas de Información.**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- [S] Servicios:

Tabla 39. Clasificación de los activos identificados dentro del grupo de "Servicios", según la metodología MAGERIT.

CODIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
S_MAI	[email]	Correo Electrónico	**Correo electrónico de uso institucional para docentes, y administrativos.**
S_GID	[int]	Gestión de Identidades	**Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras institucionales.**
S_INT	[int]	Servicios Internos	**Servicios de uso interno para docentes, estudiantes y administrativos que cuentan con datos de acceso institucionales. *Software* académico, Bases de Datos de Biblioteca, Gestión Documental y Atención al usuario.**
S_WWW	[www]	Páginas web de acceso público	**Páginas, portales, ambientes virtuales de aprendizaje, sitios y aplicativos que son disponibles para el acceso público**.

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[HW] *Hardware y Software***

Tabla 40. Clasificación de los activos identificados dentro del grupo de "*Hardware y Software*", según la metodología MAGERIT.

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
SW_STD	[std]	*Software* Estándar	***Software* desarrollado por terceros. *Software* que soporta la academia, los procesos administrativos y educación virtual y a distancia.**
SW_MAI	[email_client]	*Software* para Correo Electrónico	***Software* utilizado para el correo electrónico institucional.**
SW_DBS	[dbms]	Gestores de Bases de Datos	**Administran y gestionan las bases de datos que se utilizan para soportar todo el *software* académico, administrativo, educativo y demás que apoyan a los demás procesos institucionales.**
SW_OFM	[office]	Ofimática	***Software* necesario para la realización de las actividades, así como la producción de recursos.**
SW_AVS	[antivirus]	*Software* de Antivirus	***Software* para prevenir y eliminar el malware.**
SW_OPS	[os]	Sistemas Operativos	***Software* que administra los recursos de las computadoras de uso institucional.**
HW_ROU	[router]	Router	**Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).**
HW_SCN	[scaner]	Escáner	**Dispositivos para transformar la información en formato digital.**
HW_SWH	[switch]	Switch	**Administra las VLAN el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.**
HW_WAP	**[wap]**	**Puntos de Acceso Inalámbricos**	**Amplían la cobertura de la red por medio de conexiones inalámbricas.**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- [H] Comunicaciones:

Tabla 41. Clasificación de los activos identificados dentro del grupo de "Comunicaciones", según la metodología MAGERIT.

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
COM_INT	[internet]	Internet	**Permite el acceso a recursos de la web.**
COM_LAN	[LAN]	Red de Área Local	**Permite la interconexión de las computadoras institucionales, así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.**
COM_WIF	[wifi]	Conectividad Inalámbrica	**Permite la conectividad inalámbrica de las computadoras institucionales, así como amplía la cobertura.**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- [AUX] Equipamiento Auxiliar:

Tabla 42. Clasificación de los activos identificados dentro del grupo de "Equipamiento Auxiliar", según la metodología MAGERIT.

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
AUX_FBO	[fiber]	Fibra Óptica	**Provee transmisión de datos a alta velocidad.**
AUX_RCK	[furniture]	Rack	**Aloja los servidores, router, switches y firewall protegiéndoles de la humedad, golpes o uso malintencionado.**
AUX_PWR	[power]	Fuente de Alimentación	**Provee y regula la energía a los Servidores.**
AUX_UPS	[ups]	Sistema de Alimentación Ininterrumpida	**Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.**
AUX_WIR	[wire]	Cableado Eléctrico	**Provee energía eléctrica a las instalaciones y dispositivos.**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- [L] Instalaciones:

Tabla 43. Clasificación de los activos identificados dentro del grupo de "Instalaciones", según la metodología MAGERIT

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
L_SIT	**[site]**	**Dependencias de la Unidad Educativa Nuestra Señora de Fátima**	**Estructura física que alberga a la Unidad Educativa**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- [P] Personal:

Tabla 44. Clasificación de los activos identificados dentro del grupo de "Instalaciones", según la metodología MAGERIT

CÓDIGO	SUBTIPO	DESCRIPCIÓN	CONTENIDO
P_ADM	[adm]	Administrador de Sistema	**Persona encargada de administrar, gestionar, solucionar y ayudar en el correcto funcionamiento de los diferentes Sistemas de Información.**
P_COM	[com]	Administrador de Comunicaciones	**Persona encargada de administrar y gestionar el tráfico de datos en la red interna, así como configurar los diferentes dispositivos de comunicaciones que garanticen un óptimo rendimiento para el acceso a servicios y Sistemas de Información.**
P_DBA	[dba]	Administrador de Bases de Datos	**Persona que administra, configura y optimiza el rendimiento de las diferentes bases de datos que utilizan los Sistemas de Información para el soporte de los procesos institucionales.**
P_DES	[des]	Desarrolladores de *Software*	**Persona que se encarga de programar el código fuente para los Sistemas de Información en su defecto en el desarrollado por terceros para satisfacer las necesidades institucionales.**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

3.7. Valoración de los activos informáticos de conformidad con los impactos detectados según la metodología MAGERIT

Posterior al paso precedente, se realizó la valoración de los activos identificados en la Unidad Educativa Nuestra Señora de Fátima, conforme la tabla 44 de clasificación de los activos identificados dentro del grupo de "Instalaciones".

La valoración que acá se incluye, es el mismo que se propone aplicar en el proceso de implantación definitivo y monitoreo del SGSI. En la Tabla 45 se muestra la escala de evaluación.

Tabla 45. Escala de valoración empleada en la evaluación de los activos de la Unidad Educativa Nuestra Señora de Fátima

Impacto	Nomenclatura	Valor	Descripción
MUY ALTO	MA	10	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles
ALTO	A	7-9	El daño tiene consecuencias muy graves para la organización
MEDIO	M	4-6	El daño contiene consecuencias relevantes para la organización y su operación
BAJO	B	1-3	El daño contiene consecuencias relevantes, pero no afecta una gran parte de la organización
MUY BAJO	MB	0	El daño no contiene consecuencias relevantes para la organización

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

La valoración de los activos clasificados en el inventario, en base a la escala de la Tabla 45, es la siguiente:

- [D] Datos / Información:

Tabla 46. Valoración de los activos "Datos/Información" de la Unidad Educativa Nuestra Señora de Fátima

CODIGO	DESCRIPCION	IMPACTO	RAZÓN
D_BCK	Copias de Seguridad de los Sistemas de Información	MA	Los archivos de copias de seguridad son determinantes para la recuperación de desastres
D_CNT	Contratos	MA	Los contratos son esenciales para los procesos jurídicos-administrativos.
D_HAC	Historial Académico	MA	Datos esenciales para la evaluación del desempeño académico e histórico de los estudiantes en la institución.
D_HLB	Historial Laboral	MA	Archivos esenciales para el historial laboral de los administrativos y docentes.
D_PUB	Publicaciones	B	Archivos de publicaciones institucionales.
D_LOG	Registros de Actividad	MA	Los archivos de registros son esenciales para realizar seguimiento a fallos en los Sistemas de Información para determinar posibles causas de malfuncionamiento o acceso no autorizado.
D_SRC	Códigos Fuentes	MA	Los archivos de registros son esenciales para realizar seguimiento a fallos en los Sistemas de Información para determinar posibles causas de malfuncionamiento o acceso no autorizado

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[S] Servicios:**

Tabla 47. Valoración de los activos "Servicios" de la Unidad Educativa Nuestra Señora de Fátima

CODIGO	DESCRIPCIÓN	IMPACTO	RESPONSABLE
S_MAI	Correo Electrónico	A	**El correo electrónico se utiliza para la comunicación interna de los funcionarios, docentes y estudiantes**
S_GID	Gestión de Identidades	MA	**Acceso del personal administrativo a sus cuentas de usuario en el dominio institucional**
S_INT	Servicios Internos	MA	**Acceso a los servicios internos institucionales para el desarrollo normal de los procesos.**
S_WWW	Páginas web de acceso público	A	**Acceso a la página web institucional y otros sitos que ofrecen servicios al personal administrativo, docentes, estudiantes y público en genera**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[SW] *Software***

Tabla 48. Valoración de los activos "*Software*" de la Unidad Educativa Nuestra Señora de Fátima

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
SW_SWP	*Software* de Desarrollo Propio	MB	No se desarrolla *software*
SW_STD	*Software* Estándar	MA	Utilizados para el normal desarrollo de los procesos institucionales.
SW_MAI	*Software* para Correo Electrónico	A	Utilizado para la comunicación de administrativos, docentes y estudiantes
SW_DBS	Gestores de Bases de Datos	MA	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones
SW_OFM	Ofimática	B	Utilizado para la ejecución de tareas
SW_AVS	*Software* de Antivirus	M	Utilizado para la prevención y eliminación de *software* malintencionado, así como evitar la propagación de malware por la red
SW_OPS	Sistemas Operativos	M	Administra los recursos de *software* y *hardware* de las diferentes computadoras de uso institucional

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[HW] *Hardware*:**

Tabla 49. Valoración de los activos "*Hardware*" de la Unidad Educativa Nuestra Señora de Fátima

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
HW_BCK	Dispositivos de Respaldo	MA	Dispositivos que almacenan los archivos de las copias de seguridad necesarios para la recuperación en caso de desastres.
HW_FRW	Firewall	MA	Dispositivo que filtra los paquetes. Esencial para la configuración de seguridad de la red de datos.
HW_HOS	Servidores	MA	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos institucionales. Dentro de ellos se encuentran los Servidores de Aplicaciones, DNS, Bases de Datos, Mail y Web.
HW_PCM	Computadoras Portátiles de Uso Institucional	B	Dispositivos para la ejecución de tareas.
HW_PCP	Computadoras de Escritorio de Uso Institucional	B	Dispositivos para la ejecución de tareas.
HW_PRT	Impresoras	MB	Dispositivo para realizar impresiones en papel.
HW_ROU	Router	A	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
HW_SCN	Escáner	MB	Dispositivo para digitalizar documentos.
HW_SWH	Switch	A	Esencial para direccionar el tráfico de datos interno, administración de VLAN y segmentar el ancho de banda con el fin de optimizarla. Dentro de ellas se encuentran las VLAN administrativa, docentes y estudiantes.
HW_WAP	Puntos de acceso inalámbricos	B	Dispositivo que amplían la cobertura de la red para dar acceso inalámbrico

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[H] Comunicaciones**

Tabla 50. Valoración de los activos "Comunicaciones" de la Unidad Educativa Nuestra Señora de Fátima

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
COM_INT	Internet	A	Esencial para tener acceso a redes externas.
COM_LAN	Red de Área Local	MA	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos institucionales. Incluye todo el cableado estructurado
COM_WIF	Conectividad Inalámbrica	B	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos.

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[AUX] Equipamiento Auxiliar**

Tabla 51. Valoración de los activos "Equipamiento Auxiliar" de la Unidad Educativa Nuestra Señora de Fátima

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
AUX_FBO	Fibra Óptica	MA	Otorga alta velocidad de transmisión en el tráfico de datos interno. Da soporte de conectividad a toda la institución
AUX_RCK	Rack	A	Mantiene los dispositivos de red como el *router, switches* y servidores organizados y asegurados
AUX_PWR	Fuente de Alimentación	MA	Esencial para el funcionamiento normal de todos los dispositivos que soportan los Sistemas de Información y procesos institucionales.
AUX_UPS	Sistema de Alimentación Ininterrumpida	A	Esencial para mantener funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como también evita el daño parcial o total del *hardware*
AUX_WIR	Cableado Eléctrico	MA	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos institucionales

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[L] Instalaciones**

Tabla 52. Valoración de los activos "Instalaciones" de la Unidad Educativa Nuestra Señora de Fátima

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
L_SIT	Dependencias de la carrera	MA	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos institucionales

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

- **[P] Personal**

Tabla 53. Valoración de los activos "Personal" de la Unidad Educativa Nuestra Señora de Fátima

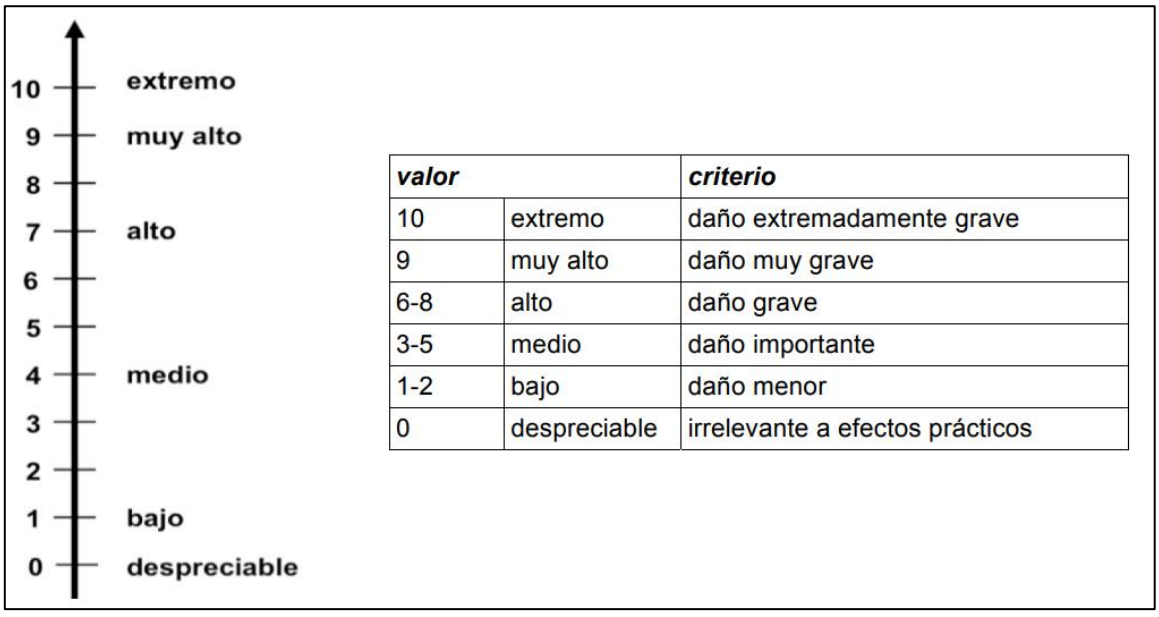
CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
P_ADM	Administrador de Sistema	A	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos institucionales y sus servicios
P_COM	Administrador de Comunicaciones	MA	Personas encargadas de administrar, soporte al normal funcionamiento de los servicios internos configurar y operar las redes de comunicación de datos que dan soporte al normal funcionamiento de los servicios internos
P_DBA	Administrador de Bases de Datos	MA	Persona encargada de administrar, configurar y optimizar el rendimiento de las bases de datos que contienen los datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros
P_DES	Desarrolladores de *Software*	M	Personas encargadas de desarrollar y/o programar institución. el *software* que se ajuste a las necesidades de la institución

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 8-13).

3.7.1. Valoración de los activos de acuerdo a las Dimensiones de Seguridad

Posterior al proceso de codificación precedente, se realizó la valoración de los activos identificados conforme a la metodología propuesta para tal fin por el método MAGERIT (2012b, pág. 19).

La escala empleada, posee 10 valores asignables, donde 0 es un valor despreciable para indicar riesgo (CSAE, 2012b, pág. 19).:



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Ilustración 6. Criterios de Valoración. Recuperado de (CSAE, 2012b, pág. 19)

Luego de agregar la valoración indicada anteriormente a las dimensiones de clasificación queda lo siguiente; (Los descriptores de la puntuación se pueden observar en el Anexo1, y son tomados del Magerit 3.0, Libro 2).

- **[D] Datos/Información**

Tabla 54. Valoración de los activos "Datos/Información" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	**[T]**
D_BCK	Copias de Seguridad de los Sistemas de Información	**3**		**2**		
D_CNT	Contratos		**2**			
D_HAC	Historial Académico		**4**	**7**	**4**	**4**
D_HLB	Historial Laboral		**3**	**2**		
D_PUB	Publicaciones	**1**				
D_LOG	Registros de Actividad	**1**		**2**		**3**
D_SRC	Códigos Fuentes		**3**	**5**		
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 55. Interpretación de la Valoración de los activos "Datos/Información" de acuerdo a las Dimensiones de Seguridad

CODIGO	DIM. SEG	DESCRIPCIÓN
D_BCK	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_CNT	[I]	2.pi1: Pudiera causar molestias a un individuo
D_HAC	[I][A][T]	4.pi2: Probablemente quebrante leyes o regulaciones
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
D_HLB	[I]	3.lro: Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_PUB	[D]	1.pi1: Pudiera causar molestias a un individuo
D_LOG	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
D_SRC	[I]	3.olm: Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	[C]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[S] Servicios**

Tabla 56. Valoración de los activos "Servicios" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
S_MAI	Correo Electrónico	**3**		**2**		
S_GID	Gestión de Identidades	**5**	**2**	**2**		**4**
S_INT	Servicios Internos	**3**				
S_WWW	Páginas web de acceso público	**3**				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 57. Interpretación de la Valoración de los activos "Servicios" de acuerdo a las Dimensiones de Seguridad

CODIGO	DIM. SEG	DESCRIPCIÓN
S_MAI	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
S_GID	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	2.pi1: Pudiera causar molestias a un individuo
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
S_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
S_WWW	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[SW] *Software*:**

Tabla 58. Valoración de los activos "*Software*" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
SW_STD	*Software* estándar	**3**		**4**	**7**	**4**
SW_MAI	*Software* de correo electrónico	**5**				**1**
SW_DBS	Gestores de base de datos	**7**	**7**	**7**	**7**	
SW_OFM	Ofimática	**1**				
SW_AVS	*Software* antivirus			**7**		
SW_OPS	Sistemas operativos	**5**	**7**			
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 59. Interpretación de la Valoración de los activos "*Software*" de acuerdo a las Dimensiones de Seguridad

CODIGO	DIM. SEG	DESCRIPCIÓN
SW_STD	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	4.pi1: Probablemente afecte a un grupo de individuos
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
SW_MAI	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	1.si: Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
SW_DBS	[D][I][A]	7.adm: Probablemente impediría la operación efectiva de la Organización
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
SW_OFM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
SW_AVS	[C]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
SW_OPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[HW] *Hardware***

Tabla 60. Valoración de los activos "*Hardware*" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**
HW_BCK	Dispositivos de respaldo			**2**		**3**
HW_FRW	Firewall	**7**				
HW_HOS	Servidores	**5**		**7**	**7**	
HW_PCM	Notebook institucional	**1**				
HW_PCP	Desktop institucional	**1**				
HW_ROU	Router	**1**			**7**	
HW_PRT	Impresoras	**1**				
HW_SCN	Scanner	**5**				
HW_SWH	Switch	**1**			**7**	
HW_WAP	Puntos de acceso inalámbrico	5				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 61. Interpretación de la Valoración de los activos "*Hardware*" de acuerdo a las Dimensiones de Seguridad

CÓDIGO	DIM SEG	DESCRIPCIÓN
HW_BCK	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
HW_FRW	[D]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_HOS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C][A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_PCM/ HW_PCP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
HW_PRT/HW_SCN	[D]	1.pi1: Pudiera causar molestias a un individuo
HW_ROU	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
HW_SWH	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_WAP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[COM] Comunicaciones**

Tabla 62. Valoración de los activos "Comunicaciones" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
COM_INT	Internet	3				
COM_LAN	Red de área local	5				
COM_WIF	Conectividad inalámbrica	1				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 63. Interpretación de la Valoración de los activos "Comunicaciones" de acuerdo a las Dimensiones de Seguridad

CÓDIGO	DIM SEG	DESCRIPCIÓN
COM_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
COM_LAN	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
COM_WIF	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[AUX] Equipo Auxiliar**

Tabla 64. Valoración de los activos "Equipo Auxiliar" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
AUX_FBO	Fibra óptica	**5**				
AUX_RCK	Rack	**5**				
AUX_PWR	Fuente de alimentación	**5**				
AUX_UPS	Sistema de alimentación ininterrumpida	**5**				
AUX_WIR	Cableado Eléctrico	5				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 65. Interpretación de la Valoración de los activos "Equipo Auxiliar" de acuerdo a las Dimensiones de Seguridad

CÓDIGO	DIM SEG	DESCRIPCIÓN
AUX_FBO	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_RCK	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_PWR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_UPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_WIR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[L] Instalaciones**

Tabla 66. Valoración de los activos "Instalaciones" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
L_SIT	Edificio Oficinas de la carrera Ingeniería en Telecomunicaciones	7				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 67. Interpretación de la Valoración de los activos "Instalaciones" de acuerdo a las Dimensiones de Seguridad

CÓDIGO	DIM SEG	DESCRIPCIÓN
L_SIT	[D]	7.adm: Probablemente impediría la operación efectiva de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

- **[P] Personal:**

Tabla 68. Valoración de los activos "Personal" de acuerdo a las Dimensiones de Seguridad

CODIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
P_ADM	Administrador de sistema	5				
P_COM	Administrador de comunicaciones	5				
P_DBA	Administrador de Base de Datos	5				
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Tabla 69. Interpretación de la Valoración de los activos "Personal" de acuerdo a las Dimensiones de Seguridad

CÓDIGO	DIM SEG	DESCRIPCIÓN
P_ADM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_COM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DBA	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
Dimensiones: [D] disponibilidad; [I] integridad; [C] confidencialidad; [A] autenticidad; [T] trazabilidad (Para interpretación de los descriptores de la puntuación asignada ver el anexo 1 del presente documento)		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b, págs. 19-23).

Posterior al paso anterior, se realizó la valoración de las amenazas en cada activo documentado. Para esto, se empleó una escala con el rango de frecuencia de posible presentación de la amenaza (anuales, mensuales y semanales) (CSAE, 2012b).

3.8. Identificación y Valorización de Amenazas

La valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones queda como sigue:

Tabla 70. Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

[D] Datos/Información						
Copias de Seguridad de los Sistemas de Información	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.1 [E.1] Errores de los usuarios	5	5%	50%	75%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	5	0%	100%	20%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.3.2 [E.2] Errores del administrador	5	50%	50%	75%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	0%	100%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	75%	75%	0%	0%
Contratos	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.1 [E.1] Errores de los usuarios	50	0%	50%	0%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	10	0%	50%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	100%	0%	0%	0%
5.3.9 [E.14] Escapes de información	10	0%	0%	100%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	75%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
Historial Académico	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	10	0%	0%	75%	0%	0%
5.3.9 [E.14] Escapes de información	10	0%	50%	50%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	75%	75%	75%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%
Historial Laboral	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	10	0%	0%	75%	0%	0%
5.3.9 [E.14] Escapes de información	10	0%	50%	50%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	75%	75%	75%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%
Publicaciones	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.10 [E.15] Alteración accidental de la información	5	0%	5%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	5	5%	0%	0%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	50%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	5%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	0%	5%	5%	0%	0%
Registros de Actividad	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.11 [E.18] Destrucción de información	5	10%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.3.3 [E.3] Errores de monitorización (log)	5	100%	0%	0%	0%	100%
5.4.1 [A.3] Manipulación de los registros de actividad (log)	5	0%	100%	0%	0%	100%
5.4.13 [A.15] Modificación deliberada de la información	5	100%	100%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	100%	0%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Códigos de Fuente	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.10 [E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.3.4 [E.4] Errores de configuración	10	20%	0%	0%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	0%	100%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	0%	100%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%
[S] Servicios						
Correo Electrónico	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.1 [E.1] Errores de los usuarios	50	0%	0%	0%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	10	0%	75%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9 [E.14] Escapes de información	50	0%	0%	100%	0%	0%
5.4.11 [A.13] Repudio	5	0%	0%	0%	100%	20%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	0%	0%	75%	75%	20%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	0%	0%
5.4.8 [A.10] Alteración de secuencia	5	0%	100%	0%	100%	0%
5.4.9 [A.11] Acceso no autorizado	10	0%	0%	100%	0%	0%
Gestión de Identidades	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.10 [E.15] Alteración accidental de la información	5	0%	100%	0%	100%	20%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9 [E.14] Escapes de información	50	0%	0%	50%	0%	0%
5.4.11 [A.13] Repudio	5	0%	0%	0%	50%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	100%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	0%	0%	100%	75%	20%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	100%	20%
5.4.9 [A.11] Acceso no autorizado	5	0%	0%	100%	0%	0%
Servicios Internos	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
Páginas Web de acceso Público	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.10 [E.15] Alteración accidental de la información	10	0%	0%	50%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
SW] *Software*						
***Software* estándar**	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	5	20%	0%	0%	0%	0%
5.3.1 [E.1] Errores de los usuarios	50	0%	0%	5%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	50%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	50	20%	0%	0%	0%	20%
5.3.2 [E.2] Errores del administrador	10	20%	20%	20%	0%	0%
5.3.6 [E.8] Difusión de *software* dañino	10	10%	0%	0%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	20%	20%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	50%	100%	100%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	5%	5%	0%	0%
5.4.16 [A.22] Manipulación de programas	5	0%	75%	75%	75%	20%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	0%	50%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	100%	100%	100%	0%
5.4.5 [A.7] Uso no previsto	5	5%	0%	0%	0%	0%
5.4.6 [A.8] Difusión de *software* dañino	10	50%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8 [A.10] Alteración de secuencia	5	100%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

***Software* de Correo Electrónico**	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	10	50%	0%	0%	0%	0%
5.3.1 [E.1] Errores de los usuarios	70	5%	0%	0%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	5	20%	0%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	1	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	50	0%	0%	100%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	10	20%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	10	50%	0%	0%	0%	0%
5.3.6 [E.8] Difusión de *software* dañino	5	20%	0%	20%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	75%	75%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	50%	50%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	0%	100%	0%
5.4.16 [A.22] Manipulación de programas	5	20%	0%	0%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	0%	100%	100%	100%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	75%	100%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	5%	0%	0%	0%	0%
5.4.6 [A.8] Difusión de *software* dañino	5	20%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	0%
5.4.8 [A.10] Alteración de secuencia	5	0%	75%	75%	75%	0%
5.4.9 [A.11] Acceso no autorizado	5	50%	75%	75%	0%	20%
Gestores de Bases de Datos	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	75%	75%	0%	75%
5.3.1 [E.1] Errores de los usuarios	10	5%	5%	5%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	5	75%	75%	0%	75%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	100%	100%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	10	50%	75%	75%	0%	0%
5.3.2 [E.2] Errores del administrador	10	50%	50%	50%	0%	0%
5.3.6 [E.8] Difusión de *software* dañino	5	5%	5%	5%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	0%	75%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	100%	100%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	75%	100%	0%	0%
5.4.16 [A.22] Manipulación de programas	5	0%	50%	50%	0%	0%
5.4.3 [A.5] Suplantación de la identidad del usuario	10	0%	0%	50%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	100%	0%
5.4.5 [A.7] Uso no previsto	5	75%	75%	75%	75%	0%
5.4.6 [A.8] Difusión de *software* dañino	5	5%	5%	5%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	0%	10%	0%	0%	0%
5.4.8 [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	100%	100%	100%	0%
Ofimática	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	10	10%	0%	0%	0%	0%
5.3.1 [E.1] Errores de los usuarios	50	5%	0%	0%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	50	50%	0%	0%	0%	0%
5.3.6 [E.8] Difusión de *software* dañino	10	50%	0%	0%	75%	0%
5.4.5 [A.7] Uso no previsto	50	0%	0%	0%	0%	0%
5.4.6 [A.8] Difusión de *software* dañino	5	50%	0%	50%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	50%	0%	0%	0%	0%
***Software* de Antivirus**	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1 [E.1] Errores de los usuarios	50	50%	0%	0%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	10	50%	0%	0%	0%	0%
5.3.6 [E.8] Difusión de *software* dañino	10	75%	0%	0%	75%	0%
5.4.5 [A.7] Uso no previsto	5	20%	0%	0%	0%	0%
5.4.6 [A.8] Difusión de *software* dañino	5	50%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	100%	0%	0%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Sistemas Operativos	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1 [E.1] Errores de los usuarios	10	75%	0%	0%	0%	20%
5.3.10 [E.15] Alteración accidental de la información	10	50%	20%	20%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	75%	0%	0%
5.3.13 [E.20] Vulnerabilidades de los programas (*software*)	5	50%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	10	75%	0%	0%	0%	20%
5.3.6 [E.8] Difusión de *software* dañino	10	75%	50%	0%	0%	0%
5.3.9 [E.14] Escapes de información	5	0%	0%	5%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	75%	100%	100%	0%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.16 [A.22] Manipulación de programas	5	0%	0%	50%	0%	50%
5.4.3 [A.5] Suplantación de la identidad del usuario	5	100%	100%	100%	0%	20%
5.4.4 [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	20%
5.4.5 [A.7] Uso no previsto	5	50%	0%	0%	0%	0%
5.4.6 [A.8] Difusión de *software* dañino	5	75%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8 [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	75%	75%	0%	20%
[HW] *Hardware*						
Dispositivos de Respaldo	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	50%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	75%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	5	50%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	50%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Firewall	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Servidores	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Notebook Institucional	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	10%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	10	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	50%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Desktop Institucional	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	10	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	50%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Router	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Impresoras	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	10	75%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
Escáner	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	10	75%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
Switch	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Puntos de acceso inálambrico	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	75%	0%	0%	0%	0%
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17 [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17 [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18 [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4 [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5 [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
[COM] Comunicaciones						
Internet	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	10	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	5	20%	0%	0%	0%	0%
5.3.7 [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10 [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12 [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18 [A.24] Denegación de servicio	10	100%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8 [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%
5.4.9 [A.11] Acceso no autorizado	10	50%	0%	0%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Red de área local	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	70	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	10	20%	0%	0%	0%	0%
5.3.7 [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10 [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12 [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18 [A.24] Denegación de servicio	70	100%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8 [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%
5.4.9 [A.11] Acceso no autorizado	50	50%	0%	0%	0%	0%
Conectividad inalámbrica	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.16 [E.24] Caída del sistema por agotamiento de recursos	70	100%	0%	0%	0%	0%
5.3.2 [E.2] Errores del administrador	10	20%	0%	0%	0%	0%
5.3.7 [E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
5.4.10 [A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
5.4.12 [A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
5.4.18 [A.24] Denegación de servicio	70	100%	0%	0%	0%	0%
5.4.7 [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	20%
5.4.8 [A.10] Alteración de secuencia	5	0%	0%	75%	75%	20%
5.4.9 [A.11] Acceso no autorizado	50	50%	0%	0%	0%	0%
[AUX] Equipamiento Auxiliar						
Fibra óptica	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	5	5%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	20%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
Rack	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	5%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	20	5%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	20%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
Fuente de alimentación	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	5%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	20	5%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	20%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
Sistema de alimentación ininterrumpida	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	5%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	20	5%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	20%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

Tabla 70. (Cont.). Valoración porcentual de la ocurrencia de las amenazas detectadas en la Unidad Educativa Nuestra Señora de Fátima, y su respectivo impacto en las dimensiones evaluadas.

Cableado eléctrico	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.2.1 [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2 [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6 [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7 [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8 [I.7] Condiciones inadecuadas de temperatura o humedad	5	5%	0%	0%	0%	0%
5.3.15 [E.23] Errores de mantenimiento / actualización de equipos (*hardware*)	5	20%	0%	0%	0%	0%
5.4.19 [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
[L] Instalaciones						
Dependencias de la carrera	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.1.3 [N.*] Desastres Naturales	5	100%	0%	0%	0%	0%
5.2.12 [I.11] Emanaciones electromagnéticas	5	20%	0%	0%	0%	0%
5.3.10 [E.15] Alteración accidental de la información	5	0%	100%	0%	0%	0%
5.3.11 [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12 [E.19] Fugas de información	5	0%	0%	100%	0%	0%
5.4.13 [A.15] Modificación deliberada de la información	5	0%	100%	100%	100%	0%
5.4.14 [A.18] Destrucción de información	5	100%	0%	100%	0%	0%
5.4.15 [A.19] Divulgación de información	5	0%	100%	100%	0%	0%
5.4.20 [A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
5.4.5 [A.7] Uso no previsto	5	50%	0%	0%	0%	0%
5.4.9 [A.11] Acceso no autorizado	5	75%	0%	0%	0%	0%
[P] Personal						
Administrador de Sistemas	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.12 [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18 [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5 [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22 [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%
Administrador de comunicaciones	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.12 [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18 [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5 [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22 [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%
Administrador de base de datos	**Frec**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
5.3.12 [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18 [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5 [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22 [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%

Diagramado por el Autor, en base a la información recabada de CSAE (2012b) (Cont.)

3.8.1. Riesgo Potencial.

La determinación del riesgo potencial de cada uno de los activos de la información caracterizados, se realizó de manera cualitativa en base a las zonas de riesgo propuestas en el método MAGERIT (CSAE, 2012b). El mismo, fue calculado en base al impacto encontrado en cada uno de los activos según la amenaza general a la que está expuesto (CSAE, 2012b).

De esta manera, las matrices de riesgo potencial individuales por activo y dimensión, quedan como se muestran a continuación:

- **[D] Datos/Información**

Tabla 71. Riesgo Potencial de los activos "Datos/Información"

CÓD	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
D_BCK	Copias de Seguridad de los Sistemas de Información	**MA**	**MB**	**E*, A***	R_D_BCK	A
D_CNT	Contratos	**MA**	**M**	**E*, A***	R_D_CNT	MA
D_HAC	Historial Académico	**MA**	**B**	**E*, A***	R_D_HAC	MA
D_HLB	Historial Laboral	**MA**	**B**	**E*, A***	R_D_HLB	MA
D_PUB	Publicaciones	**B**	**MB**	**E*, A***	R_D_PUB	MB
D_LOG	Registros de Actividad	**MA**	**MB**	**E*, A***	R_D_LOG	A
D_SRC	Códigos Fuentes	**MA**	**B**	**E*, A***	R_D_SRC	MA

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. (Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[S] Servicios**

Tabla 72. Riesgo Potencial de los activos "Servicios"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
S_MAI	Correo Electrónico	A	M	E*, A*	R_S_MAI	A
S_GID	Gestión de Identidades	MA	M	E*, A*	R_S_GID	MA
S_INT	Servicios Internos	MA	M	E*, A*	R_S_INT	MA
S_WWW	Páginas web de acceso público	A	M	E*, A*	R_S_WWW	A

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. (Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[SW] *Software***

Tabla 73. Riesgo Potencial de los activos "*Software*"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
SW_STD	*Software* Estándar	MA	M	I*, E*, A*	R_SW_STD	MA
SW_MAI	*Software* para Correo Electrónico	A	A	I*, E*, A*	R_SW_MAI	MA
SW_DBS	Gestores de Bases de Datos	MA	B	I*, E*, A*	R_SW_DBS	MA
SW_OFM	Ofimática	B	M	I*, E*, A*	R_SW_OFM	B
SW_AVS	*Software* de Antivirus	M	M	I*, E*, A*	R_SW_AVS	M
SW_OPS	Sistemas Operativos	M	B	I*, E*, A*	R_SW_OPS	M

Amenazas: [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados. (Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[HW] *Hardware***

Tabla 74. Riesgo Potencial de los activos "*Hardware*"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
HW_BCK	Dispositivos de Respaldo	MA	M	I*, E*, A*	R_HW_BCK	MA
HW_FRW	Firewall	MA	M	I*, E*, A*	R_HW_FRW	MA
HW_HOS	Servidores	MA	M	I*, E*, A*	R_HW_HOS	MA
HW_PCM	Computadoras Portátiles de Uso Institucional	B	M	I*, E*, A*	R_HW_PCM	B
HW_PCP	Computadoras de Escritorio de Uso Institucional	B	M	I*, E*, A*	R_HW_PCP	B
HW_PRT	Impresoras	MB	M	I*, E*, A*	R_HW_PRT	MB
HW_ROU	Router	A	M	I*, E*, A*	R_HW_ROU	A
HW_SCN	Escáner	MB	M	I*, E*, A*	R_HW_SCN	MB
HW_SWH	Switch	A	M	I*, E*, A*	R_HW_SWH	A
HW_WAP	Puntos de Acceso Inalámbricos	B	M	I*, E*, A*	R_HW_WAP	B

Amenazas: [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados.
(Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[COM] Comunicaciones**

Tabla 75. Riesgo Potencial de los activos "Comunicaciones"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
COM_INT	Internet	A	A	E*, A*	R_COM_INT	MA
COM_LAN	Red de Área Local	MA	A	E*, A*	R_COM_LAN	MA
COM_WIF	Conectividad Inalámbrica	B	A	E*, A*	R_COM_WIF	M

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados.
(Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[AUX] Equipo Auxiliar**

Tabla 76. Riesgo Potencial de los activos "Equipo Auxiliar"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
AUX_FBO	Fibra Óptica	MA	M	I*, E*, A*	R_AUX_FBO	MA
AUX_RCK	Rack	A	M	I*, E*, A*	R_AUX_RCK	A
AUX_PWR	Fuente de Alimentación	MA	M	I*, E*, A*	R_AUX_PWR	MA
AUX_UPS	Sistema de Alimentación Ininterrumpida	A	M	I*, E*, A*	R_AUX_UPS	A
AUX_WIR	Cableado Eléctrico	MA	M	I*, E*, A*	R_AUX_WIR	MA

Amenazas: [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados.
(Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[L] Instalaciones**

Tabla 77. Riesgo Potencial de los activos "Instalaciones"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
L_SIT	Oficina de Sistemas de Información y Telemática	MA	MB	N*, I*,E*,A*	R_L_SIT	A
Amenazas: [N] Desastres naturales; [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados. (Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

- **[P] Personal**

Tabla 78. Riesgo Potencial de los activos "Personal"

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO
P_ADM	Administrador de Sistema	A	B	E*, A*	R_P_ADM	A
P_COM	Administrador de Comunicaciones	MA	B	E*, A*	R_P_COM	MA
P_DBA	Administrador de Bases de Datos	MA	B	E*, A*	R_P_DBA	MA
Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. (Impacto/Probabilidad/Riesgo: **MA:** Muy Alto; **A: Alto; M: Medio; B: Bajo; MB: Muy Bajo)**						

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

La categorización de los riesgos en base a índice establecido en el método de MAGERIT queda como se muestra a continuación:

Tabla 79. Mapeo general de riesgo por activos de la información

RIESGO		PROBABILIDAD				
		MB	B	M	A	**MA**
IMPACTO	MA	R_D_BCK, R_D_LOG, R_L_SIT	R_D_HAC, R_D_HCL, R_D_HLB, R_D_SRC, R_SW_DBS, R_P_COM, R_P_DBA	R_D_CNT, R_S_GID, R_S_INT, R_SW_SWP, R_SW_STD, R_HW_BCK, R_HW_FRW, R_HW_HOS, R_AUX_FBO, R_AUX_PWR, R_AUX_WIR	R_COM_LAN	
	A		R_P_ADM	R_S_MAI, R_S_WWW, R_HW_ROU, R_HW_SWH, R_AUX_RCK, R_AUX_UPS	R_SW_MAI, R_COM_INT	
	M	R_D_RDG	R_SW_OPS	R_SW_AVS,		
	B	R_D_PUB,		R_SW_OFM, R_HW_PCM, R_HW_PCP, R_HW_WAP	R_COM_WIF	
	MB	R_D_OVA,		R_HW_PRT, R_HW_SCN		

Diagramado por el Autor, en base a la información recabada de CSAE (2012b).

Como se puede apreciar de los elementos anteriormente analizados, la Unidad Educativa Nuestra Señora de Fátima, posee una gran mayoría de los riesgos detectados en los grupos de alto y muy alto riesgo.

Los elementos ubicados en estas categorías deben ser atendidos con premura, pero de manera controlada, ya que principalmente se asocian al mantenimiento del *hardware* y a las redes, y la corrección de los fallos en estos elementos debe ser individualizada y exhaustiva.

Además de lo anterior, una situación riesgosa también detectada, es la de la existencia de la posibilidad de filtración de información al estar expuesto el sistema informático en cierta medida a la intercepción de la información ya que las comunicaciones o los elementos que contextualizan estos, no son encriptados y no existen políticas de intervención activas.

Adicionalmente, el *software* ofimático y el *hardware* que no es de procesamiento de información se catalogan en una zona de riesgo baja debido a que tienen muy bajo impacto en la operación de los procesos de la institución, sin embargo, este grupo de elementos, tal como se constató de manera presencial, no se encuentra actualizado y en el caso del sistema operativo de la mayoría de las computadoras ya se encuentra fuera de servicio (*Windows* XP).

La característica de riesgo por estos elementos, podría disminuir mucho más su impacto si se consideran políticas para la actualización total de las unidades de computo.

También se considera, que a pesar de que la institución se encuentra en un país que sufre de una serie de eventos sísmicos, las catástrofes naturales no representan un riesgo tan alto para los activos de la información debido a las condiciones de la construcción del edificio donde hace vida la unidad educativa, son adecuadas para soportar gran parte de estos eventos, sin embargo, los aspectos relacionados con el control físico del acceso a las diversas áreas. podrían facilitar que se generen daños voluntarios o involuntarios en el *hardware* o equipos.

3.9. Declaración de Aplicabilidad.

3.9.1. Propósito, Alcance y Usuarios.

En esta sección de la propuesta, se debe definir los controles más idóneos a implementarse en la Unidad Educativa Nuestra Señora de Fátima, así mismo, se incluyen los objetivos propuestos para dichos controles y la forma de implementación de los mismos. Los elementos que componen esta sección, se corresponden a los controles aplicables de la normativa ISO/IEC 27001:2013 en base a la implementación de un SGISI.

3.9.2. Aplicabilidad de Controles

El principal objetivo de esta sección, es la de definir cuáles de las medidas de seguridad, incluidos en el estándar ISO 27001:2013 son los que pueden aplicarse. A continuación, se muestran estos:

Tabla 80. Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.5.1	***Orientación de la dirección para la gestión de la seguridad de la información***		
A.5.1.1	Políticas para la seguridad de la información	**SI**	Se redactan y documentan las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los empleados y público en general.
A.5.1.2	Revisión de las políticas para la seguridad de la información	**SI**	Las políticas de seguridad de la información se revisan y evalúan periódicamente y/o cuando sea necesario. La revisión es llevada a cabo por el Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad de la Información y la Dirección Estratégica. Se documentan los cambios y las justificaciones de los mismos.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	***Organización Interna***		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	**SI**	Los roles y responsabilidades de la seguridad de la información están definidas.
A.6.1.2	Separación de deberes	**SI**	El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad mantiene los contactos actualizados para incidentes de seguridad
A.6.1.4	Contacto con grupos de interés especial	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad mantienen contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.
A.6.1.5	Seguridad de la información en la gestión de proyectos	**SI**	El Jefe de Seguridad es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.
A.6.2	***Dispositivos móviles y trabajo a distancia***		
A.6.2.1	Políticas para dispositivos móviles	**SI**	Se documenta una política de seguridad apropiada para los móviles. Los dispositivos móviles son configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional.
A.6.2.2	Trabajo a distancia	**NO**	**NA**

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.1	***Antes de asumir el empleo***		
A.7.1.1	Selección	**SI**	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
A.7.1.2	Términos y condiciones del empleo	**SI**	Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
A.7.2	***Durante la ejecución del empleo***		
A.7.2.1	Responsabilidades de la dirección	**SI**	La dirección comprende la importancia de la seguridad de la información y soporta el diseño del SGSI.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad realizan campañas y talleres de formación y educación en la seguridad de la información de forma periódica al personal administrativo
A.7.2.3	Proceso disciplinario	**SI**	Los funcionarios son sometidos a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
A.7.3	***Terminación y cambio de empleo***		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**SI**	El Jefe de Seguridad vela que el funcionario que termine contrato o cambie de responsabilidades, se le sean reasignados los permisos y condiciones de seguridad de la información.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	***Responsabilidad por los activos***		
A.8.1.1	Inventario de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad junto a los funcionarios, realizan el inventario de activos y se documentan con su clasificación y responsable.
A.8.1.2	Propiedad de los activos	**SI**	Los activos inventariados tienen asignados los funcionarios responsables.
A.8.1.3	Uso aceptable de los activos	**SI**	Los funcionarios se comprometen a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Devolución de activos	**SI**	Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.
A.8.2	***Clasificación de la información***		
A.8.2.1	Clasificación de la información	**SI**	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos
A.8.2.2	Etiquetado de la información	**SI**	Cada uno de los activos inventariados están etiquetados con la clasificación de la información asociada.
A.8.2.3	Manejo de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad junto a los funcionarios realizan y documentan los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
A.8.3	***Manejo de medios***		
A.8.3.1	Gestión de medios removibles	**SI**	Existe una política para la gestión de los medios removibles y se clasifican y protegen de acuerdo a su tipo.
A.8.3.2	Disposición de los medios	**SI**	Los medios removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
A.8.3.3	Transferencia de medios físicos	**NO**	**NA**
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.9	**CONTROL DE ACCESO**		
A.9.1	***Requisitos del negocio para control de acceso***		
A.9.1.1	Política de control de acceso	**SI**	La política de control de acceso está documentada en las Políticas de la Seguridad de Información.
A.9.1.2	Acceso a redes y a servicios en red	**SI**	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.9.2	***Gestión de acceso de usuarios***		
A.9.2.1	Registro y cancelación de registro de usuarios	**NO**	**NA**
A.9.2.2	Suministro de acceso de usuarios	**NO**	**NA**
A.9.2.3	Gestión de derechos de acceso privilegiado	**SI**	A los funcionarios se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los funcionarios son agrupados bajo Perfiles de Usuario.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**SI**	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
A.9.2.5	Revisión de los derechos de acceso de usuarios	**SI**	El Jefe de Seguridad junto a los funcionarios encargados verifican que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se realiza de forma periódica y cualquier anormalidad es debidamente documentada.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad verifican y eliminan los permisos asignados al personal que sea retirado.
A.9.3	***Responsabilidades de los usuarios***		
A.9.3.1	Uso de información de autenticación secreta	**SI**	La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
A.9.4	***Control de acceso a sistemas y aplicaciones***		
A.9.4.1	Restricción de acceso a la información	**SI**	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del empleado en la organización.
A.9.4.2	Procedimiento de ingreso seguro	**SI**	Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro. Se emplean mecanismos seguros de cifrado de información.
A.9.4.3	Sistema de gestión de contraseñas	**SI**	Se implementan mecanismos de recuperación de contraseñas de forma automática y se garantiza que la nueva contraseña del funcionario cumpla con los requisitos de seguridad expuestos en la Política de Seguridad de contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados	**SI**	El Líder del Proceso de Desarrollo Tecnológico verifica que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados. Se realiza una verificación de forma aleatoria.
A.9.4.5	Control de acceso a códigos fuente de programas	**SI**	El Jefe de Seguridad verifica que los códigos fuentes de los programas permanecen de forma confidencial.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.10	**CRIPTOGRAFÍA**		
A.10.1	***Controles criptográficos***		
A.10.1.1	Política sobre el uso de controles criptográficos	**SI**	Existe una política de seguridad que documente el uso de los controles criptográficos, la escogencia y justificación de los algoritmos de cifrado y su aplicación en los servicios que la requieran.
A.10.1.2	Gestión de llaves	**SI**	Existe una política de seguridad que documente el proceso y ciclo de vida de las llaves criptográficas.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	***Áreas Seguras***		
A.11.1.1	Perímetro de seguridad física	**SI**	El perímetro físico controlado por tarjetas de acceso, así como personal de seguridad en la infraestructura que contiene el *hardware* de las operaciones críticas.
A.11.1.2	Controles de acceso físicos	**SI**	El acceso físico a la infraestructura que contiene el *hardware* de las operaciones críticas está controlado por medio de tarjetas inteligentes que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**NO**	**NA**
A.11.1.4	Protección contra amenazas externas y ambientales	**SI**	Existe un Plan de Continuidad del Negocio y de Recuperación de Desastres que es puesto a prueba a intervalos regulares.
A.11.1.5	Trabajo en áreas seguras	**NO**	**NA**
A.11.1.6	Áreas de despacho y carga	**SI**	Existe un área diseñada y estructurada para recibir el descargue de los equipos que impiden el acceso al interior de la oficina e infraestructura que contiene el *hardware* de las operaciones críticas.
A.11.2	***Equipos***		
A.11.2.1	Ubicación y protección de los equipos	**SI**	Los equipos están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. Y existen políticas de seguridad de la información documentadas para su uso.
A.11.2.2	Servicios de suministro	**SI**	Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.
A.11.2.3	Seguridad del cableado	**SI**	El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
A.11.2.4	Mantenimiento de equipos	**SI**	Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.
A.11.2.5	Retiro de activos	**SI**	El Jefe de Mantenimiento en concordancia con el Líder del Proceso de Desarrollo Tecnológico documenta el retiro de los activos.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**NO**	**NA**
A.11.2.7	Disposición segura o reutilización de equipos	**SI**	El Jefe de Mantenimiento y el Líder del Proceso de Desarrollo Tecnológico realizan un procedimiento seguro y documentado para la disposición o reutilización de equipos.
A.11.2.8	Equipos de usuario desatendido	**SI**	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	**SI**	El Jefe de Seguridad garantiza que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	***Procedimientos operacionales y responsabilidades***		
A.12.1.1	Procedimientos de operación documentados	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios documentan los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.
A.12.1.2	Gestión de cambios	**SI**	El Jefe de Seguridad verifica que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
A.12.1.3	Gestión de capacidad	**SI**	El Líder del Proceso de Desarrollo Tecnológico y los funcionarios realizan un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo a las necesidades críticas de la organización.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**SI**	El Jefe de Seguridad asegura que los ambientes de desarrollo, pruebas y operación están debidamente separados y no ponen en riesgo la información.
A.12.2	***Protección contra códigos maliciosos***		
A.12.2.1	Controles contra códigos maliciosos	**SI**	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el *software* de código malicioso. El Jefe de Seguridad y los funcionarios verifican que el *software* está protegido con antivirus y existe una política documentada de actualización de todo el *software* utilizado, antivirus y sistema operativo.
A.12.3	***Copias de respaldo***		
A.12.3.1	Respaldo de la información	**SI**	El Jefe de Seguridad y funcionarios pertinentes realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	***Registro y seguimiento***		
A.12.4.1	Registro de eventos	**SI**	El Jefe de Seguridad y funcionarios pertinentes revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información. El proceso es auditado y documentado.
A.12.4.2	Protección de la información de registro	**SI**	Se implementan controles de seguridad que garanticen la protección de la información de los registros.
A.12.4.3	Registros del administrador y del operador	**SI**	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes	**SI**	El Líder del Proceso de Desarrollo Tecnológico asegura que todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.
A.12.5	***Control de software operacional***		
A.12.5.1	Instalación de *software* en los sistemas operativos	**SI**	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y *software*, que cumpla con las políticas de seguridad de la información.
A.12.6	***Gestión de la vulnerabilidad técnica***		
A.12.6.1	Gestión de las vulnerabilidades técnicas	**SI**	Existe una metodología de análisis y evaluación de riesgos sistemática y documentada.
A.12.6.2	Restricciones sobre la instalación de *software*	**SI**	La instalación de *software* es realizada sólo por el personal autorizado y con *software* probado y licenciado, además de otorgar el principio del menor privilegio. El procedimiento de instalación es documentado.
A.12.7	***Consideraciones sobre auditorías de sistemas de información***		
A.12.7.1	Controles de auditorías de sistemas de información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes acuerdan sobre las fechas de auditorías internas para los sistemas de información. El procedimiento es documentado.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	***Gestión de la seguridad de las redes***		
A.13.1.1	Controles de redes	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.1.2	Seguridad de los servicios de red	**SI**	El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
A.13.1.3	Separación en las redes	**SI**	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.13.2	***Transferencia de información***		
A.13.2.1	Políticas y procedimientos de transferencia de información	**SI**	Las políticas y procedimientos para la transferencia de la información están debidamente documentados y se aplican los mecanismos de seguridad necesarios para garantizar la confidencialidad e integridad de la información.
A.13.2.2	Acuerdos sobre transferencia de información	**SI**	Existen documentos y acuerdos sobre los algoritmos de cifrado a utilizar para la transferencia de información que garanticen su confidencialidad e integridad.
A.13.2.3	Mensajería electrónica	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	**SI**	En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	***Requisitos de seguridad de los sistemas de información***		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**SI**	Existe una política documentada que establece los requisitos relativos a la seguridad de la información para la adquisición de los nuevos equipos.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.2	***Seguridad en los procesos de desarrollo y soporte***		
A.14.2.1	Política de desarrollo seguro	**NO**	**NA**
A.14.2.2	Procedimientos de control de cambios en sistemas	**NO**	**NA**
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**SI**	Existe una documentación sobre la implementación de las nuevas aplicaciones y son sometidas a pruebas para garantizar que no haya impactos adversos en la seguridad de la información. El Líder del Proceso del Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes realizan las pruebas bajo simulaciones críticas.
A.14.2.4	Restricciones en los cambios a los paquetes de *software*	**NO**	**NA**
A.14.2.5	Principios de construcción de los sistemas seguros	**NO**	**NA**
A.14.2.6	Ambiente de desarrollo seguro	**NO**	**NA**
A.14.2.7	Desarrollo contratado externamente	**SI**	El Jefe de Seguridad y los funcionarios pertinentes evalúan el *software* desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información.
A.14.2.8	Pruebas de seguridad de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Pruebas de aceptación de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.3	Datos de prueba	**SI**	Los funcionarios pertinentes verifican que los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	***Seguridad de la información en las relaciones con los proveedores***		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**SI**	Existe una política de seguridad de la información relacionada con los proveedores.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2	***Gestión de la prestación de servicios de proveedores***		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	***Gestión de incidentes y mejoras de la seguridad de la información***		
A.16.1.1	Responsabilidades y procedimientos	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.2	Reporte de eventos de seguridad de la información	**SI**	Los funcionarios están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir.
A.16.1.3	Reporte de debilidades de seguridad de la información	**SI**	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**SI**	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.5	Respuesta a incidentes de seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**SI**	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recolección de evidencia	**SI**	Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes.
CONTROL_ID	**CONTROL**	**APLICABLE**	**IMPLEMENTACIÓN**
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	***Continuidad de seguridad de la información***		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.2	***Redundancias***		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	**SI**	En el Plan de Continuidad del Negocio se establece la instalación e infraestructura disponible para el procesamiento de información.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

Tabla 80. (Cont.). Controles aplicables de la normativa ISO 27001:2013 a la Unidad Educativa Nuestra Señora de Fátima, en base a los hallazgos realizados en las secciones precedentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.18	**CUMPLIMIENTO**		
A.18.1	***Cumplimiento de los requisitos legales y contractuales***		
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	**SI**	Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
A.18.1.2	Derechos de propiedad intelectual	**NO**	**NA**
A.18.1.3	Protección de registros	**SI**	Los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados.
A.18.1.4	Privacidad y protección de información de datos personales	**SI**	Los datos personales son almacenados y protegidos de acuerdo a las conformidades de la ley y regulaciones.
A.18.1.5	Reglamentación de controles criptográficos	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.18.2	***Revisiones de seguridad de la información***		
A.18.2.1	Revisión independiente de la seguridad de la información	**SI**	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**SI**	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información.
A.18.2.3	Revisión del cumplimiento técnico	**SI**	Exista la documentación para la realización periódica de los test de penetración y verificación de resultados e informes.

Fuente: ISO (2014). Diagramado por el Autor. (Cont.)

3.10. Plan de tratamiento de riesgos.

3.10.1. Propósito.

El propósito de la presente sección, es la de definir los controles más apropiados para el caso de estudio, basándose en los que se encuentran expuestos en la metodología MAGERIT (CSAE, 2012a).

3.10.2. Tratamiento de riesgos

Se define al tipo de tratamiento de riesgos para cumplir el objetivo de la presente propuesta, en este caso, en las tablas de implementación que se muestran más adelante, quedar señalado en cada caso donde corresponda, alguna de las siguientes connotaciones:

Tabla 81. Definición de acciones a seguir para el tratamiento del riesgo encontrado en los activos de la información

Acción	Descripción
Asumirlos (AS):	La dirección asume el riesgo ya que en este punto se encuentra por debajo de un valor aceptable. Se debe documentar y establecer que la dirección conoce y acepta estos riegos. Estos han de ser controlados y revisados periódicamente de cara a evitar que evolucionen.
Definir controles (DC)	Para reducir mediante la implantación de control que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar lo métodos para iniciar la gestión de estos.
Transferirlos a terceros (TT)	se deben evaluar las opciones y tomar acciones pertinentes en función del valor del activo y del costo de realizar esta transferencia (no solo económico, sino que, el riesgo que conlleva la transferencia del riesgo a un tercero).

Fuente: MAGERIT (CSAE, 2012a). Diagramado por el Autor.

Una estrategia para la aplicación del tratamiento del riesgo que en este documento se propone, es la referente, a que la Unidad Educativa, bajo la figura de su consejo directivo, y con el asesoramiento de la comisión técnica que se instaure para la aplicación del SGSI, definan las prioridades de aplicación de los correctivos, en este caso, se recomiendo que se comience con las situaciones menos aceptables, y que de esta manera se avance hasta alcanzar cubrir la totalidad de las acciones recomendadas.

3.10.3. Aplicabilidad de los controles de seguridad.

Los controles propuestos son aplicables en la Institución Educativa Nuestra Señora de Fátima, Los mismos, responden a la necesidad de subsanar los elementos críticos y esenciales para la instauración de un SGSI que aún no se encuentren cubiertos. A continuación se muestran los controles propuestos, mismos que se sustentan tanto en la normativa ISO 27001 (ISO, 2014) y la MAGERIT (CSAE, 2012a):

- **[D] Datos/Información**

Tabla 82. Aplicabilidad de controles en los activos "Datos/Información" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
D_BCK	Copias de Seguridad de los Sistemas de Información	**E*, A***	R_D_BCK	**A**	DC	• D. Protección de la Información • D.A Copias de seguridad de los datos • D.C Cifrado de la información	A.8.2. A.12.3.1 A.10.1.
D_CNT	Contratos	**E*, A***	R_D_CNT	**MA**	DC	• D.C Cifrado de la información • D.DS Uso de firmas electrónicas • D.I Aseguramiento de la integridad	A.10.1.
D_HAC	Historial Académico	**E*, A***	R_D_HAC	**MA**	DC	• D.C Cifrado de la información • D.DS Uso de firmas electrónicas • D.I Aseguramiento de la integridad	A.10.1.
D_HLB	Historial Laboral	**E*, A***	R_D_HLB	**MA**	DC	• D.C Cifrado de la información • D.DS Uso de firmas electrónicas • D.I Aseguramiento de la integridad	A.10.1.
D_PUB	Publicaciones	**E*, A***	R_D_PUB	**MB**	DC	• D.A Copias de Seguridad de los datos	A.12.3.1
D_LOG	Registros de Actividad	**E*, A***	R_D_LOG	**A**	DC	• D Protección de la Información • D.C Cifrado de la información	A.8.2. A.10.1.
D_SRC	Códigos Fuentes	**E*, A***	R_D_SRC	**MA**	DC	• D Protección de la Información • D.C Cifrado de la información	A.8.2. A.10.1.

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; A: Alto; MA: Muy Alto; MB: Muy Bajo); DC: Definir Controles.

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[S] Servicios**

Tabla 83. Aplicabilidad de controles en los activos "Servicios" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
S_MAI	Correo Electrónico	E*, A*	R_S_MAI	A	DC	• S.email Protección del correo electrónico S.www Protección de servicios y aplicaciones web	A.13.2.3 A.12.5.1
S_GID	Gestión de Identidades	E*, A*	R_S_GID	MA	DC	• S.A Aseguramiento de la disponibilidad S.dir Protección del directorio S.SC Se aplican perfiles de seguridad	A.17.1. A.8.2. A.9.4.3
S_INT	Servicios Internos	E*, A*	R_S_INT	MA	DC	• S.A Aseguramiento de la disponibilidad • S.dns Protección del servidor de nombres de dominio (DNS)	A.17.1. A.9.4.
S_WWW	Páginas web de acceso público	E*, A*	R_S_WWW	A	DC	• S.A Aseguramiento de la disponibilidad • S.www Protección de servicios y aplicaciones web	A.17.1. A.12.5.1

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; A: Alto; MA: Muy Alto); DC: Definir Controles.

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[SW] *Software***

Tabla 84. Aplicabilidad de controles en los activos " *Software*" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
SW_STD	*Software* Estándar	I*, E*, A*	R_SW_STD	MA	DC	SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.SC Se aplican perfiles de seguridad	▪ A.14.2. ▪ A.12.3.1
SW_MAI	*Software* para Correo Electrónico	I*, E*, A*	R_SW_MAI	MA	DC	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad	▪ A.14.2.
SW_DBS	Gestores de Bases de Datos	I*, E*, A*	R_SW_DBS	MA	DC	SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.CM Cambios (actualizaciones y mantenimiento) SW.SC Se aplican perfiles de seguridad	▪ A.14.2. ▪ A.12.3.1
SW_OFM	Ofimática	I*, E*, A*	R_SW_OFM	B	DC	SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.SC Se aplican perfiles de seguridad	▪ A.14.2. ▪ A.12.3.1
SW_AVS	*Software* de Antivirus	I*, E*, A*	R_SW_AVS	M	DC	SW Protección de las Aplicaciones Informáticas SW.SC Se aplican perfiles de seguridad	▪ A.12.2.1
SW_OPS	Sistemas Operativos	I*, E*, A*	R_SW_OPS	M	DC	SW Protección de las Aplicaciones Informáticas SW.A Copias de seguridad (backup) SW.SC Se aplican perfiles de seguridad	▪ A.14.2. ▪ A.12.3.1 ▪ A.12.2.1 ▪ A.12.5.1 ▪ A.12.6.

Amenazas: [I] De origen industrial [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; B: Bajo; MA: Muy Alto; M: Medio); DC: Definir Controles.

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[HW] *Hardware***

Tabla 85. Aplicabilidad de controles en los activos "*Hardware*" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
HW_BCK	Dispositivos de Respaldo	I*, E*, A*	R_HW_BCK	MA	DC	HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1 A.12.3.1
HW_FRW	Firewall	I*, E*, A*	R_HW_FR W	MA	DC	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad HW.SC Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_HOS	Servidores	I*, E*, A*	R_HW_HOS	MA	DC	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad HW.SC Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 * A.11.2.1
HW_PCM	Computadoras Portátiles de Uso Institucional	I*, E*, A*	R_HW_PC M	B	DC	HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PCP	Computadoras de Escritorio de Uso Institucional	I*, E*, A*	R_HW_PCP	B	DC	HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PRT	Impresoras	I*, E*, A*	R_HW_PRT	MB	AS	HW Protección de los Equipos Informáticos HW.print Reproducción de documentos	A.11.1.1 A.11.1.2 A.11.2.1
HW_ROU	Router	I*, E*, A*	R_HW_RO U	A	DC	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad HW.SC Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_SCN	Escáner	I*, E*, A*	R_HW_SCN	MB	AS	HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_SWH	Switch	I*, E*, A*	R_HW_SW H	A	DC	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad HW.SC Se aplican perfiles de eguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_WAP	Puntos de Acceso Inalámbricos	I*, E*, A*	R_HW_WA P	B	DC	HW Protección de los Equipos Informáticos HW.A Aseguramiento de la disponibilidad	A.11.1.1 A.11.1.2 A.11.2.1

Amenazas: [I] De origen industrial [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; A: Alto B: Bajo; MA: Muy Alto; MB: Muy Bajo); DC: Definir Controles AS: Asumir Control.

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[COM] Comunicaciones**

Tabla 86. Aplicabilidad de controles en los activos " Comunicaciones" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
COM_INT	Internet	E*, A*	R_COM_IN T	MA	DC	COM Protección de las Comunicaciones COM.A Aseguramiento de la disponibilidad COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	A.9.1.2 A.10.1.1 A.11.2.3 A.13.1.* A.13.2.1 A.13.2.2
COM_LAN	Red de Área Local	E*, A*	R_COM_LA N	MA	DC	COM Protección de las Comunicaciones COM.A Aseguramiento de la disponibilidad COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	A.9.1.2 A.10.1.1 A.11.2.3 A.13.1.* A.13.2.1 A.13.2.2
COM_W	Conectividad	E*, A*	R_COM_WI	M	DC	COM Protección de las Comunicaciones	A.9.1.2

IF	Inalámbrica		F			COM.A Aseguramiento de la disponibilidad COM.C Protección criptográfica de la confidencialidad de los datos intercambiados COM.wifi Seguridad Wireless(WiFi)	A.10.1.1 A.13.1.* A.13.2.1 A.13.2.2
Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; MA: Muy Alto; M: Medio); DC: Definir Controles.							

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[AUX] Equipo Auxiliar**

Tabla 87. Aplicabilidad de controles en los activos "Equipo Auxiliar" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
AUX_FBO	Fibra Óptica	I*, E*, A*	R_AUX_FBO	MA	DC	AUX.A Aseguramiento de la disponibilidad AUX.AC Climatización AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.11.2.6 ▪ A.13.2.1
AUX_RCK	Rack	I*, E*, A*	R_AUX_RCK	A	DC	AUX.A Aseguramiento de la disponibilidad AUX.AC Climatización AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_PWR	Fuente de Alimentación	I*, E*, A*	R_AUX_PWR	MA	DC	AUX.A Aseguramiento de la disponibilidad AUX.AC Climatización AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_UPS	Sistema de Alimentación Ininterrumpida	I*, E*, A*	R_AUX_UPS	A	DC	AUX.A Aseguramiento de la disponibilidad AUX.AC Climatización AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_WIR	Cableado Eléctrico	I*, E*, A*	R_AUX_WIR	MA	DC	AUX.A Aseguramiento de la disponibilidad AUX.power Suministro eléctrico AUX.wires Protección del cableado	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.11.2.6 ▪ A.13.2.1
Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; MA: Muy Alto; A: Alto); DC: Definir Controles							

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[L] Instalaciones**

Tabla 88. Aplicabilidad de controles en los activos "Instalaciones" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

COD	ACTIVO	AMENAZA	RIESGO_ID	Ri	TRAT.	SALVAGUARDA	ANEXO ISO 27001:2013
L_SIT	Oficina de Sistemas de Información y Telemática	**N*, I*, E*, A***	R_L_SIT	**A**	**AS**	L. Protección de las Instalaciones L.A Aseguramiento de la disponibilidad L.AC Control de los accesos físicos	**A.11.1. A.17.**
[N] Desastres naturales; [I] De origen industrial; [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; A: Alto); AS: Asumir Controles							

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

- **[P] Personal**

Tabla 89. Aplicabilidad de controles en los activos "Personal" Según indicaciones de la ISO/IEC 27001:2013 y la metodología MAGERIT

CÓD	ACTIVO	IMPACTO	PROB	AMENAZA	RIESGO_ID	RIESGO	CÓD
P_ADM	Administrador de Sistema	E*, A*	R_P_ADM	A	TT	PS Gestión del Personal PS.A Aseguramiento de la disponibilidad PS.AT Formación y concienciación	A.7.*
P_COM	Administrador de Comunicaciones	E*, A*	R_P_COM	MA	TT	PS Gestión del Personal PS.A Aseguramiento de la disponibilidad PS.AT Formación y concienciación	A.7.*
P_DBA	Administrador de Bases de Datos	E*, A*	R_P_DBA	MA	TT	PS Gestión del Personal PS.A Aseguramiento de la disponibilidad PS.AT Formación y concienciación	A.7.*
P_DES	Desarrolladores de *Software*	E*, A*	R_P_DES	M	TT	PS Gestión del Personal PS.A Aseguramiento de la disponibilidad PS.AT Formación y concienciación	A.7.*

Amenazas: [E] Errores y fallos no intencionados; [A] Ataques intencionados. Ri: (Riesgo; A: Alto; MA: Muy Alto; M: Medio); TT: Ransferir a terceros

Fuentes, ISO 27001:2013 (ISO, 2014) y la MAGERIT (CSAE, 2012a). Diagramado por el Autor.

3.11. Plan de Continuidad

3.11.1. Propósito.

El propósito de este **Plan de Continuidad del Negocio** (BCP) es el de asegurar que la Unidad Educativa Nuestra Señora de Fátima, se mantenga activa a pesar de eventos ajenos a los grupos de interés de la institución. Que la perdida de información o los intentos de sustraer, manipular estos elementos, no afecten la operatividad, ya que gracias al SGSI, se lograría el restablecimiento de las condiciones óptimas de funcionamiento en el menor tiempo posible.

3.11.2. Objetivos

- Servir como guía para la recuperación de desastres.

- Proveer los procedimientos y recursos para ayudar en el proceso de recuperación.
- Identificar a los responsables y notificar a la brevedad posible.
- Ayudar a evitar confusiones durante el desastre a través de documentación
- Establecer procedimientos para el almacenamiento, resguardo y recuperación de información vital para la organización.

3.11.3. Definiciones

Se adoptan como definiciones de este plan de continuidad, las descritas en el documento normativo del MAGERIT v3.0 (CSAE, 2012a, págs. 97-105).

3.11.4. Usuarios

Los usuarios que utilizaran este documento son todas aquellas que internas o externas a la organización tienen un rol en la continuidad del negocio.

3.12. Plan de Continuidad del Negocio

3.12.1. Contenido del Plan

Este plan entrara en funcionamiento cuando se genere un evento catalogado como desastre. Este, se mantendrá activo el tiempo que se requiera para que las actividades normales de la institución se desarrollen nuevamente en el emplazamiento original (En caso de haber sido desplazados por el evento), o en su defecto, que sea designado otro emplazamiento formal de funcionamiento.

En este documento se establece la composición del equipo encargado de la continuidad de la operación del negocio en la eventualidad de un incidente mayor o desastre, cuándo se activa/desactiva el plan y el orden de los procedimientos y actividades prioritarias.

3.12.2. Roles y Responsabilidades

El equipo encargado del BCP se compone de los siguientes roles:

Tabla 90. Roles del Equipo de BCP

ROL	RESPONSABILIDADES
Administrador Plan de Continuidad del Negocio (BCP Manager)	Establecer la coordinación interna/externa con la alta gerencia, empleados incluidos en el BCP, entre otros, con el fin de establecer los requerimientos y procesos para el normal funcionamiento de las actividades críticas y estratégicas. Establecer las políticas para el BCP desarrollando estrategias que complementen y soporten los riesgos y objetivos de seguridad. Asegurarse de que los procesos críticos de negocio son lo suficientemente resistentes para continuar con la operación efectiva más allá de los incidentes o desastres.
Administrador del Plan de Recuperación de Desastres	Encargarse de restaurar los procesos y servicios críticos en el tiempo estipulado después del incidente o desastre.
(BRP Manager)	Evaluar y priorizar los procesos de negocio para la restauración. Determinar los requerimientos de recuperación teniendo en cuenta la interdependencia de los procesos. Justificar las inversiones adicionales al BRP.
Administración de Evaluación Técnica (Líderes de Recuperación del estado de las redes, bases de datos y de servidores)	Trabajar conjuntamente con los otros responsables del BCP para proveer evaluación y requerimientos técnicos para una efectiva recuperación. Diseñar las herramientas de evaluación para determinar el nivel apropiado de los servicios de recuperación. Evaluar la resistencia y las capacidades de recuperación y riesgos inherentes a la infraestructura de TI. Proveer el uso de nuevas tecnologías y procesos para soportar la recuperación de desastres de TI.

Desarrollado a partir de las indicaciones de la Norma ISO 27001:2013. Diagramación por el autor.

3.12.3. Contactos Claves

A continuación, se incluye un listado en el que debe contener los contactos claves para la ejecución oportuna del BCP sea efectiva:

Tabla 91. Formato propuesto para identificación de contactos en el SG

N°	ROL	NOMBRES Y APELLIDOS	ÁREA	TELÉFONOS
1				

2				
3				
4				
5				

Creado por el Autor.

3.12.4. Activación y Desactivación del Plan

La activación define las acciones tomadas una vez exista una interrupción en los servicios críticos de la Unidad Educativa Nuestra Señora de Fátima, o en su defecto, cuando se detecten o parezca ser inminente. Se incluyes las actividades para notificar al personal de recuperación de desastres, conducir una evaluación de la interrupción y activar el BCP.

El BCP será activado cuando se presenten algunos de los siguientes eventos:

- Cuando el tipo de desastre suponga una interrupción de los servicios en más de 4 horas, dentro de ellas se encuentran:
    - Falla del *Hardware*.
    - Interrupción del fluido eléctrico o telecomunicaciones.
    - Fallas en Aplicaciones o corrupción de las bases de datos.
    - Errores humanos, sabotaje o golpes.
    - Ataque y propagación de *software* malicioso.
    - Hacking de los sistemas.
    - Desastres naturales.
- Cuando la infraestructura física de las oficinas esté dañada o no disponible en un período de 4 horas.
- Cualquier otro criterio que suponga una interrupción de los servicios críticos por tiempo indefinido.

Las personas con los roles establecidos y que sean parte de la implementación del BCP serán notificados inmediatamente. Independientemente del tipo de desastre o incidente, la vida, salud, bienestar y seguridad de las personas será la prioridad.

3.12.5. Comunicación

Los canales de comunicación se utilizarán en caso del incidente o desastre. El equipo encargado del BCP utilizará los teléfonos celulares personales y/o cualquier otro dispositivo de comunicación. De igual forma, se informará a las autoridades competentes por algún medio de comunicación y medios impresos.

3.12.6. Sitios Físicos y de Transporte

Con el fin de darle continuidad al negocio y a los procesos críticos que se ejecutan en las oficinas de Unidad Educativa Nuestra Señora de Fátima, se utilizará lo siguiente:

(En este punto, debe establecerse de manera escrita, la posible o posibles ubicaciones alternativas para reactivar las actividades, estas, de ser varias las posibilidades, deben colocarse en orden de preferencia de uso, partiendo desde la más óptima, en todo caso, se debe listar también con los servicios o facilidades con las que se dispone en cada una de las opciones.)

3.12.7. Orden de recuperación de actividades

Se realizan los procedimientos formales para las operaciones de recuperación después que haya sido activado el BCP, evaluados las interrupciones y el personal notificado.

En esta fase se implementan las estrategias para recuperar el sistema, reparar los daños y reanudar las capacidades originales a la ubicación alternativa. Después de implementada esta etapa, las actividades y procesos críticos de la sede administrativa de la institución y de las telecomunicaciones deben ser funcionales.

Para dar continuidad efectivamente en el menor tiempo posible, se deben ejecutar las siguientes actividades generales en el orden aquí establecido:

1. Identificar el lugar para dar continuidad.
2. Identificar los recursos requeridos para realizar los procedimientos de continuidad y recuperación.

3. Recuperar las copias de seguridad y los medios de instalación.
4. Recuperar el *hardware* y los sistemas operativos.
5. Recuperar el sistema desde las copias de seguridad y los medios de instalación.

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Los sistemas de información en general son importantes para garantizar la prestación de servicios por parte de una empresa, además de asegurar la integridad de los empleados clientes, dado que el empleo de herramientas tecnológicas conlleva a un riesgo de pérdida o manipulación de información sensible.

Este proyecto permitió identificar los riesgos asociados a los activos de la información de la Unidad Educativa Nuestra Señora de Fátima, así como el porcentaje de cumplimiento actual para la futura aplicación del estándar ISO 27001:2013. En este sentido, se encontró 72% de incumplimiento de los requisitos formales de la normativa ISO/IEC 27001:2013. De igual manera, se encontró un 78% de incumplimiento de los recaudos asociados al ANEXO A de la normativa ISO/IEC 27001:2013, estos son imprescindibles (Obligatorios) para lograr la certificación con el mencionado estándar.

De acuerdo a la valoración de riesgo, se encontró que la mayoría de los riesgos que se detectaron, se ubicaron dentro de la categoría de Alto y muy alto riesgo, con lo cual, se evidencia una particular urgencia para que sean asumido posturas correctivas que subsanen estos fallos de seguridad, incluso antes de la implementación del sistema de gestión de la información. Se detectó un alto nivel de vulnerabilidad de la transferencia de información debido a que en ningún caso se emplean estrategias de encriptado de la información enviada o recibida por correo electrónico. Así mismo, se observó que a pesar de que las computadoras de la institución mantienen un buen resguardo contra accesos no autorizados, el tiempo de vida actual de los mismo, incluso de los sistemas operativos instalados, llego a su fin, es decir, son máquinas con *software* y *hardware* desactualizado y fuera de garantía o de servicio técnico, por lo cual, representan una importante entrada a vulnerabilidades de la red y de todo el sistema de información.

Se detectó que la Unidad Educativa, carece de la documentación de muchos de los procesos claves para la acreditación con la normativa ISO 27001:2013, lo que demuestra que el personal directivo debe tomar medidas urgentes para conformar una comisión que garantice definir todos los procesos que se requieren documentar y que lleve a cabo esto a pesar de que en lo inmediato no sea comenzada la aplicación formal del SGSI.

Mediante el presente trabajo, quedaron manifiestos los beneficios organizacionales para la Unidad Educativa Nuestra Señora de Fátima, tras la implementación formal de un estándar internacional como la ISO/IEC 27001:2013, debido a que, en la fase de diseño de una propuesta de implementación, quedaron manifiestas los requerimientos básicos para optimizar la gestión informática de la institución. Se logró, en base a los análisis preliminares, generar una propuesta de políticas básicas de seguridad de la información que deben ser socializadas con los diversos grupos de interés para que las condiciones de seguridad se mantengan estables mientras se concreta la implementación del SGSI.

Se logró proponer un Plan de Continuidad del Negocio con el fin de mantener o restablecer en el menor tiempo posible el funcionamiento de los servicios informáticos de la institución en el supuesto caso de ocurrencia de algún evento adverso que atente contra la continuidad e integridad de los activos de la información de la institución.

4.2. Recomendaciones

- Se recomienda la conformación pertinente de un equipo multidisciplinario que se encargue del inicio de la preparación de los elementos requeridos para la implementación de un SGSI.

- Se recomienda que se manifieste la gerencia de la institución, a través de un comunicado, en el cual se exponga el compromiso de esta por el establecimiento de un SGSI y en el cual se exhorte a todos los grupos de interés a que estén al tanto de las normativas que en tal efecto se emitan

- Se recomienda que los análisis de riesgo y vulnerabilidades, sea realizada nuevamente de manera exhaustiva, en todos los elementos que se aborden a partir de los presentes resultados, para así tener una visión adecuada y real, al momento de la implementación y diseño del sistema de gestión de la información.

- Por otra parte, para obtener resultados más precisos y de actualización automática, se recomienda adquirir un *software* de gestión de riesgos para la metodología MAGERIT que permita disponer en tiempo real el cálculo de los niveles de riesgo potencial y residual, para realizar comparaciones con los niveles de riesgos aceptables.

- Se recomienda que se realice una inversión previa para sustituir o actualizar los activos informáticos de uso cotidiano para que de esta manera se logren reducir los riesgos de ataque por estas vías.

- Finalmente, se recomienda generar e impartir, con la ayuda de expertos, un proceso de capacitación dirigido a todos los grupos de interés, con la finalidad de generar conciencia sobre la importancia de la seguridad de la información en la institución

REFERENCIAS BIBLIOGRÁFICAS

Areitio, J. (2008). *Seguridad de la Información. Rees, Informática y Sistemas de Información* (ISBN: 978-84-9732-502-8 ed.). Madrid: Paraninfo.

Areitio, J. (2014). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Editorial Paraninfo.

Baccarini, D., Salm, G., & Love, P. (2004). Management of risks in information technology projects. *Industrial Management & Data Systems, 104*(4), 286-295. doi:DOI 10.1108/02635570410530702

Berumen, S., & Arriaza, K. (2008). *Evolución y desarrollo de las TIC en la economía del conocimiento.* Madrid, España: Ecobook Editorial de Economista.

Borges, L. (2016). *Gestão da Segurança da Informação. Conceitos básicos e introdução ao tema da Gestão da Segurança da Informação no contexto do digital e dos Sistemas e Tecnologias de Informação.* Informe Tecnico V. 1.1. Obtenido de https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf

Celi, E., & Díaz, R. (2017). *Políticas de seguridad de la información en función del comportamiento de los usuarios de tecnologías de la información en el sector microfinanciero de Lambayeque.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo.

Colegio N.SRA. Fatima. (S.F). *Escuela y colegio Nuestra Señora de Fátima*. Recuperado el 05 de Noviembre de 2018, de Historia: http://nsfatim6.wixsite.com/nsfatima?fbclid=IwAR03WAWYZawntpuqclHlqg00oYFWYq7er6Iu6e9os_vwloGu0r71gXbgkP8

Condori, H. (2012). *Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario.* Lima: Universidad Inca Garcilaso de la Vega. Recuperado el 06 de Noviembre de 2018, de http://repositorio.concytec.gob.pe/bitstream/CONCYTEC/115/1/condori_ah.pdf

Córdoba, A. (2015). *Diseño e implementación de un SGSI para el área de informática de la Curaduría Urbana segunda de PASTO bajo la norma ISO/IEC 27001*. Pasto: Universidad Nacional Abierta Y Distancia "UNAD".

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

CSAE. (2012b). *MAGERIT – versión 3.0. Libro II. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Catálogo de Elementos.* Madrid: CSAE.

CTIC. (2017). *ANEXO B. Guía Para la Metodología de Gestión de Riesgos.*

DAFP. (2006). *Guía Administración del Riesgo Departamento Administrativo de la Función Pública.* Bogota: DAFP.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, 4*, 92-100. doi:http://dx.doi.org/10.4236/jis.2013.42011

ESAN. (11 de Mayo de 2016). *Importancia y beneficios de contar con un Sistema de Gestión de Seguridad de Información*. Recuperado el 7 de Noviembre de 2018, de Web de la ESAN: https://www.esan.edu.pe/apuntes-empresariales/2016/05/importancia-y-beneficios-de-contar-con-un-sistema-de-gestion-de-seguridad-de-informacion/

Fache, J. (2016). *Estudio sobre la aplicación de hardening para mejorar la seguridad informática en el centro tecnico laboral de Tunja–Cotel.* Tunja: UNAD.

Gaona, K. (2013). *Aplicación de la metodología MAGERIT Para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial BRAVITO S.A. en la ciudad de Machala.* Cuenca: Universidad Politécnica Salesiana.

García, A., & Alegre, M. d. (2011). *Seguridad Informática.* Madrid, España: Ediciones Paraninfo S.A.

García, J., & Salazar, P. (2005). *Métodos de Administración y Evaluación de Riesgos.* Primavera: Universidad de Chile.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, 16-30. doi:https://doi.org/10.1016/j.cose.2004.11.002

GMV. (16 de Octubre de 2007). *Factores de exito en la implantacion de un SGSI*. Recuperado el 06 de Noviembre de 2018, de

http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1181254890620&ssbinary=true

Gómez, Á. (2014). Respuesta a incidentes de Seguridad y planes para la continuidad del Negocio. En Á. Gómez, *Enciclopedia de la Seguridad Informática.* Madrid: RA-MA, S.A. Editorial y Publicaciones.

ISO. (2005). *ISO / IEC 17799: 2005 (Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información).* ISO.

ISO. (2005). *ISO/IEC 27002* . Geneva: ISO/IEC.

ISO. (2007). *ISO/IEC 27001:2005.* Geneva: ISO.

ISO. (2014). *NTP-ISO/IEC 27001:2014. (EQV. ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR 1 Information technology -- Security techniques --Information security management systems – Requirements).* Lima: NTP.

ISO. (2018). *ISO/IEC 27000:2018.* Geneva: ISO.

ISO27000.es. (2015). *Sistema de Gestión de la Seguridad de la Información.* Recuperado el 07 de Noviembre de 2018, de Web de ISO27000.es: http://www.iso27000.es/download/doc_sgsi_all.pdf

iso27000.es. (s.f). *Glosario*. Recuperado el 10 de Noviembre de 2018, de Web de ISO27000.es: http://www.iso27000.es/glosario.html

ISOTools. (8 de Septimbre de 2015). *Beneficios de aplicar la norma ISO 27001*. Recuperado el 6 de Noviembre de 2018, de SIOTools: https://www.isotools.org/2015/09/08/beneficios-de-aplicar-la-norma-iso-27001/

ISOTools. (30 de Marzo de 2015). *ISO 27001: Los activos de información*. Recuperado el 2 de noviembre de 2018, de Blow de SGSI, de ISOTools: https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

ISOTools. (14 de Septiembre de 2017). *ISO 27001 ¿Cómo se debe realizar la clasificación de la información?* Obtenido de Blog de SGSI de ISOTools: https://www.pmg-ssi.com/2017/09/iso-27001-clasificacion-de-la-informacion-2/

itSMF. (2015). *Para Além do ITIL: Tradição e Novas Tendências | 12ª Conferência Anual itSMF Portugal '15*. Recuperado el 06 de Noviembre de 2018, de itSMF Portugal: https://www.itsmf.pt/Default.aspx?tabid=212&language=pt-PT

Joya, J., & Sacristán, C. (2017). *Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para la Empresa Javesalud I.P.S.* Bogotá: Universidad Católica De Colombia. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/15405/1/Proyecto%20Final%20Especializacion%20Seguridad%20de%20la%20Informacion.pdf

Konzen, M. (2013). *Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança.* Santa Maria: Universidade Federal De Santa Maria.

Lichtenstein, S. (1996). Factors in the selection of a risk assessment method. *Information Management & Computer Security*, *4*(4), 20-25. doi:https://doi.org/10.1108/09685229610130503

Marciano, J., & Marques, M. (2006). O enfoque social da segurança da informação. *Ci. Inf., Brasília, 35*(3), 89-98.

Mataracioglu, T. (2017). Proposal for the Next Version of the ISO/IEC 27001 Standard. *ISACA Journal, 4*, 1-5.

Mayorga, T. (2014). *Seguridad informática y la relación en la utilización de internet como herramienta de apoyo en la formación de niños, niñas y adolescentes de educación inicial y básica del Centro Educativo la Pradera.* Ambato: Universidad técnica de Ambato.

Mendoza, M. (6 de Noviembre de 2017). *6 consideraciones previas a la implementación del SGSI*. Obtenido de Web de ESET: https://www.welivesecurity.com/la-es/2017/11/06/consideraciones-implementacion-del-sgsi/

Mikov, D. (2014). Analisys of methods and tools which are used in the various stages of information security risk assessment. *Voprosy kiberbezopasnosti, 4*(7), 49-54.

NTP. (2007). *EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.* Lima: NTP.

Odegov, S. (2013). *Methods of reducing the risk of information security of cloud services based on quantifying the levels of security and optimizing the composition of resources.* San Petersburgo: Universidad Nacional de Investigación de San

Petersburgo de Tecnologías de la Información, Mecánica y Óptica. Obtenido de http://tekhnosfera.com/metodika-snizheniya-riskov-informatsionnoy-bezopasnosti-oblachnyh-servisov-na-osnove-kvantifitsirovaniya-urovney-zaschisc

Perafán, K. (2015). *Diagnostico y mejoras de la situación actual al proceso: Gestión de Seguridad de la Información de la Universidad Autónoma de Occidente*. Santiago De Cali: Universidad Autónoma De Occidente.

Pérez, A. (04 de Noviembre de 2018). *Riesgo, Amenaza y Vulnerabilidad (ISO 27001)*. Obtenido de EQ2B Consulting: https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/

Prats, E. (., Buxarrais, M., & Tey, A. (2014). *Ética de la Información.* Barcelona, España: UOC Editorial.

Project Management Institute. (2017). *Guía del PMBOK* (Sexta ed.). Newtown Square: Project Management Institute, Inc.

Ramírez, A. (2014). *Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013.* Barcelona: Universitat Autonoma de Barcelona.

Ramos, B. (2015). *Avances en criptología y seguridad de la información* (Segunda ed.). Madrid: Ediciones Díaz de Santos.

Romero, C. (2014). *Transmisión de información por medios convencionales e informáticos.* Madrid, España: IC Editorial.

Seclén, J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. Lima: Universidad Nacional Mayor De San Marcos. Recuperado el 06 de Noviembre de 2018, de http://200.62.146.31/bitstream/handle/cybertesis/4884/Seclen_aj.pdf?sequence=1&isAllowed=y

Steinberg, R., Everson, M., Martens, F., & Nottingham, L. (2004). *Enterprise Risk Management –Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission (COSO).* COSO.

Suárez, D., & Ávila, A. (2015). Una forma de interpretar la seguridad informática. *Journal of Engineering and Technology*, *4*(2), 16-23.

Tarazona, C. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*, *28*(84), 137-146. Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/965

Torrent-Sellens, J. (2008). TIC, conocimiento y actividad económica: hacia la economía del conocimiento. En S. Berumen, & K. Arraiza, *Evolución y desarrollo de las TIC en la economía del conocimiento* (págs. 35-74). Madrid: Ecobook- Editorial del Economista.

Torres, E. (2015). *Políticas de Seguridad de la información basado en la Norma ISO/ICE27002:2013 para la Dirección de Tecnologíasde Información y Comunicación de la Universidad Técnica de Ambato.* Ambato: Universidad Técnica De Ambato.

VHGroup. (2018). *Compliance y SGSI.* Recuperado el 06 de Noviembre de 2018, de VHGroup: https://www.vhgroup.net/blog/portfolio-item/compliance-sgsi#toggle-id-6

Vybornova, O. (2015). Ontological model of the process of risk assessment. *Vestn. Astrakhan State Technical Univ. Ser. Management, Computer Sciences and Informatics*(2), 97-102.

ANEXOS

Anexo 1. Descriptores de las tablas de valoración de riesgo. Recuperado de (CSAE, 2012b, págs. 19-23)

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE