UNIVERSIDAD DON BOSCO

VICERRECTORÍA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACIÓN

"ANÁLISIS GAP DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN DE LAS UNIVERSIDADES ACREDITADAS POR LA CdA EN EL SALVADOR CON BASE A LOS REQUERIMIENTOS DE LA ISO 27001:2013"

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTIÓN DE RIESGOS INFORMÁTICOS

ASESOR:

Mg. RENÉ ARTURO ANGULO ARRIAZA

PRESENTADO POR:

RONALD ALEXIS CHACHAGUA

DAVID JONATHAN MENJÍVAR

ELISA MARÍA NAVES

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Agosto 2018

Índice

Introducción

En la actualidad, la información en conjunto con todos los procesos y sistemas que hacen uso de ella son activos de gran importancia en una organización. Por tal razón, los pilares de la seguridad confidencialidad, integridad y disponibilidad de información son esenciales para que las organizaciones tengan niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial deseados, es por esto que es muy importante el tener un nivel adecuado de seguridad de la información utilizada en la organización, para que se cumplan los objetivos estratégicos de la organización.

La cantidad de estudiantes por Universidad en el Salvador varía desde 50 hasta aproximadamente 50,000 en las diferentes carreras técnicas, de grado y postgrado ofrecidas en cada una de estas, lo que indica que la cantidad de información sensible de estudiantes y empleados en estas instituciones puede llegar a ser bastante grande y para garantizar la protección y cumplimiento de los objetivos de negocio es de suma importancia que las instituciones de educación superior poseen implementados controles de seguridad de información en todos sus procesos.

En El Salvador actualmente existen aproximadamente veinticuatro Universidades, once institutos especializados y seis Institutos Tecnológicos, de los cuales nueve Universidades y cuatro Institutos Especializados se encuentran acreditados por CdA.

Se selecciona el estudio a las Universidades acreditadas por la CdA sobre el nivel de seguridad de información implementado con respecto a los requerimientos de un Sistema de Gestión de la Seguridad de la Información planteados en la Norma ISO 27001:2013, porque se desconoce de una manera oficial los procedimientos de Seguridad de la Información que las instituciones educativas de nivel superior en El Salvador realizan.

1. Metodología de trabajo

1.1. Objetivo General y específicos

1.1.1 General

- ✓ Determinar el nivel de madurez actual de las universidades acreditadas por la CdA en El Salvador según los requerimientos definidos en la norma ISO 27001:2013.

1.1.2 Específicos

- ✓ Identificar los controles de Seguridad de Información que cumplen o dan tratamiento las universidades acreditadas por la CdA en El Salvador.
- ✓ Comparar los controles utilizados por las universidades contra los requerimientos especificados en la norma ISO 27001:2013.
- ✓ Mostrar los niveles de madurez que presentan las universidades acreditadas por la CdA en El Salvador con respecto a los requerimientos de la norma ISO 27001:2013.
- ✓ Determinar la brecha entre el nivel de madurez obtenido para las universidades acreditadas por la CdA en El Salvador con respeto a lo requerido en la norma ISO 27001:2013.

1.2. Planteamiento del Problema

Según el estudio de la revista Eset Security Report Latinoamérica 2016, únicamente el 42% de las empresas que participaron en el estudio confirman que sus normativas se encuentren alineadas con respecto a la norma ISO 27001, ITIL, COBIT o bien alguna legislación obligatoria; y siendo la información el activo más importante en las empresas el porcentaje de empresas que se basan en alguna norma o buena práctica para la implementación de controles de seguridad es muy bajo, Lo cual es alarmante.

Y a pesar de que tanto a nivel de Latinoamérica como en El Salvador las empresas comienzan a realizar inversiones en la seguridad de la información, la seguridad informática aún se encuentra en un nivel bastante bajo en la región.

Las Universidades son empresas que a pesar de dedicarse al rubro de servicio educacional deben de considerar la seguridad de la información como uno de sus elementos básicos dentro de cada uno de los procesos que se realizan en las mismas ya que son empresas como cualquier otra que poseen contacto con empleados de

diferentes áreas, proveedores, junta directiva, clientes, etc., manejando información de diversas áreas de interés y debiendo de protegerla de la manera más adecuada posible.

Sin embargo, al pensar en seguridad de la información se deja olvidado el sector de servicios educacionales es por esto que es importante determinar el nivel de madurez de seguridad de la información que poseen las Universidades acreditadas por la CdA en el país.

1.3. Hipótesis por responder en la investigación

Las Universidades acreditadas por la CDA en El Salvador no cuentan con un sistema de gestión de la seguridad de la información o se encuentran en un nivel de seguridad de la información bajo comparado con los requerimientos de la ISO27001:2013.

2. Metodología de la Investigación

1.1. Tipo de Investigación

El método a utilizar es descriptivo – cuantitativo, para el cual la fuente de información fueron los encargados de las áreas de informática de las Universidades quienes se encargan del control y la toma de medidas de seguridad en cada una de las instituciones, la información se obtendrá a través de técnicas de encuesta, permitiendo determinar el estado de la seguridad de información en las instituciones.

En la investigación se evalúa el nivel de seguridad de la información en base a los requerimientos y controles planteados en la ISO 27001:2013.

1.2. Diseño de la investigación

El diseño de la investigación a utilizar es no experimental, esto debido a que es caracterizado por ser de tipo Transversal y descriptivo.

En la investigación no se realizará ningún tipo de manipulación de las variables a estudiar. Las condiciones de estudio no se verán afectadas y únicamente se realizará una recolección de información del estado actual de la seguridad de la información en las universidades acreditadas por la CdA en El Salvador.

1.3. Unidad de análisis

El personal técnico o jefe de sistemas de las Instituciones educativas de nivel superior acreditadas por la CdA en El Salvador son las unidades de estudio que servirán para llevar a cabo el desarrollo del trabajo de investigación.

1.4. Población y muestra

La población a la que se dirigirá la investigación son las trece universidades que están acreditadas por la CdA en nuestro país. Para esto se utilizó una muestra de nueve del total de trece Universidades, tomando en consideración las universidades que tienen más tiempo de poseer dicha acreditación y disponibilidad de proporcionar a los investigadores la información necesaria para realizar la labor planteada.

1.5. Instrumento

El instrumento a utilizar para la recolección de la información será una encuesta cerrada, basada en el modelo o escala de Likert, en la que el encuestado deberá seleccionar de entre cinco opciones diferentes, que indicarán el nivel de conocimiento e implementación que más se adecue según el control evaluado.

La encuesta es un medio destinado a recopilar información de una o varias personas

cuyo conocimiento y opiniones son de interés para el investigador. Dentro de una encuesta, es necesario definir reglas o métricas que nos permitan obtener la información de forma según lo definido, para ello, se debe crear una encuesta sistemática en la que se obtengan los mismos tipos de resultados independientemente de quien realice la evaluación.

Dentro de nuestra investigación, la encuesta estará conformada con trece secciones que corresponden a las secciones definidas en la norma ISO 27001:2013, en la que cada sección, contendrá un número cerrado de preguntas que buscan conocer el nivel de implementación de los controles que se incluyen en la norma. Cada pregunta deberá ser respondida de forma cerrada, es decir, el encuestado posee cinco diferentes opciones para determinar el nivel de implementación del control referente a la pregunta.

Nivel de implementación	**Valor**
Óptimo	5
Alto	4
Moderado	3
Poco	2
Nulo	1

Tabla 1- Opciones de respuesta de la encuesta

Para cada respuesta dentro de la encuesta, se le asignará un valor entre uno y cinco que corresponderá al nivel de implementación según el control o pregunta generada. Al totalizar todos estos valores, se determinará el nivel de implementación a la que institución en evaluación corresponde. Los niveles se muestran en la siguiente tabla.

Nivel de implementación				
Nulo	Poco	Moderado	Alto	Óptimo
Nivel bajo		Nivel medio	Nivel alto	

Tabla 2- Niveles de implementación según Likert

Para determinar el nivel de implementación al que corresponde una institución, se deberá totalizar las respuestas obtenidas, según el valor de cada respuesta, es decir, si en una pregunta, la respuesta es “Óptimo”, se la asignará un valor de 5 a dicha respuesta, o bien, si responde con un “nula”, se asigna un valor de 1. Dentro de la

encuesta, existen 13 secciones que totalizan 106 preguntas, que al dan una valorización máxima por respuestas de 530 puntos. En la siguiente tabla, se describe la sección de la encuesta, junto con su cantidad de preguntas y los puntos máximos que estas podrían generar.

Sección de la encuesta	**Cantidad de preguntas**	**Puntos máximos por respuesta**
Política de Seguridad	3	15
Organización de la Seguridad de la Información	7	35
Seguridad de los Recursos Humanos	6	30
Gestión de activos	8	40
Control de Accesos	13	65
Cifrado	2	10
Seguridad Física y Ambiental	10	50
Seguridad en la Operativa	13	65
Seguridad en las Telecomunicaciones	16	80
Desarrollo y Mantenimiento de los sistemas informáticos	9	45
Gestión de Incidentes de Seguridad	6	30
Gestión de la Continuidad del Negocio	6	30
Cumplimiento regulatorio	5	25
Total	**104**	**520**

Tabla 3 – Puntos totales de la encuesta

Para obtener los resultados de una encuesta, se sumarán los valores generados por las 104 preguntas, teniendo un valor máximo de 520 puntos, en el caso que todas las

respuestas fueran marcadas como “Óptimo”, y un valor mínimo de 104 puntos si todas ellas obtuvieran respuesta de “nulo”.

Finalmente, para determinar el nivel de implementación, se ha definido que para los resultados que oscilen en el rango de [0% al 40%] corresponderán a un nivel de implementación bajo, del]40% al 70%] un nivel medio y del]70% al 100%] corresponde al nivel alto de implementación. En la siguiente tabla, se describen los porcentajes a utilizar y su respectivo rango de valores.

Nivel de implementación	Porcentaje	Rango de valores
Nivel alto	]70% - 100%]	[365 - 520]
Nivel medio	]40% - 70%]	[209 - 364]
Nivel bajo	[0% - 40%]	[0 - 208]

Tabla 4- Niveles y rangos según Likert

La encuesta nos brindará la posibilidad de evaluar y medir el nivel de implementación que las diferentes universidades que participaron en la investigación poseen en cuanto a los requerimientos detallados en la norma.

Así mismo, se realizará un análisis por sección que englobe el conjunto de preguntas realizadas en la norma, esto con el fin de tener un mejor análisis para evaluar puntualmente cada subconjunto de preguntas realizadas.

Se definen para cada sección de preguntas, un rango valores máximo y mínimo que se acopla al mismo intervalo definido para la evaluación global, en la que, por sección, se conocerá el nivel de implementación por las respuestas brindadas por el encuestado.

Se detalla la tabla de rangos de valores para cada sección de la encuesta.

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Política de Seguridad	3	15	Nivel alto	]70% - 100%]	[11-15]
			Nivel medio	]40% - 70%]	[7-10]
			Nivel bajo	[0% - 40%]	[0 - 6]
Organización de la Seguridad de la Información	7	35	Nivel alto	]70% - 100%]	[26-35]
			Nivel medio	]40% - 70%]	[15-25]
			Nivel bajo	[0% - 40%]	[0 - 14]
Seguridad de los Recursos Humanos	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]
Gestión de activos	8	40	Nivel alto	]70% - 100%]	[29-40]

			Nivel medio	]40% - 70%]	[17-28]
			Nivel bajo	[0% - 40%]	[0 - 16]
Control de Accesos	13	65	Nivel alto	]70% - 100%]	[47-65]
			Nivel medio	]40% - 70%]	[27-46]
			Nivel bajo	[0% - 40%]	[0 - 26]
Cifrado	2	10	Nivel alto	]70% - 100%]	[8-10]
			Nivel medio	]40% - 70%]	[5-7]
			Nivel bajo	[0% - 40%]	[0 - 4]
Seguridad Física y Ambiental	10	50	Nivel alto	]70% - 100%]	[36-50]
			Nivel medio	]40% - 70%]	[21-35]
			Nivel bajo	[0% - 40%]	[0 - 20]
Seguridad en la Operativa	13	65	Nivel alto	]70% - 100%]	[47-65]
			Nivel medio	]40% - 70%]	[27-46]
			Nivel bajo	[0% - 40%]	[0 - 26]
Seguridad en las Telecomunicaciones	16	80	Nivel alto	]70% - 100%]	[57-80]
			Nivel medio	]40% - 70%]	[33-56]
			Nivel bajo	[0% - 40%]	[0 - 32]
Desarrollo y Mantenimiento de los sistemas informáticos	9	45	Nivel alto	]70% - 100%]	[33-45]
			Nivel medio	]40% - 70%]	[19-32]
			Nivel bajo	[0% - 40%]	[0 - 18]
Gestión de Incidentes de Seguridad	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]
Gestión de la Continuidad del Negocio	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]
Cumplimiento regulatorio	5	25	Nivel alto	]70% - 100%]	[19-25]
			Nivel medio	]40% - 70%]	[11-18]
			Nivel bajo	[0% - 40%]	[0 - 10]
Total	**104**	**520**			

Tabla 5- Niveles y rangos por sección según Likert

2.5.1. Encuesta

ANÁLISIS GAP DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN DE LAS UNIVERSIDADES ACREDITADAS POR LA CdA EN EL SALVADOR CON BASE A LOS REQUERIMIENTOS DE LA ISO 27001:2013

Encuesta de estudio

Encuestado: _____ Fecha: ____/____/____

Universidad: _____

Cargo desempeñado: _____

A continuación, encontrará una serie de preguntas destinadas a conocer el nivel de Seguridad de la Información que su universidad posee realizando preguntas, separadas por categorías según lo especificado en la norma ISO 27001:2013. Mediante esto queremos conocer cómo se maneja la información dentro de su institución.

SECCIÓN 1: IMPLEMENTACIÓN DE REQUERIMIENTOS ISO 27001:2013

Evalué el nivel de implementación en los temas presentados a continuación en una escala de 1 a 5, la cual mide el nivel en que se encuentra implementado el control requerido por la norma, donde 1 significa nada o nulo, 2 es poco, 3 es moderado, 4 es alto y 5 es óptimo.

Por favor seleccione la alternativa que más se parece a su respuesta.

Política de Seguridad

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿En qué nivel considera que se encuentra su política de seguridad de la información?	1	2	3	4	5
2. ¿Con qué frecuencia se actualiza la política de seguridad de la información?	1	2	3	4	5
3. ¿Cómo califica el nivel de conocimiento que poseen los empleados de su institución con respecto a la política de seguridad de la información?	1	2	3	4	5

Organización de la Seguridad de la Información

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Cómo califica la asignación de roles y responsabilidades para la seguridad de la información?	1	2	3	4	5
2. ¿Cómo califica la asignación de roles y responsabilidades con respecto a la recepción, almacenamiento, modificación y eliminación de la información en su institución?	1	2	3	4	5
3. ¿Qué tanto conoce los contactos a los que se le debe de comunicar en caso de un evento de seguridad?	1	2	3	4	5
4. ¿Qué tan implementado tiene el proceso de firma de acuerdos de confidencialidad con empleados, proveedores y otros terceros?	1	2	3	4	5
5. ¿Con qué frecuencia se hace el análisis de riesgo sobre nuevos proyectos a implementarse?	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
6. ¿En qué nivel considera que se encuentra la seguridad en los dispositivos móviles?	1	2	3	4	5
7. ¿En qué nivel considera que se encuentra la seguridad en las conexiones de trabajo desde fuera de las instalaciones de su institución?	1	2	3	4	5

Seguridad de los Recursos Humanos

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Cómo clasifica el proceso de verificación de antecedentes para nuevos empleados y proveedores?	1	2	3	4	5
2. ¿Qué tan clara considera los términos y condiciones plasmados en los contratos con respecto a las funciones y responsabilidades con respecto a empleados, proveedores y otros terceros?	1	2	3	4	5
3. ¿Qué tanto se les exige a los empleados, proveedores y otros terceros el cumplimiento de la seguridad con respecto a las políticas y procedimientos establecidos en su institución?	1	2	3	4	5
4. ¿Con qué frecuencia se someten los empleados, proveedores y otros terceros a capacitaciones en concientización de seguridad adecuada a su función dentro de la institución?	1	2	3	4	5
5. ¿Cómo considera que es el proceso disciplinario hacia los empleados, proveedores y otros terceros a incumplimientos de la política de seguridad?	1	2	3	4	5
6. ¿Cómo califica el nivel de conocimiento de los empleados, proveedores y otros terceros con respecto a las condiciones de finalización de contrato?	1	2	3	4	5

Gestión de activos

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. Califique el nivel de actualización de inventario de activos en la institución.	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
2. ¿A qué nivel se encuentran identificados los responsables de los activos de datos, software, equipos y servicios?	1	2	3	4	5
3. ¿Qué tan eficiente es el procedimiento de clasificación de activos de datos, software, equipos y servicios?	1	2	3	4	5
4. ¿Cómo califica el nivel del etiquetado y clasificación de los activos?	1	2	3	4	5
5. ¿Cómo considera que es el cumplimiento de los controles de seguridad para la manipulación y tratamiento de los activos de información?	1	2	3	4	5
6. ¿Qué tan implementada está la política de manejo de medios de almacenamiento de información electrónica en su institución?	1	2	3	4	5
7. ¿Qué tan desarrollado está el procedimiento de eliminación de medios de almacenamiento de información electrónica en su institución?	1	2	3	4	5
8. ¿Cómo considera la seguridad en el transporte de activos fuera de las instalaciones de la institución?	1	2	3	4	5

Control de Accesos

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Qué tan segura es su política de control de accesos?	1	2	3	4	5
2. ¿Cómo evalúa el control de accesos y privilegios de los usuarios a las redes y servicios asociados?	1	2	3	4	5
3. ¿Qué tan eficientemente trabajan sus procedimientos de asignación de servicios de acceso a los sistemas y servicios de información?	1	2	3	4	5
4. ¿Qué tan eficientemente funcionan los procedimientos en toda la etapa del ciclo de vida de los usuarios en la empresa?	1	2	3	4	5
5. ¿Cómo evalúa la forma en la que se manejan los usuarios con accesos privilegiados los cuales podrían saltar o anular la eficacia de los controles del sistema?	1	2	3	4	5
6. ¿Qué tan eficientes son los procedimientos de altas y bajas de los usuarios?	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
7. ¿Cómo evalúa el proceso de asignación y revocación de derechos de acceso a los usuarios?	1	2	3	4	5
8. Evalúe el proceso de la asignación de información confidencial para la autenticación.	1	2	3	4	5
9. Evalúe el nivel de conciencia de los usuarios sobre sus responsabilidades en temas de control de acceso, contraseñas y equipos asignados.	1	2	3	4	5
10. ¿A qué nivel se cumple la política de escritorio y monitores limpios?	1	2	3	4	5
11. ¿Cómo evalúa la protección de documentos, medios informáticos, datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizada?	1	2	3	4	5
12. ¿Qué tan efectivo es la restricción de acceso al código fuente de las aplicaciones software a usuarios no autorizados?	1	2	3	4	5
13. ¿Qué tan seguro es su sistema de login a los sistemas de información?	1	2	3	4	5

Cifrado

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿En qué nivel considera que se encuentra el desarrollo e implementación de una política que regule el uso de controles criptográficos para la protección de la información?	1	2	3	4	5
2. ¿Cómo califica su política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida?	1	2	3	4	5

Seguridad Física y Ambiental

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Qué tan seguro es el perímetro de seguridad física establecido?	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
2. ¿Cuán efectivos son los controles de entrada para protegerse frente al acceso de personal no autorizado?	1	2	3	4	5
3. ¿Cómo considera la protección de las instalaciones ante eventos naturales?	1	2	3	4	5
4. ¿Cómo evalúa el nivel de aislamiento que existe entre las áreas de carga y expedición?	1	2	3	4	5
5. ¿Qué tan buena es la ubicación de los equipos para minimizar los accesos innecesarios?	1	2	3	4	5
6. Evalúe las protecciones frente a fallos en la alimentación eléctrica	1	2	3	4	5
7. Evalúe la seguridad en el cableado frente a daños e intercepciones	1	2	3	4	5
8. ¿Cómo clasifica el nivel de integridad y disponibilidad de los equipos?	1	2	3	4	5
9. ¿Cómo evalúa el nivel de seguridad en los equipos retirados o ubicados exteriormente?	1	2	3	4	5
10. ¿Cuál es el nivel de seguridad en equipos móviles?	1	2	3	4	5

Seguridad en la Operativa

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. Clasifique el nivel de documentación de los procedimientos operativos y la disposición de estos a todos los usuarios que los necesiten.	1	2	3	4	5
2. ¿En qué nivel considera que se encuentra implementado el procedimiento de control de los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información?	1	2	3	4	5
3. Califique el nivel de desarrollo del monitoreo y ajuste del uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.	1	2	3	4	5
4. ¿Qué tan implementado poseen la separación de los entornos de desarrollo, pruebas y operacionales para reducir los	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
riesgos de acceso o de cambios no autorizados en el entorno operacional?					
5. ¿Cuán implementados considera que se encuentran los controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios?	1	2	3	4	5
6. Califique la política de backup sobre realización de pruebas de las copias de la información, del software y de las imágenes del sistema.	1	2	3	4	5
7. ¿Con que frecuencia se realiza una revisión de los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información?	1	2	3	4	5
8. ¿En qué nivel se encuentra el procedimiento de protección contra posibles alteraciones y accesos no autorizados a la información de los registros?	1	2	3	4	5
9. Califique la frecuencia con la cual se valida el registro de las actividades del administrador y del operador del sistema y los registros asociados.	1	2	3	4	5
10. ¿Cómo califica el nivel de sincronización de los relojes de todos los sistemas de procesamiento de información pertinentes?	1	2	3	4	5
11. ¿Qué tan implementado se encuentra el procedimiento para controlar la instalación de software en sistemas operacionales?	1	2	3	4	5
12. ¿Cómo clasifica el procedimiento de detección y mitigación de vulnerabilidades técnicas de los sistemas de información?	1	2	3	4	5
13. Indique el nivel en el cual se encuentra el procedimiento de control y restricción de instalación de software por parte de los usuarios.	1	2	3	4	5

Seguridad en las Telecomunicaciones

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Qué tan efectiva es la documentación de los procedimientos operativos identificados en la política de seguridad?	1	2	3	4	5

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
2. ¿Qué tan correcta es la asignación de responsabilidades establecidas para controlar los cambios en equipos?	1	2	3	4	5
3. Evalúe las responsabilidades establecidas para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	1	2	3	4	5
4. ¿Cómo evalúa el método que emplea su institución para reducir el mal uso accidental o deliberado de los sistemas?	1	2	3	4	5
5. ¿Cómo considera que es la separación de los entornos de desarrollo y producción en su institución?	1	2	3	4	5
6. ¿Cómo evalúa su gestión de nuevos sistemas de información y software, incluyendo actualizaciones, nuevas versiones, y controles contra software maligno?	1	2	3	4	5
7. ¿Qué tan confiables son las copias de backup de la información esencial para el negocio?	1	2	3	4	5
8. Evalúe la confiabilidad de los logs para las actividades realizadas por los operadores y administradores, así como los que son para fallos detectados	1	2	3	4	5
9. ¿Cómo considera que son sus controles en las redes?	1	2	3	4	5
10. ¿Qué tan efectivos son sus controles establecidos para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	1	2	3	4	5
11. ¿Qué tan confiable es su procedimiento establecido para la eliminación de medios informáticos que contengan información sensible?	1	2	3	4	5
12. ¿Qué tan seguro es el medio de almacenamiento de documentación de los sistemas?	1	2	3	4	5
13. Evalúe la seguridad de los medios en el tránsito de la información	1	2	3	4	5
14. ¿Qué tan seguro es su proceso de comercio electrónico?	1	2	3	4	5
15. ¿Cómo considera que son sus medidas establecidas e implantadas para proteger la confidencialidad e integridad de la información publicada?	1	2	3	4	5
16. ¿Qué tan efectivas son las medidas de seguridad en las transacciones en línea?	1	2	3	4	5

Desarrollo y Mantenimiento de los sistemas informáticos

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Se desarrolla y da mantenimiento a los sistemas informáticos en la institución?	1	2	3	4	5
2. ¿Cuán implementada esta la seguridad de la información en los sistemas de información?	1	2	3	4	5
3. ¿Existe seguridad implementada en las aplicaciones utilizadas?	1	2	3	4	5
4. ¿Se implementan controles criptográficos para el manejo de información?	1	2	3	4	5
5. ¿Cuenta con seguridad implementada en los ficheros de los sistemas?	1	2	3	4	5
6. ¿Se implementa seguridad en los procesos de desarrollo de software, testeo y soporte del mismo?	1	2	3	4	5
7. ¿Existen controles de controles de seguridad para los resultados de los sistemas?	1	2	3	4	5
8. ¿Se implementa un control de cambios en los sistemas de información?	1	2	3	4	5
9. ¿Cuán seguido se controlan las vulnerabilidades de los equipos y sistemas?	1	2	3	4	5

Gestión de Incidentes de Seguridad

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Cuán comprometida esta la institución con el manejo de incidentes de seguridad?	1	2	3	4	5
2. ¿Con que frecuencia se comunican los eventos de seguridad?	1	2	3	4	5
3. ¿Con que frecuencia se comunican y dan tratamiento a las debilidades de seguridad?	1	2	3	4	5
4. ¿Cuánto conocimiento existe sobre las responsabilidades y actores que ejercen ante un incidente de seguridad?	1	2	3	4	5
5. ¿Cuenta con un procedimiento formal ante incidentes de seguridad?	1	2	3	4	5
6. ¿Implementa y funciona su gestión de incidentes de seguridad?	1	2	3	4	5

Gestión de la Continuidad del Negocio

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Cuenta su institución con un proceso de continuidad del negocio?	1	2	3	4	5
2. ¿Qué tan eficiente es su plan de continuidad del negocio y análisis de impacto a los sistemas o procesos críticos de la institución?	1	2	3	4	5
3. ¿Existe un diseño, redacción e implementación de planes de continuidad del negocio?	1	2	3	4	5
4. ¿Cuenta con una planificación para la continuidad del negocio?	1	2	3	4	5
5. ¿Qué tan frecuente se prueban, dan mantenimiento y reevalúan los planes de continuidad del negocio?	1	2	3	4	5
6. ¿Cuentan con procesos de auditoria por parte de entidades internas o externas que revisen la continuidad del negocio?	1	2	3	4	5

Cumplimiento regulatorio

Tema	Nivel de implementación				
	Nulo	Poco	Moderado	Alto	Óptimo
1. ¿Se cuenta con un requerimiento con el cumplimiento con la legislación por parte de los sistemas?	1	2	3	4	5
2. ¿Se implementan controles para el resguardo de la propiedad intelectual?	1	2	3	4	5
3. ¿Existe resguardo de los registros de la institución?	1	2	3	4	5
4. ¿Con que frecuencia se revisa la política de seguridad y de conformidad técnica?	1	2	3	4	5
5. ¿Existen consideraciones sobre las auditorias de los sistemas?	1	2	3	4	5

2.6. Recolección de la información

Se utilizó información contenida en libros, documentales, tesis, páginas web, entre otros, esto permitió enriquecer y profundizar en los aspectos más importantes sobre la problemática en estudio, siendo principalmente la ISO27001:2013 la principal fuente bibliográfica consultada.

3. Marco Teórico

3.1. La Información en las organizaciones

La información es un conjunto de datos que al ser procesados de manera ordenada crean un mensaje que al ser transmitido puede tener influencia en la toma de decisiones.

Con el paso del tiempo las organizaciones han ido reconociendo la importancia de administrar y asegurar sus activos más importantes y la información se ha colocado en uno de los primeros lugares como uno de los principales activos que poseen las empresas actualmente.

El conocimiento y la información son los insumos fundamentales para el logro de la productividad; la cual es una medida de la eficiencia del empleo, de los recursos para generar bienes y servicios; por lo tanto, es la relación del valor de los resultados con el costo de los insumos.

Por todo lo antes mencionado es importante que las organizaciones posean una correcta gestión de la misma. La gestión de la información tiene elementos básicos como el acceso, evaluación, administración, organización, seguridad, filtrado y distribución de la información de tal manera que la información puede ser útil para el usuario final.

3.1.1. Gestión de la Información

La gestión de la información se define como la explotación de la información para la consecución de los objetivos de una entidad. Su creación, adquisición, procesamiento y difusión.

Hoy en día un bien intangible como es la información es capaz de generar resultados visibles y lograr el cumplimiento de los objetivos para una organización. La información es un objeto de mercadeo, se compra y se vende, y puede proporcionar a aquellos que la poseen beneficios reales y efectivos.

Esto es tan evidente que los líderes de las empresas de gran renombre han diseñado políticas que les permitan gestionar este recurso en beneficio de los intereses de la organización. Sin embargo, la gestión de información es un campo ciertamente amplio en el que es fácil perderse debido a que la cantidad de soluciones y aplicaciones que han surgido a lo largo de los últimos años se han encargado de dificultar el panorama, es por esto que en ocasiones ante esta confusión los líderes empresariales simplifican la gestión de la información con la incorporación de tecnologías de la información de última generación, que si bien tienen una importancia fundamental como herramientas para la gestión de la información en si misma sólo pueden considerarse un soporte para

dar cobertura a la Gestión de la información.

La gestión de la información se presenta en dos grandes ámbitos: el externo y el interno.

- **Gestión de información interna**

  La gestión de información interna está definida de forma clara con lo que se conoce como inteligencia de negocio. Esta se enfoca en tratar y analizar todos los datos internos que se generan en una organización y por lo tanto su objetivo principal es conseguir mejoras de eficiencia y productividad en distintos departamentos o áreas de la organización.

  Este enfoque ha dado lugar soluciones como CRM y ERP así como al Cuadro de Mando Integral. Todos ellos, elementos pensados para apoyar la gestión de la empresa.

- **Gestión de información externa**

  Se centra en gestionar toda la información importante que se genera fuera de la empresa. Es una fuente constante de potenciales oportunidades y amenazas.

  Las disciplinas y aplicaciones tradicionalmente asociadas con este ámbito son la vigilancia tecnológica, inteligencia competitiva, la inteligencia de mercado, etc. El objetivo final de estas disciplinas es el de monitorizar el entorno competitivo e informativo de la organización para crear ventajas sostenibles en el tiempo y así crear innovaciones, lanzar nuevas tecnologías o toma de decisiones estratégicas.

3.2. Seguridad de la Información

La Seguridad de la Información puede ser vista desde su rol estratégico en los procesos de negocio, al identificar con qué recursos se debe contar para alcanzar la efectividad entre las actividades de resguardo o protección de los activos de información y la habilitación del acceso apropiado a los mismos, siendo los tres pilares principales de la seguridad de información la confidencialidad, integridad y disponibilidad, sin los cuales no se podrá realizar una correcta gestión de la seguridad de la información.

La seguridad de la información es la recopilación de actividades y medidas preventivas y reactivas que realizan las organizaciones y los sistemas tecnológicos para resguardar y proteger la información con el objetivo de mantener la confidencialidad, la disponibilidad e integridad de la misma.

Garantizar un nivel de protección total es virtualmente imposible, poseer seguridad de la información a nivel total en la práctica no es alcanzable porque no existe un sistema

seguro al ciento por ciento, esto debido a que la información está expuesta a un mayor rango de amenazas y vulnerabilidades, y los tipos de ataque y las metodologías implementadas cambian y evolucionan de una forma acelerada.

Tomando en cuenta lo anterior el propósito de la seguridad en todos sus ámbitos de aplicación es reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes.

Por lo cual la adopción de seguridad de la información en una organización protege la información de un amplio rango de amenazas para asegurar la continuidad del negocio, minimiza los posibles daños y maximizar el retorno de las inversiones.

3.2.1. Tipos de seguridad en sistemas de información

A continuación, se definen los dos principales tipos de seguridad de información que se deben de tener en cuenta.

- **Seguridad preventiva**
  Es aquella que reduce la probabilidad de ocurrencia de eventos no deseados que coloquen en peligro la integridad, confidencialidad o disponibilidad de la información, así como minimiza el impacto a la organización en aquellos casos que se presente un evento.
- **Seguridad reactiva**
  Se activa una vez ha ocurrido un evento no deseado, tiene como objetivo estructurar la organización para minimizar las consecuencias de lo ocurrido y permitir enfrentar el presente y futuro de la mejor forma posible, a pesar de lo ocurrido.

3.3. Sistema de Gestión de Seguridad de la Información (SGSI)

Un Sistema de Gestión de Seguridad de la Información es un conjunto de responsabilidades, políticas y procesos por medio de los cuales se gestiona de manera eficiente la accesibilidad a la información, asegurando el mantenimiento de la confidencialidad, integridad y disponibilidad de los activos de información, siendo un proceso sistemático documentado y conocido por toda la organización permite la disminución de los riesgos.

La implantación completa de un SGSI supondrá un cambio radical para las organizaciones sustituyendo las medidas tomadas de forma intuitiva por sistemas de información con acceso ordenado. Esta implementación permite un mejor conocimiento de la organización y su funcionamiento, facilitando así el acceso a la información.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

3.3.1. Importancia de la implementación de un SGSI

En la actualidad todas las organizaciones poseen información sensible y esta es considerada su mayor activo. La cantidad de amenazas a las que se ve sometida aumenta cada día, es por esto que las organizaciones deben tomar las medidas necesarias para proteger su activo más valioso, la información.

Por lo que la implementación de un sistema de gestión de seguridad de la información se vuelve de suma importancia para mantener la disponibilidad, integridad y confidencialidad de la información.

3.3.2. Fundamentos de un SGSI

Para garantizar que se está realizando de forma correcta la gestión de seguridad de la información se debe identificar su ciclo de vida y los aspectos relevantes adoptados para garantizar su confidencialidad, integridad y disponibilidad. Donde:

- **Confidencialidad:** la información no se encuentra disponible ni se revela a individuos, entidades o procesos que no están autorizados.
- **Integridad:** la información no se ve alterada y/o modificada y se asegura la exactitud de la misma y sus métodos de proceso.
- **Disponibilidad:** la información se encuentra disponible en tiempo y forma para los individuos, entidades o procesos autorizados cuando lo requieran.

Basado en el conocimiento del ciclo de vida de la información en la institución se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

3.4. Organización de Normas ISO y sus antecedentes

La Organización de Normas ISO surgió luego de la segunda guerra mundial como iniciativa de los delegados de la UNSCC (United Nations Standards Coordinating Committee), organización que empujaba el desarrollo manufacturero de armamento que fue impulsando la estandarización. La idea que tenía la UNSCC era la creación de un único organismo conjunto internacional dedicado a la normalización y fue así como en conjunto con la International Federation of the National Standardizing conocida como ISA se fundó la ISO.

El significado de las siglas ISO es “Organización Internacional para la Estandarización”, y el objeto de su creación es la creación de una serie de normas para fabricación, comercio y comunicación en todas las ramas industriales.

ISO fue creada en el año 1946 con la presencia de representantes provenientes de 25 países, en Londres, Inglaterra en la sede del Instituto de Ingenieros Civiles. Pero fue hasta el 27 de febrero de 1947 que se hace oficial la creación de la Organización e inicia actividades.

En el año 1951 es publicada la primera norma ISO sin embargo en ese momento no se publicó como un estándar sino más bien como una “recomendación”. A la fecha la Organización de Normas ISO ha creado y publicado más de 19,500 normas para todos los sectores de industria, salud, sector alimentario, tecnológico, entre otros.

A lo largo del tiempo ISO ha logrado tener un gran impacto e incidencia a nivel mundial, sin embargo, la adopción de las normas es opcional ya que la misma no posee autoridad de imponer sus normas a ningún país u organización.

3.5. Estructura de Alto Nivel (HLS)

La Estructura de Alto Nivel conocida por sus siglas en inglés como **HLS** (**High Level Structure)** es el nombre como se conoce al modelo normalizado, establecido para preparar un sistema de redacción de las normas de gestión ISO, obtenido por el grupo de trabajo de ISO en la búsqueda de crear una estructura general para todos los estándares de Sistemas de Gestión con el fin de que los mismos sean simétricos en forma sin importar el área a la cual vaya dirigido cada uno de ellos, es decir, que las normas de Sistemas de Gestión poseen la misma estructura, definiciones y texto fundamentales idénticos.

La Estructura de Alto Nivel se encuentra definida en el Apéndice SL del documento ISO/IEC Directivas, Parte 1.

El objetivo de esta normalización, es fomentar la compatibilidad entre las diversas normas de sistemas de gestión, para facilitar su integración y su implementación, en las organizaciones certificadas o que quieran certificarse.

Con la Estructura de Alto Nivel se permite que las características y las exigencias propias a cada norma, se integren en los capítulos definidos según la estructura de forma apropiada.

La Estructura de Alto Nivel está desarrollada de la siguiente manera:

1. **Introducción**

2. **Alcance (Objeto y campo de aplicación)**

   Se le presentan a las organizaciones los requerimientos que son genéricos y aplicables a cada una de ellas no importando el rubro en el que se desarrollan, siendo este alcance el del estándar ISO como tal y no así del sistema.

3. **Referencias normativas (Normas para consulta)**

   Sección creada con el fin de mantener la numeración alineada a los estándares ISO, aunque no existan como tal en las versiones próximas de algunas de ellas.

4. **Términos y definiciones**

   En la actualidad algunas Normas ya incluyen una sección de términos y definiciones sin embargo otras lo incluyen dentro de alguna otra norma de la familia, sin embargo, con la Estructura de Alto Nivel las Normas de Sistemas de Gestión ya contarán con esta sección dentro de su contenido.

5. **Contexto de la organización**

   Para ISO es necesario que sean identificados los factores que afectan a las organizaciones es decir que generan alguna influencia en ellas indiferentemente de si sean externas o internas en cualquier área. Además de esto, se debe entender los intereses de las partes interesadas para que sean alineadas al entendimiento del alcance del Sistema de Gestión.

6. **Liderazgo**

   No importando el área en la que el Sistema de Gestión se maneje se deben de tener clara dentro de las organizaciones las responsabilidades y autoridades, comunicarlas de manera objetiva, además de establecer correctamente las políticas.

7. **Planificación**

   Un enfoque basado en riesgos es necesario en las organizaciones ya que se debe de asegurar que el Sistema de Gestión haga lo que esta supuesto a hacer y que se prevengan esos eventos que no se desea que sucedan. Es por lo antes mencionado que esta sección tiene como objetivo desarrollar planes para el cumplimiento de los objetivos, y que estos vayan en cascada y de una manera holística.

8. **Soporte (incluyendo Recursos)**

   Dentro de la parte de soporte entran la infraestructura y el ambiente, monitoreo de equipos y su mantenimiento, así como otros recursos necesarios para la actividad realizada y contratar el personal competente.

9. **Operación**

El énfasis principal en este apartado es que cada organización identifique cuales procesos requieren en sus operaciones.

10. **Evaluación del desempeño**

    Esta sección es para aquellas normas ISO que necesitan una evaluación de cumplimiento, un monitoreo de la satisfacción del cliente o la evaluación de la correcta realización de un proceso específico.

11. **Mejora**

    Es necesario en las organizaciones que sus Sistemas de Gestión sean idóneos, adecuados y efectivos. El enfoque es basado en riesgos y ya no solo en acciones preventivas. Con el fin de que las organizaciones sepan reaccionar adecuadamente a los incidentes, tomar acciones de control, corregir, lidiar con las consecuencias y manejar las posibles re ocurrencias de los hechos.

3.6. Familia ISO 27000

En 1995 la organización BSI (British Standards Institution) incorporo el primer conjunto de buenas prácticas para la gestión de seguridad de la información con el nombre BS 7799-1, en la primera fase se le realizaron varios cambios antes de convertirse en ISO y la misma fuera una norma certificada con el nombre de ISO27001 la cual es una de las normas principales pertenecientes a la familia ISO27000.

La familia de normas ISO 27000 es un conjunto de estándares en los cuales se brindan las mejores prácticas sobre la Gestión 2de Seguridad de la Información que ofrecen a las organizaciones ayuda para mantener la seguridad en sus activos de información. Adoptar esta familia de normas proporciona a las organizaciones una opción de cómo administrar la seguridad de los activos, tales como informaciones financieras, propiedad intelectual, detalles de los funcionarios o información confiada por terceros, por medio de la implementación de un Sistema de Gestión de Seguridad de la Información.

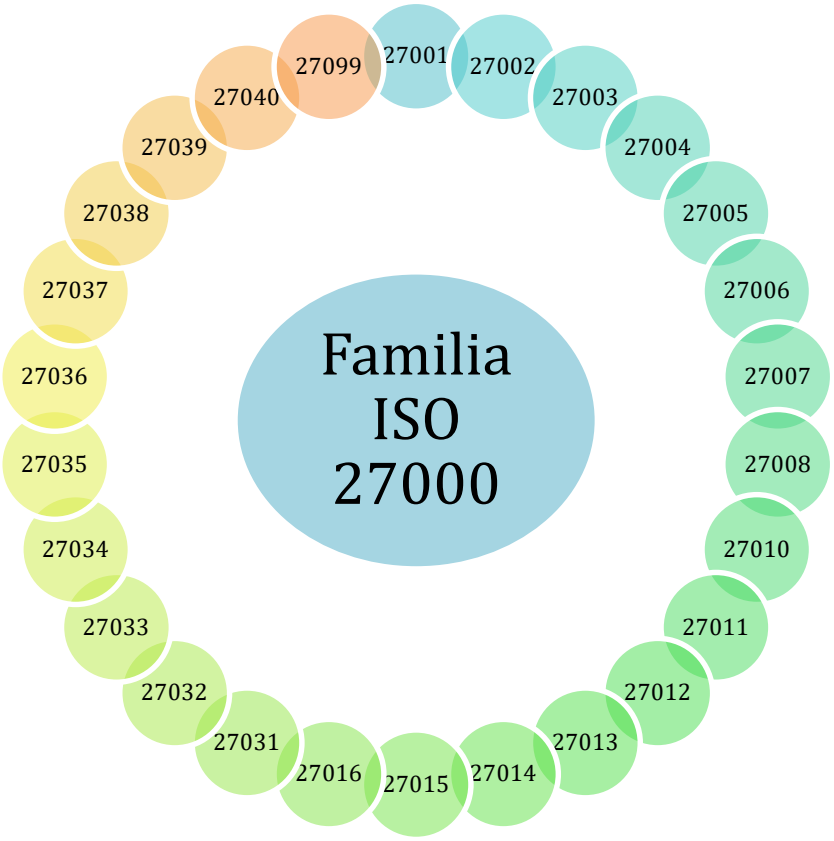


Ilustración 1- Familia ISO 27000

A continuación, se detalla la lista de normas que pertenecen a la familia ISO27000:

- ISO/IEC 27000: Es la norma que proporciona una visión general de las normas que componen la serie 27000.
- ISO/IEC 27001: Es la norma principal y contiene los requisitos del sistema de gestión de seguridad de la información.
- ISO/IEC 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- ISO/IEC 27003: Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo a la norma ISO/IEC 27001.
- ISO/IEC 27004: Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
- ISO/IEC 27005: Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001.

- ISO/IEC 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- ISO/IEC 27007: Guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
- ISO/IEC 27008: Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- ISO/IEC 27010: Guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.
- ISO/IEC 27011: Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.
- ISO/IEC 27012: Conjunto de requisitos y directrices de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.
- ISO/IEC 27013: Guía de implementación integrada de ISO/IEC 27001 y de ISO/IEC 20000-1.
- ISO/IEC 27014: Guía de gobierno corporativo de la seguridad de la información.
- ISO/IEC 27015: Guía de SGSI para organizaciones del sector financiero y de seguros.
- ISO/IEC 27016: Guía de SGSI relacionada con aspectos económicos en las organizaciones.
- ISO/IEC 27031: Describe los conceptos y principios de la tecnología de información y comunicación (TIC)
- ISO/IEC 27032: Guía referente a la ciberseguridad.
- ISO/IEC 27033: Seguridad en redes. Tiene 7 partes:
    - 27033-1, conceptos generales
    - 27033-2, directrices de diseño e implementación de seguridad en redes
    - 27033-3, escenarios de redes de referencia
    - 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad

- 27033-5, aseguramiento de comunicaciones mediante VPNs
- 27033-6, convergencia IP
- 27033-7, redes inalámbricas

- ISO/IEC 27034: Conjunto de guías de seguridad para aplicaciones informáticas.
- ISO/IEC 27035: Guía de gestión de incidentes de seguridad de la información.
- ISO/IEC 27036: Guía de seguridad de outsourcing (externalización de servicios).
- ISO/IEC 27037: Guía de identificación, recopilación y preservación de evidencias digitales.
- ISO/IEC 27038: Guía de especificación para la redacción digital.
- ISO/IEC 27039: Guía para la selección, despliegue y operativa de sistemas de detección de intrusos.
- ISO/IEC 27040: Guía para la seguridad en medios de almacenamiento.
- ISO 27799: Norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002.

3.7. ISO 27001:2013

ISO 27001:2013 es el estándar principal de la familia de Normas ISO27000, en esta se presentan los requerimientos para el desarrollo y operación de un Sistema de Gestión de Seguridad de la Información incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información.

La última publicación de la Norma es del año 2013, esta norma se encuentra elaborada bajo la Estructura de Alto Nivel (HLS) que determina el Anexo SL, por esta razón en la última versión se visualizaron cambios en todo el contenido, así como en la estructura de la norma.

De la familia de Normas ISO 27000 está es la única que es certificable, con la obtención de la certificación de esta norma se podrá demostrar de cara a clientes y accionistas que para toda la información se garantiza las tres siguientes dimensiones de la seguridad:

- **Confidencialidad:** Consiste en que la información no se coloca a disposición, ni se revela a individuos, entidades o procesos no autorizados. Posee como objetivo controlar que el acceso a la información sea restringido solo a personas autorizadas.
- **Integridad:** Consiste cuando el activo de información no ha sido alterado de

manera no autorizada. Su objetivo es garantizar que los métodos de procesamiento de información son exactos, y asegura datos completos y correctos.

* **Disponibilidad:** Es aquella en que las entidades o procesos autorizados tienen acceso a la información cuando lo requieren. Su objetivo es controlar que sólo las personas autorizadas podrán acceder a la información cuando lo soliciten o sea necesario.

3.7.1. Estructura de ISO 27001:2013

La Norma ISO 27001 posee una estructura de 11 secciones más el anexo A; para la implementación de todos los requerimientos de la norma las secciones 0 a 3 son introductorias y no son obligatorias para la implementación, mientras que las secciones 4 a 10 son obligatorias. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

Ilustración 2 - Estructura ISO 27001:2013

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que

todas aquellas normas que se encuentren bajo la Estructura de Alto nivel.

- ✓ **Introducción**

  Explica la razón de ser de esta norma, indicando que se busca el establecimiento, implementación, mantenimiento y mejora continua de un SGSI.

  Específica los tres compromisos de la seguridad de la información: confidencialidad, integridad y disponibilidad. Así como también indica que el orden en el que son presentados los requisitos no refleja la importancia ni el orden en que deben ser implementados.

- ✓ **Alcance (Objeto y campo de aplicación)**

  En esta sección se menciona que los requisitos del estándar son aplicables a cualquier organización, sin importar su tipo, tamaño o naturaleza con el propósito de proteger los activos de información y brindar confianza a las partes interesadas.

- ✓ **Referencias normativas**

  La norma ISO/IEC 27000 es única referencia normativa de consulta obligatoria.

- ✓ **Términos y definiciones**

  Para consultas en los términos nos hace referencia a la norma ISO/IEC 27000.

- ✓ **Contexto de la organización**

  En esta cláusula se determina quienes son los beneficiarios del SGSI, propone las pautas y puntos de vista que se debe plantear la organización para la correcta identificación de los mismos.

- ✓ **Liderazgo**

  Se presentan los aspectos que definen al SGSI como un proceso estratégico de la organización y establece el compromiso que deberá de tomar la alta dirección con respecto al mismo.

- ✓ **Planificación**

  Esta sección se enfoca en detallar el proceso para la evaluación de riesgos, la detección de oportunidades y la definición de los objetivos de seguridad.

- ✓ **Soporte**

  En esta sección se presentan las referencias a los medios que serán necesarios en la organización para alcanzar el desarrollo completo de un SGSI. Adicional se denota la importancia de los recursos humanos, en las capacidades de cada miembro de la organización, insistiendo en su concienciación y formación para asegurar un buen desempeño del sistema de seguridad de la información.

Se encuentra adicional una descripción de la forma en que se deberá tratar la información documentada de la organización, desde su creación y accesibilidad hasta su protección.

- ✓ **Operación**
  Se explica la manera en la cual se logra un correcto funcionamiento del SGSI una vez implementado en la organización.

- ✓ **Evaluación del desempeño**
  El análisis de los resultados en comparación con los objetivos y las metas a cumplir es muy importante en un SGSI, por lo que en esta sección se presentan los lineamentos para el planteamiento de medios de análisis que comprueben si dichos objetivos se están cumpliendo o no.

- ✓ **Mejora**
  En esta sección se especifican los métodos por medio de los cuales se puede implementar el proceso de mejora continua a partir de los hallazgos en la evaluación del desempeño del SGSI.

3.7.2. Objetivos de Control de ISO 27001:2013

El Anexo A de la Norma ISO 27001 es la sección de la norma en la cual se provee una herramienta esencial para la gestión de la seguridad: una lista de los controles (o medidas) de seguridad que pueden ser usados para mejorar la seguridad de la información.

El Anexo A tiene 14 categorías de control (del 5 al 18) con un total de 114 controles, la mejor manera de comprender el contenido del Anexo A es visualizarlo como un catálogo de controles de seguridad del que se pueden seleccionar los que apliquen en la organización. A continuación, se mencionan las categorías y controles:

- ∗ **A5 Política de seguridad de información**
  En esta sección se presentan controles acerca de cómo deben ser escritas y revisadas las políticas de seguridad de la información. Las subsecciones del apartado A5 son:

  - ✓ A.5.1.1 Políticas de Seguridad de la Información.
  - ✓ A.5.1.2 Revisión de las políticas para la seguridad de la información.

- ∗ **A6 Organización de la seguridad de la información**
  Controles para los cuales se debe de definir asignan las responsabilidades de seguridad de información; en esta sección también se incluyen los controles para los dispositivos móviles y el teletrabajo. Las subsecciones del apartado A6 son:

- ✓ A.6.1 Organización interna.
  - ➢ A.6.1.1 Roles y responsabilidades para la seguridad de la información.
  - ➢ A.6.1.2 Separación de deberes.
  - ➢ A.6.1.3 Contacto con las autoridades.
  - ➢ A.6.1.4 Contacto con grupos de interés especial.
  - ➢ A.6.1.5 Seguridad de la información en la gestión de proyectos.
- ✓ A.6.2 Dispositivos móviles y teletrabajo.
  - ➢ A.6.2.1 Política para dispositivos móviles.
  - ➢ A.6.2.2 Teletrabajo.

* **A7 Seguridad de los recursos humanos**

  Se presentan controles antes, durante y después de realizar contrataciones de empleados y/o proveedores. Las subsecciones del apartado A7 son:

  - ✓ A.7.1 Antes de asumir el empleo.
    - ➢ A.7.1.1 Investigación de antecedentes.
    - ➢ A.7.1.2 Términos y condiciones de contratación.
  - ✓ A.7.2 Durante la ejecución del empleo.
    - ➢ A.7.2.1 Responsabilidades de gestión.
    - ➢ A.7.2.2 Concienciación, educación y capacitación en SI.
    - ➢ A.7.2.2 Proceso disciplinario.
  - ✓ A.7.3 Cese o cambio de puesto de trabajo.
    - ➢ A.7.3.1 Cese o cambio de puesto de trabajo.

* **A8 Gestión de activos**

  Controles relacionados con el inventario de recursos y su uso de forma aceptable, también se presentan controles para la clasificación de la información y la gestión de los medios de almacenamiento. Las subsecciones del apartado A8 son:

  - ✓ A.8.1 Responsabilidad sobre los activos.
    - ➢ A.8.1.1 Inventario de activos.
    - ➢ A.8.1.2 Propiedad de los activos.
    - ➢ A.8.1.3 Uso aceptable de los activos.
    - ➢ A.8.1.4 Devolución de activos.
  - ✓ A.8.2 Clasificación de la información.
    - ➢ A.8.2.1 Directrices de clasificación.
    - ➢ A.8.2.2 Etiquetado y manipulado de la información.
    - ➢ A.8.2.3 Manipulación de activos.

- ✓ A.8.3 Manejo de los soportes de almacenamiento.
  - ➢ A.8.3.1 Gestión de soportes extraíbles.
  - ➢ A.8.3.2 Eliminación de soportes.
  - ➢ A.8.3.3 Soportes físicos en tránsito.

* **A9 Control de Acceso**

  Se presentan controles para las políticas de control de acceso, la gestión de acceso de los usuarios, el control de acceso a los sistemas y aplicaciones, y las responsabilidades del usuario. Las subsecciones del apartado A9 son:

  - ✓ A.9.1 Requisitos de negocio para el control de accesos.
    - ➢ A.9.1.1 Política de control de accesos.
    - ➢ A.9.1.2 Control de acceso a las redes y servicios asociados.
  - ✓ A.9.2 Gestión de acceso de usuario.
    - ➢ A.9.2.1 Gestión de altas/bajas en el registro de usuarios.
    - ➢ A.9.2.2 Gestión de los derechos de acceso asignados a usuarios.
    - ➢ A.9.2.3 Gestión de los derechos de acceso con privilegios especiales.
    - ➢ A.9.2.4 Gestión de información confidencial de autenticación de usuarios.
    - ➢ A.9.2.5 Revisión de los derechos de acceso de los usuarios.
    - ➢ A.9.2.6 Retirada o adaptación de los derechos de acceso.
  - ✓ A.9.3 Responsabilidades del usuario.
    - ➢ A.9.3.1 Uso de información confidencial para la autenticación.
  - ✓ A.9.4 Control de acceso a sistemas y aplicaciones.
    - ➢ A.9.4.1 Restricción del acceso a la información.
    - ➢ A.9.4.2 Procedimientos seguros de inicio de sesión.
    - ➢ A.9.4.3 Gestión de contraseñas de usuario.
    - ➢ A.9.4.4 Uso de herramientas de administración de sistemas.
    - ➢ A.9.4.5 Control de acceso al código fuente de los programas.

* **A10 Cifrado**

  En esta sección se encuentran los controles relacionados con la gestión de cifrado y claves. Las subsecciones del apartado A10 son:

  - ✓ A.10.1 Controles criptográficos.
    - ➢ A.10.1.1 Política de uso de los controles criptográficos.
    - ➢ A.10.1.2 Gestión de claves.

* **A11 Seguridad física y Ambiental**

  Se presentan controles que definen áreas seguras, controles de entrada,

protección contra amenazas, seguridad de equipos, descarte seguro de activos, políticas de escritorio y pantalla despejadas. Las subsecciones del apartado A11 son:

- ✓ A.11.1 Áreas seguras.
  - ➢ A.11.1.1 Perímetro de seguridad física.
  - ➢ A.11.1.2 Controles físicos de entrada.
  - ➢ A.11.1.3 Seguridad de oficinas.
  - ➢ A.11.1.4 Protección contra las amenazas externas y ambientales.
  - ➢ A.11.1.5 El trabajo en áreas seguras.
  - ➢ A.11.1.6 Áreas de acceso público, carga y descarga.
- ✓ A.11.2 Seguridad de los equipos.
  - ➢ A.11.2.1 Emplazamiento y protección de equipos.
  - ➢ A.11.2.2 Instalaciones de suministro.
  - ➢ A.11.2.3 Seguridad del cableado.
  - ➢ A.11.2.4 Mantenimiento de los equipos.
  - ➢ A.11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - ➢ A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - ➢ A.11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - ➢ A.11.2.8 Equipo informático de usuario desatendido.
  - ➢ A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

* **A12 Seguridad Operacional**

En la sección se definen los controles relacionados con la gestión de la producción en TI como: la gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc. Las subsecciones del apartado A12 son:

- ✓ A.12.1 Responsabilidades y procedimientos de operación.
  - ➢ A.12.1.1 Documentación de procedimientos de operación.
  - ➢ A.12.1.2 Gestión de cambios.
  - ➢ A.12.1.3 Gestión de capacidades.
  - ➢ A.12.1.4 Separación de entornos de desarrollo, prueba y producción.
- ✓ A.12.2 Protección contra código malicioso.

- ➢ A.12.2.1 Controles contra el código malicioso
- ✓ A.12.3 Copias de seguridad.
  - ➢ A.12.3.1 Copias de seguridad de la información
- ✓ A.12.4 Registro de actividad y supervisión.
  - ➢ A.12.4.1 Registro y gestión de eventos de actividad.
  - ➢ A.12.4.2 Protección de los registros de información.
  - ➢ A.12.4.3 Registros de actividad del administrador y operador del sistema.
  - ➢ A.12.4.4 Sincronización de relojes.
- ✓ A.12.5 Control del software en explotación.
  - ➢ A.12.5.1 Instalación del software en sistemas en producción.
- ✓ A.12.6 Gestión de la vulnerabilidad técnica.
  - ➢ A.12.6.1 Gestión de las vulnerabilidades técnicas.
  - ➢ A.12.6.2 Restricciones en la instalación de software.
- ✓ A.12.7 Consideraciones de las auditorías de los sistemas de información.
  - ➢ A.12.7.1 Controles de auditoría de los sistemas de información.

* **A13 Seguridad en las Telecomunicaciones**

  Controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc. Las subsecciones del apartado A13 son:

  - ✓ A.13.1 Gestión de la seguridad en las redes.
    - ➢ A.13.1.1 Controles de red.
    - ➢ A.13.1.2 Mecanismos de seguridad asociados a servicios en red.
    - ➢ A.13.1.3 Segregación de redes.
  - ✓ A.13.2 Intercambio de información con partes externas.
    - ➢ A.13.2.1 Políticas y procedimientos de intercambio de información.
    - ➢ A.13.2.2 Acuerdos de intercambio.
    - ➢ A.13.2.3 Mensajería electrónica.
    - ➢ A.13.2.4 Acuerdos de confidencialidad y secreto.

* **A14 Adquisición, desarrollo y mantenimiento de Sistemas**

  Presenta controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte Las subsecciones del apartado A14 son:

  - ✓ A.14.1 Requisitos de seguridad de los sistemas de información.
    - ➢ A.14.1.1 Análisis y especificación de los requisitos de seguridad.
    - ➢ A.14.1.2 Seguridad de las comunicaciones en servicios

accesibles por redes públicas.

- ➢ A.14.1.3 Protección de las transacciones por redes telemáticas.

✓ A.14.2 Seguridad en los procesos de desarrollo y soporte.

- ➢ A.14.2.1 Política de desarrollo seguro de software.
- ➢ A.14.2.2 Procedimientos de control de cambios en los sistemas.
- ➢ A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- ➢ A.14.2.4 Restricciones a los cambios en los paquetes de software.
- ➢ A.14.2.5 Uso de principios de ingeniería en protección de sistemas.
- ➢ A.14.2.6 Seguridad en entornos de desarrollo.
- ➢ A.14.2.7 Externalización del desarrollo de software.
- ➢ A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- ➢ A.14.2.9 Pruebas de aceptación.

✓ A.14.3 Datos de prueba.

- ➢ A.14.3.1 Protección de los datos utilizados en prueba.

* **A15 Relaciones con los proveedores**

Controles sobre lo que se debe incluir en los contratos, y cómo hacer el seguimiento a los proveedores. Las subsecciones del apartado A15 son:

✓ A.15.1 Seguridad de la información en las relaciones con suministradores.

- ➢ A.15.1.1 Política de seguridad de la información para suministradores.
- ➢ A.15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
- ➢ A.15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

✓ A.15.2 Gestión de la prestación del servicio por suministradores.

- ➢ A.15.2.1 Supervisión y revisión de los servicios prestados por terceros.
- ➢ A.15.2.2 Gestión de cambios en los servicios prestados por terceros.

* **A16 Gestión de Incidentes**

Presenta controles para el reporte de eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.

Las subsecciones del apartado A16 son:

- ✓ A.16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - ➢ A.16.1.1 Responsabilidades y procedimientos.
  - ➢ A.16.1.2 Notificación de los eventos de seguridad de la información.
  - ➢ A.16.1.3 Notificación de puntos débiles de la seguridad.
  - ➢ A.16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - ➢ A.16.1.5 Respuesta a los incidentes de seguridad.
  - ➢ A.16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - ➢ A.16.1.7 Recopilación de evidencias.

* **A17 Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio**

  Controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI. Las subsecciones del apartado A17 son:

  - ✓ A.17.1 Continuidad de la seguridad de la información.
    - ➢ A.17.1.1 Planificación de la continuidad de la seguridad de la información.
    - ➢ A.17.1.2 Implantación de la continuidad de la seguridad de la información.
    - ➢ A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
  - ✓ A.17.2 Redundancias.
    - ➢ A.17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

* **A18 Cumplimiento**

  Controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales y revisiones de la seguridad de la información. Las subsecciones del apartado A18 son:

  - ✓ A.18.1 Cumplimiento de los requisitos legales y contractuales.
    - ➢ A.18.1.1 Identificación de la legislación aplicable.
    - ➢ A.18.1.2 Derechos de propiedad intelectual (DPI).
    - ➢ A.18.1.3 Protección de los registros de la organización.

- ➢ A.18.1.4 Protección de datos y privacidad de la información personal.
- ➢ A.18.1.5 Regulación de los controles criptográficos.

✓ A.18.2 Revisiones de la seguridad de la información.

- ➢ A.18.2.1 Revisión independiente de la seguridad de la información.
- ➢ A.18.2.2 Cumplimiento de las políticas y normas de seguridad.
- ➢ A.18.2.3 Comprobación del cumplimiento.

3.8. CdA

CdA es la Comisión de Acreditación de la Calidad de la Educación Superior a través de la cual el Estado Salvadoreño reconoce a las Instituciones de Educación Superior que muestran estar comprometidas con la mejora continua con una acreditación. Este proceso es voluntario para cada universidad e institutos tecnológicos especializados.

3.8.1. Sistema de mejora de educación superior

En 1997 se establece el sistema de mejora de educación superior que se ramifica en tres subsistemas más los cuales son la calificación, la evaluación y la acreditación.

La calificación consiste en el envío de los documentos que reflejan la cantidad de docentes tiempo completo por estudiante, número de estudiantes por computadora, etc., estos documentos son publicados por el Ministerio de Educación anualmente y es de carácter obligatorio.

La evaluación se considera un proceso cualitativo en el que cada institución cada tres años realiza tanto una autoevaluación como una evaluación realizada por invitados.

Para la realización de la autoevaluación el Ministerio de Educación cuenta con un lineamiento que contiene las siguientes 11 categorías:

- Misión Institucional
- Gobierno y administración institucional
- Estudiantes
- Académicos
- Carreras y otros programas académicos
- Investigación
- Proyección social
- Recursos educacionales
- Administración financiera
- Infraestructura física

- Integridad institucional
- Acreditación

Resultado de los dos subsistemas anteriores. Además, se realiza una entrevista donde se muestran los detalles de sus logros.

La acreditación no es permanente está debe de ser validada y re-evaluada cada cinco años, solicitando el proceso al Ministerio de Educación el inicio del proceso mostrando compromiso y procurando la mejora continua. El proceso de renovación tiene que seguir los mismos lineamientos de la acreditación inicial.

3.9. Escala de Likert

La escala de Likert es un conjunto de interrogantes que permiten evaluar el conocimiento que se posee sobre un tema en particular, en la que se pueden definir respuestas colectivas y el formato en las que estas son evaluadas según un rango de valores. Una escala de Likert sirve para realizar mediciones y obtener el conocimiento del grado de conformidad o implementación de una persona hacia un determinado tema o control.

El objetivo de una escala de Likert es lograr medir una actitud o unas predisposiciones en un contexto en particular, es conocida, además, como una escala de sumatoria, debido a que el resultado viene dado mediante la suma de las respuestas obtenidas en cada interrogante. Esta escala, es construida en base a una serie de interrogantes que reflejen una actitud positiva o negativa acerca de un estímulo o conocimiento de una persona, frecuencia de una actividad, relevancia de un factor, valoraciones de empresas, productos o servicios, probabilidad de acciones en el futuro, etc.

Cada pregunta, se formula mediante diferentes alternativas de respuesta, como, por ejemplo:

Acuerdo	Frecuencia	Importancia	Probabilidad	Conocimiento
- Totalmente de acuerdo	- Muy frecuentemente	- Muy importante	- Casi siempre	- Óptimo
- De acuerdo	- Frecuentemente	- Importante	- Usualmente	- Alto
- Indeciso	- Ocasionalmente	- Moderadamente importante	- Ocasionalmente	- Moderado
- En desacuerdo	- Raramente	- De poca importancia	- Usualmente no	- Poco
- Totalmente en desacuerdo	- Nunca	- Sin importancia	- Casi nunca	- Nulo

Tabla 6- Escala de Likert ejemplificada

Cabe recalcar, que cuando se construye una encuesta mediante el modelo de escala de Likert, cada opción de respuesta se debe relacionar fácilmente con el tipo de

respuesta brindada a la interrogante, sin importar que la relación entre la pregunta y las opciones de respuesta sea lógica.

Cada opción de respuesta debe tener tiempo dos posturas contrarias, así como una opción intermedia que permita un equilibrio entre las dos posturas. Es importante recalcas, que usualmente se utilizan 5 opciones de respuesta, pero el uso de más alternativas genera una mejor precisión en los resultados finales.

4. Análisis e interpretación de los resultados

En este capítulo se presentan los resultados del análisis de los datos obtenidos en la investigación. Estos resultados mostrarán el nivel de seguridad que existe actualmente en las universidades acreditadas por CdA.

4.1. Preámbulo

El objetivo en este capítulo es esencialmente el de determinar el nivel de madurez actual de las universidades acreditadas por la CdA en El Salvador según los requerimientos definidos en la norma ISO 27001:2013, así como la comprobación de la hipótesis planteada.

El análisis que a continuación se estructurará en una serie de secciones que incluyen todas las áreas comprendidas dentro de la ISO27001:2013.

4.2. Análisis de Resultados

A continuación, se presentan los resultados de la investigación en base a la información recolectada mediante el instrumento de estudio en datos cuantitativos de análisis mediante gráficos en donde se refleja el nivel de Seguridad de Información que poseen las Universidades acreditadas por la CdA en cada una de las secciones establecidas en la ISO27001.

Las 13 secciones en las que se divide la evaluación de Seguridad de Información son:

- ✓ Política de seguridad
- ✓ Organización de la seguridad de la información
- ✓ Seguridad de los recursos humanos
- ✓ Gestión de activos
- ✓ Control de accesos
- ✓ Cifrado
- ✓ Seguridad física y Ambiental
- ✓ Seguridad en la Operativa
- ✓ Seguridad en las Telecomunicaciones
- ✓ Adquisición, desarrollo y Mantenimiento de los sistemas de información
- ✓ Gestión de Incidentes
- ✓ Aspectos de la SI en la Gestión de la Continuidad de Negocio
- ✓ Cumplimiento

Se asigna una nomenclatura para cada universidad, en la que será utilizado para el análisis de cada sección de la encuesta, esto con el fin de no revelar el nombre de la institución evaluada.

Universidad	Nomenclatura
ISEADE-FEPADE	U1
Universidad Don Bosco	U2
Tecnológica	U3
ITCA-FEPADE	U4
UNICAES	U5
UFG	U6
Dr. José Matías Delgado	U7
Universidad José Simeón Cañas UCA	U8
Escuela Superior de Economía y Negocios	U9

Tabla 7- Nomenclatura de Universidades

Para la realización de la interpretación de los resultados se tomaron en cuenta los siguientes factores de las universidades que participaron en la investigación:

Universidad	Cantidad de estudiantes	Cuota mínima estimadas	Cuota máxima estimada	Fundación	Antigüedad en años	Fecha acreditación
U1	300	$185.00	$250.00	1988	30	2005
U2	8,509	$68.00	$270.00	1984	34	2001
U3	21,008	$61.00	$75.00	1981	37	2003
U4	5,394	$40.00	$70.00	1969	49	2003
U5	6,970	$65.00	$70.00	1982	36	2002
U6	11,983	$80.00	$100.00	1981	37	2004
U7	7,440	$45.00	$450.00	1977	41	2003
U8	7,953	$95.00	$332.00	1965	53	2002
U9	791	$630.00	$630.00	1994	24	2003

Tabla 8- Variables tomadas en cuenta para el estudio

Para el análisis de datos y la presentación de los resultados, se utiliza la siguiente tabla de nomenclaturas con respecto a las respuestas de la encuesta.

Respuesta	Nomenclatura	Valor
NULO	N	1
POCO	P	2
MODERADO	M	3
ALTO	A	4
ÓPTIMO	O	5

Tabla 9- Nomenclatura de escala de Likert

Política de Seguridad

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Política de Seguridad	3	15	Nivel alto	]70% - 100%]	[11-15]
			Nivel medio	]40% - 70%]	[7-10]
			Nivel bajo	[0% - 40%]	[0 - 6]

Tabla 10- Resultados de sección Política de Seguridad

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿En qué nivel considera que se encuentra su política de seguridad de la información?	M	M	M	A	M	M	M	M	A
2. ¿Con qué frecuencia se actualiza la política de seguridad de la información?	B	B	M	A	M	M	B	A	A
3. ¿Cómo califica el nivel de conocimiento que poseen los empleados de su institución con respecto a la política de seguridad de la información?	N	B	A	A	M	O	B	A	A
Total	6	7	10	12	9	11	7	11	12

Tabla 11- Resultados de respuesta Política de Seguridad

De acuerdo con los resultados de la encuesta, se puede aseverar que todas las universidades encuestadas cuentan con una política de Seguridad de la Información documentada. Al analizar los datos, no se observa una tendencia en base a antigüedad, ingresos o números de estudiantes con respecto a la frecuencia con la que actualizan esta política; sin embargo, se observa una frecuencia con respecto a la antigüedad de las universidades para la calificación con el nivel de conocimiento que poseen los empleados de ella.

Por lo consiguiente, los factores analizados como son cantidad de estudiantes, ingresos y especialización de la universidad no afectan directamente el nivel de implementación de la política de Seguridad de la Información y el seguimiento que se le da a la misma.

Organización de la Seguridad de la Información

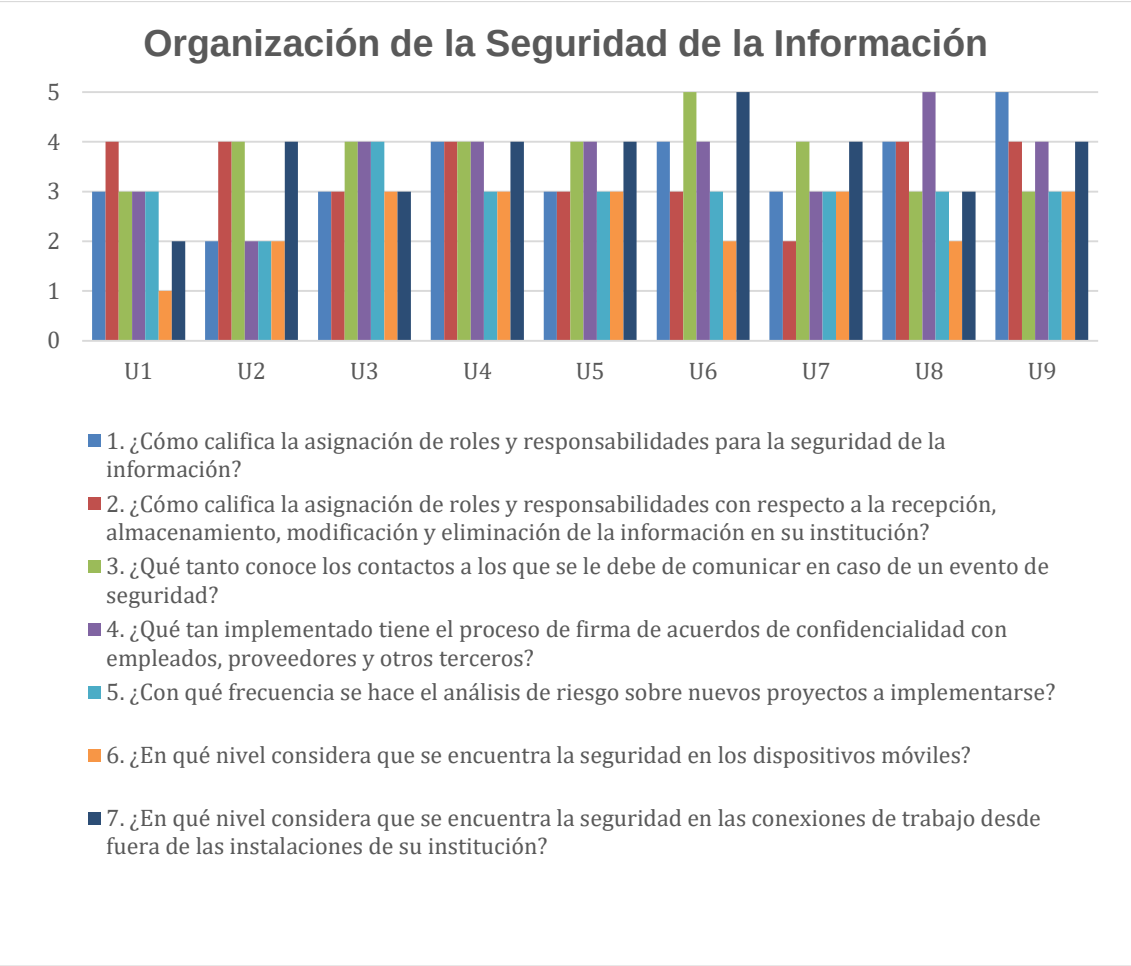
Para esta sección se evalúa el nivel de seguridad de información.

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Organización de la Seguridad de la Información	7	35	Nivel alto	]70% - 100%]	[26-35]
			Nivel medio	]40% - 70%]	[15-25]
			Nivel bajo	[0% - 40%]	[0 - 14]

Tabla 12- Resultados de sección Organización Seguridad de la Información

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Cómo califica la asignación de roles y responsabilidades para la seguridad de la información?	M	B	M	A	M	A	M	A	O
2. ¿Cómo califica la asignación de roles y responsabilidades con respecto a la recepción, almacenamiento, modificación y eliminación de la información en su institución?	A	A	M	A	M	M	B	A	A
3. ¿Qué tanto conoce los contactos a los que se le debe de comunicar en caso de un evento de seguridad?	M	A	A	A	A	O	A	M	M
4. ¿Qué tan implementado tiene el proceso de firma de acuerdos de confidencialidad con empleados, proveedores y otros terceros?	M	B	A	A	A	A	M	O	A
5. ¿Con qué frecuencia se hace el análisis de riesgo sobre nuevos proyectos a implementarse?	M	B	A	M	M	M	M	M	M
6. ¿En qué nivel considera que se encuentra la seguridad en los dispositivos móviles?	N	B	M	M	M	B	M	B	M
7. ¿En qué nivel considera que se encuentra la seguridad en las conexiones de trabajo desde fuera de las instalaciones de su institución?	B	A	M	A	A	O	A	M	A
Total	19	20	24	26	24	26	22	24	26

Tabla 13- Resultados de respuesta Organización Seguridad de la Información



En la mayoría de las universidades, con excepción de una, se cuenta con un nivel aceptable tanto para la asignación de roles y responsabilidades respecto al ciclo de procesamiento de la seguridad de la información, como de la firma de acuerdo de confidencialidad con los colaboradores y proveedores externos de la universidad. Se puede observar que la mayoría de las universidades encuestadas tienden a darle una importancia moderada al análisis de riesgos de los proyectos a implementar.

En base a los resultados obtenidos se puede observar que las universidades cuentan con los controles necesarios para garantizar que las conexiones remotas a sus sistemas son seguras mientras que con respecto a los controles establecidos para los dispositivos móviles es todo lo contrario.

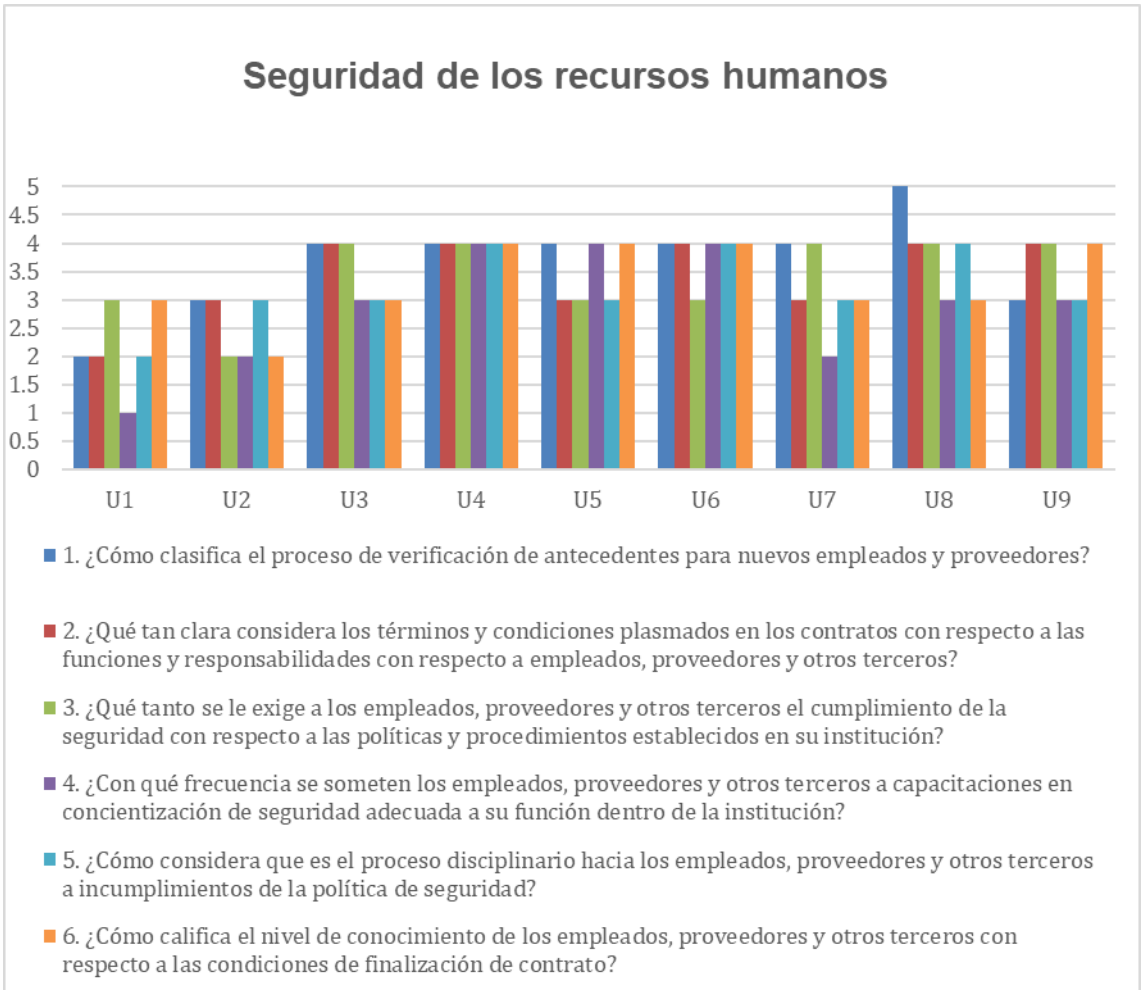
Seguridad de los recursos humanos

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Seguridad de los Recursos Humanos	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]

Tabla 14- Resultados de Seguridad en los Recursos Humanos

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Cómo clasifica el proceso de verificación de antecedentes para nuevos empleados y proveedores?	B	M	A	A	A	A	A	O	M
2. ¿Qué tan clara considera los términos y condiciones plasmados en los contratos con respecto a las funciones y responsabilidades con respecto a empleados, proveedores y otros terceros?	B	M	A	A	M	A	M	A	A
3. ¿Qué tanto se le exige a los empleados, proveedores y otros terceros el cumplimiento de la seguridad con respecto a las políticas y procedimientos establecidos en su institución?	M	B	A	A	M	M	A	A	A
4. ¿Con qué frecuencia se someten los empleados, proveedores y otros terceros a capacitaciones en concientización de seguridad adecuada a su función dentro de la institución?	N	B	M	A	A	A	B	M	M
5. ¿Cómo considera que es el proceso disciplinario hacia los empleados, proveedores y otros terceros a incumplimientos de la política de seguridad?	B	M	M	A	M	A	M	A	M
6. ¿Cómo califica el nivel de conocimiento de los empleados, proveedores y otros terceros con respecto a las condiciones de finalización de contrato?	M	B	M	A	A	A	M	M	A
Total	13	15	21	24	21	23	19	23	21

Tabla 15- Resultados de respuesta Seguridad en los Recursos Humanos



Las universidades encuestadas en su mayoría se preocupan por la verificación de los antecedentes del personal contratado, así como de los proveedores que les brindan un servicio y que estos estén informados de los términos y condiciones de la contratación y ante qué eventos se podría dar finalización a estos, además de tener claras las funciones que deben desempeñar dentro de la institución y de las.

La tendencia que muestra la gráfica con respecto a la concientización de la seguridad de la información y de las políticas y procedimientos que la respaldan, así como el conocimiento que los empleados tienen de estas y sus procesos disciplinarios en caso de incumplimientos es media-alta lo cual desde el punto de vista de la seguridad de la información es aceptable y con esto se reduce el riesgo de ocurrencia de eventos de seguridad por ignorancia de los empleados y/o proveedores.

Las universidades en esta sección se encuentran en un nivel medio y alto de seguridad en los recursos humanos sin embargo no existe un patrón que indique que el nivel de seguridad en este caso sea directamente proporcional al número de estudiantes de la universidad o al ingreso económico de las instituciones, los años que tiene de estar en funcionamiento.

Gestión de activos

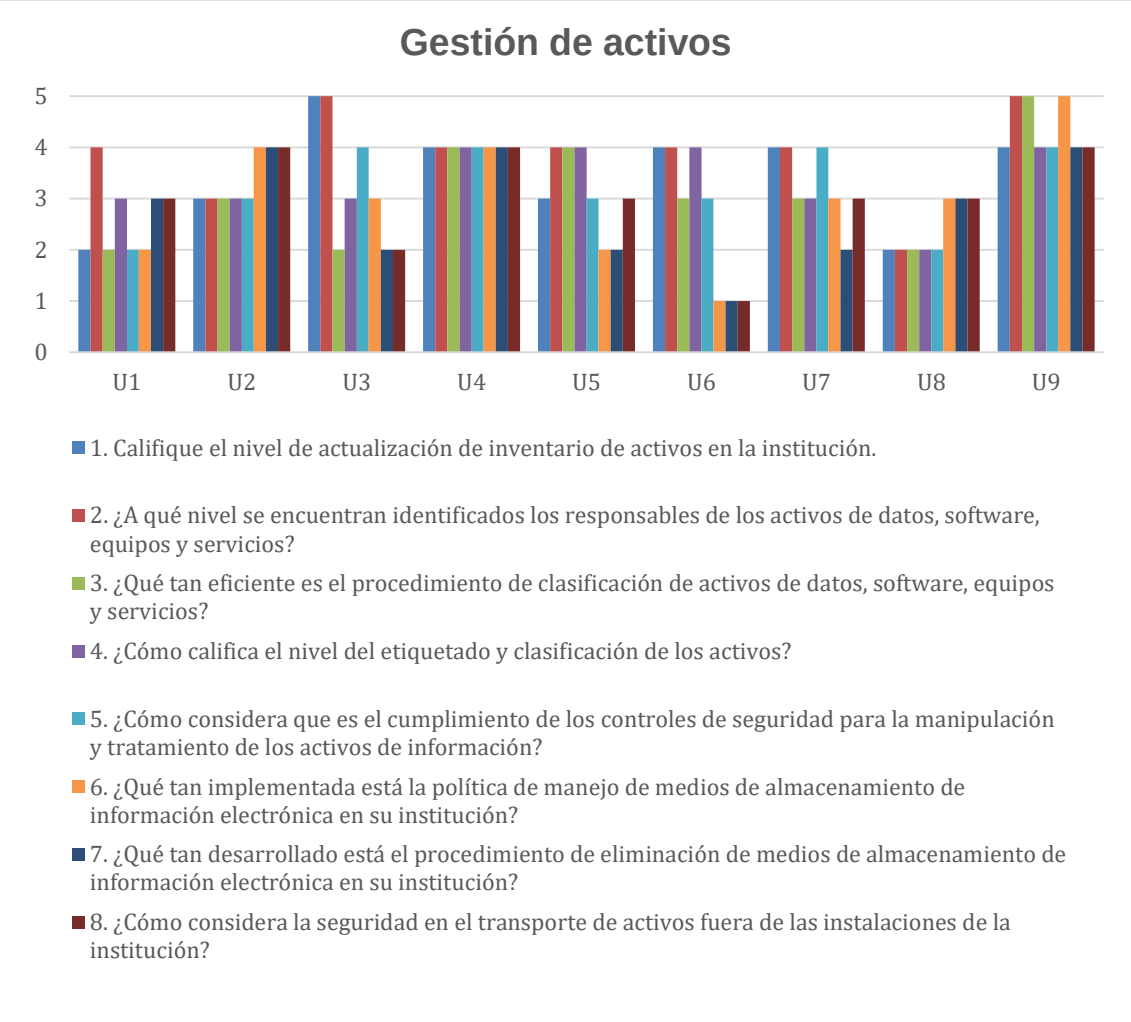
Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Gestión de activos	8	40	Nivel alto	]70% - 100%]	[29-40]
			Nivel medio	]40% - 70%]	[17-28]
			Nivel bajo	[0% - 40%]	[0 - 16]

Tabla 16- Resultados de sección Gestión de Activos

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. Califique el nivel de actualización de inventario de activos en la institución.	B	M	O	A	M	A	A	B	A
2. ¿A qué nivel se encuentran identificados los responsables de los activos de datos, software, equipos y servicios?	A	M	O	A	A	A	A	B	O
3. ¿Qué tan eficiente es el procedimiento de clasificación de activos de datos, software, equipos y servicios?	B	M	B	A	A	M	M	B	O
4. ¿Cómo califica el nivel del etiquetado y clasificación de los activos?	M	M	M	A	A	A	M	B	A
5. ¿Cómo considera que es el cumplimiento de los controles de seguridad para la manipulación y tratamiento de los activos de información?	B	M	A	A	M	M	A	B	A
6. ¿Qué tan implementada está la política de manejo de medios de almacenamiento de información electrónica en su institución?	B	A	M	A	B	N	M	M	O

7. ¿Qué tan desarrollado está el procedimiento de eliminación de medios de almacenamiento de información electrónica en su institución?	M	A	B	A	B	N	B	M	A
8. ¿Cómo considera la seguridad en el transporte de activos fuera de las instalaciones de la institución?	M	A	B	A	M	N	M	M	A
Total	21	27	26	32	25	21	26	19	35

Tabla 17- Resultados de respuesta Gestión de Activos



Las universidades encuestadas en su mayoría tienen bien identificada la persona que desempeñará el cargo de responsable de los activos, pero pierden un poco el interés a la hora de considerar el cumplimiento de los controles para la manipulación de dichos activos, así como también el transporte de estos fuera de las instalaciones. Por otro lado, le dan una importancia media a la actualización de los activos en la institución y del etiquetado y clasificación de estos lo que puede impactar financieramente a la institución.

La tendencia media baja reflejada con respecto a la política de manipulación de medios de almacenamiento de electrónico y su destrucción impacta la seguridad en estas instituciones ya que el nivel de confidencialidad con el que se debe manejar esta información es alto porque puede incluir datos personales de empleados,

estudiantes, proveedores, etc.

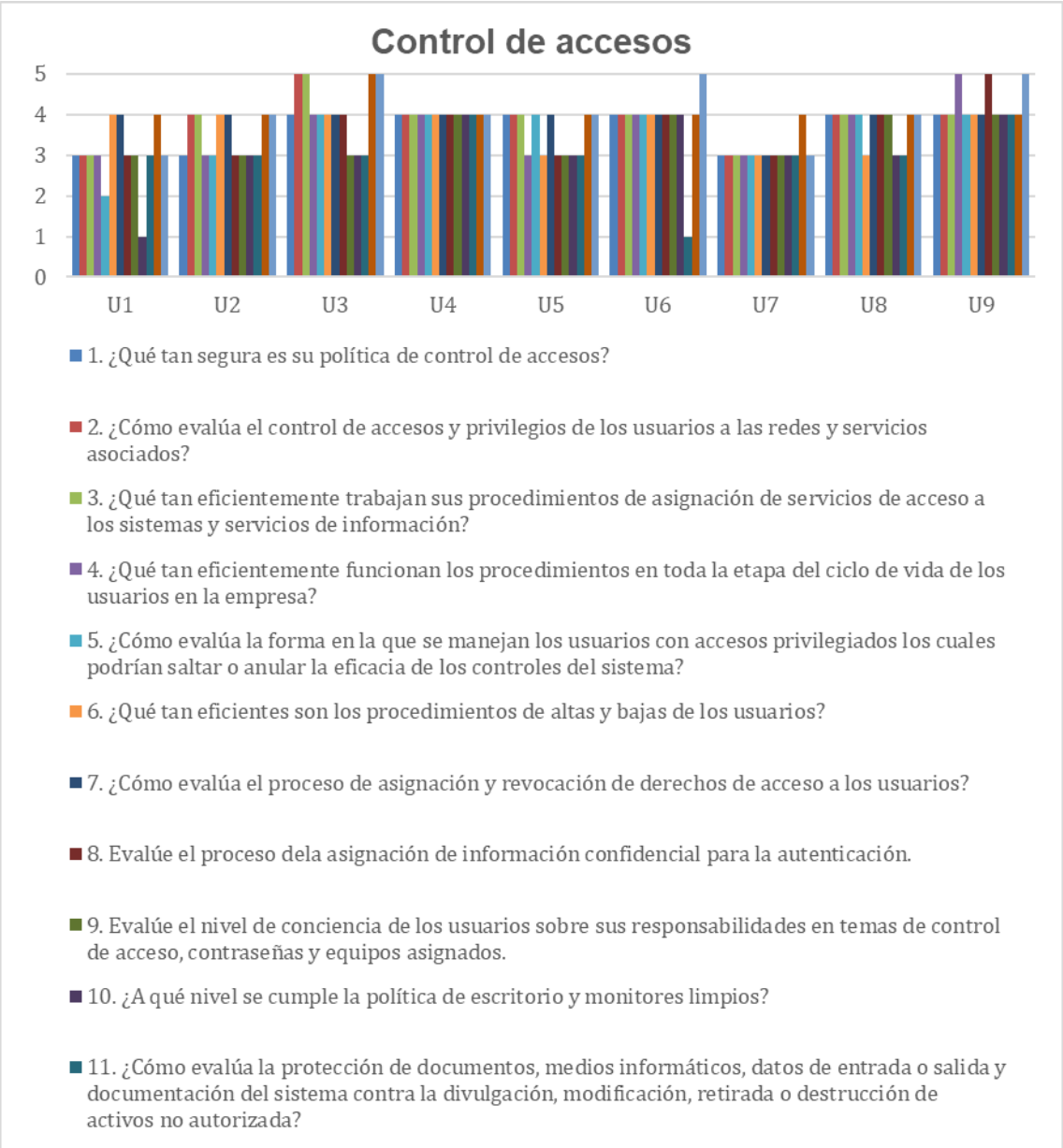
Control de accesos

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Control de Accesos	13	65	Nivel alto	]70% - 100%]	[47-65]
			Nivel medio	]40% - 70%]	[27-46]
			Nivel bajo	[0% - 40%]	[0 - 26]

Tabla 18- Resultados de sección Control de Accesos

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Qué tan segura es su política de control de accesos?	M	M	A	A	A	A	M	A	A
2. ¿Cómo evalúa el control de accesos y privilegios de los usuarios a las redes y servicios asociados?	M	A	O	A	A	A	M	A	A
3. ¿Qué tan eficientemente trabajan sus procedimientos de asignación de servicios de acceso a los sistemas y servicios de información?	M	A	O	A	A	A	M	A	A
4. ¿Qué tan eficientemente funcionan los procedimientos en toda la etapa del ciclo de vida de los usuarios en la empresa?	M	M	A	A	M	A	M	A	O
5. ¿Cómo evalúa la forma en la que se manejan los usuarios con accesos privilegiados los cuales podrían saltar o anular la eficacia de los controles del sistema?	B	M	A	A	A	A	M	A	A
6. ¿Qué tan eficientes son los procedimientos de altas y bajas de los usuarios?	A	A	A	A	M	A	M	M	A
7. ¿Cómo evalúa el proceso de asignación y revocación de derechos de acceso a los usuarios?	A	A	A	A	A	A	M	A	A
8. Evalúe el proceso de la asignación de información confidencial para la autenticación.	M	M	A	A	M	A	M	A	O
9. Evalúe el nivel de conciencia de los usuarios sobre sus responsabilidades en temas de control de acceso, contraseñas y equipos asignados.	M	M	M	A	M	A	M	A	A
10. ¿A qué nivel se cumple la política de escritorio y monitores limpios?	N	M	M	A	M	A	M	M	A
11. ¿Cómo evalúa la protección de documentos, medios informáticos, datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizada?	M	M	M	A	M	N	M	M	A
12. ¿Qué tan efectivo es la restricción de acceso al código fuente de las aplicaciones software a usuarios no autorizados?	A	A	O	A	A	A	A	A	A
13. ¿Qué tan seguro es su sistema de login a los sistemas de información?	M	A	O	A	A	O	M	A	O
Total	39	45	53	52	46	50	40	49	55

Tabla 19- Resultados de respuesta Control de Accesos



Dado que todas las universidades cuentan con un documento formal con relación al control de accesos, en su mayoría cumple en un nivel alto con los controles necesarios para implementar seguridad de accesos para personal. Esto brinda eficiencia en el proceso de asignación de acceso a los sistemas de información porque todas ellas implementan un ciclo de vida para las cuentas de usuarios de sus colaboradores, desarrollando controles de altas y bajas de estos en los sistemas, así como la determinación de si se lleva una correcta administración de las cuentas privilegiadas, creando conciencia sobre estos usuarios en las responsabilidades y roles que sus accesos conllevan con relación a la seguridad de la información.

Sin embargo, en la mayoría para las instituciones el reglamento de escritorios limpios tiene una importancia media tomando en cuenta que esta es una de las políticas de

gran importancia para garantizar la seguridad de la información, por lo que debería de tener una importancia alta para evitar la fuga de información. Finalmente se evidencia que todas las universidades poseen una correcta segregación de funciones en el ámbito del acceso al código fuente de los sistemas de información, implementando un sistema de login que según se evidencia en la encuesta la mayoría de instituciones poseen un alto nivel de implementación.

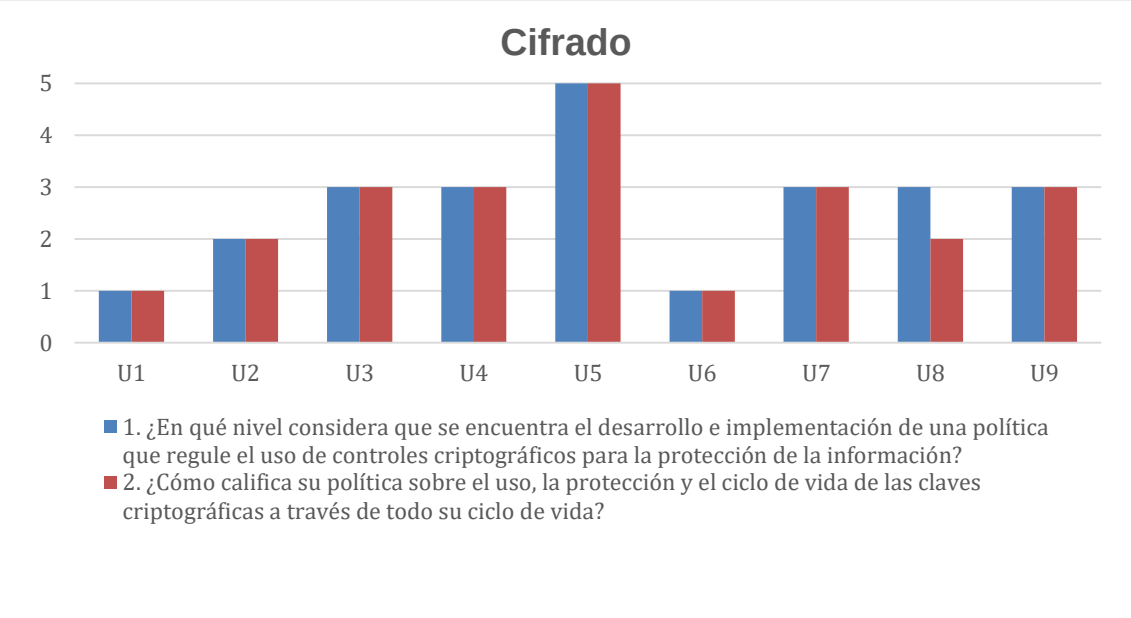
Cifrado

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Cifrado	2	10	Nivel alto	]70% - 100%]	[8-10]
			Nivel medio	]40% - 70%]	[5-7]
			Nivel bajo	[0% - 40%]	[0 - 4]

Tabla 20- Resultados de sección Cifrado

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿En qué nivel considera que se encuentra el desarrollo e implementación de una política que regule el uso de controles criptográficos para la protección de la información?	N	B	M	M	O	N	M	M	M
2. ¿Cómo califica su política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida?	N	B	M	M	O	N	M	B	M
Total	2	4	6	6	10	2	6	5	6

Tabla 21- Resultados de respuesta Cifrado



Solo una de todas las universidades muestra nivel óptimo en el tema de la política de implementación de controles criptográficos para la protección de la información, la cual también incluye la duración de la vida de sus llaves; esto impacta directamente la seguridad ya que hoy en día como es bien conocido en la rama, la

criptografía juega un papel importante para asegurar los sistemas de información digital.

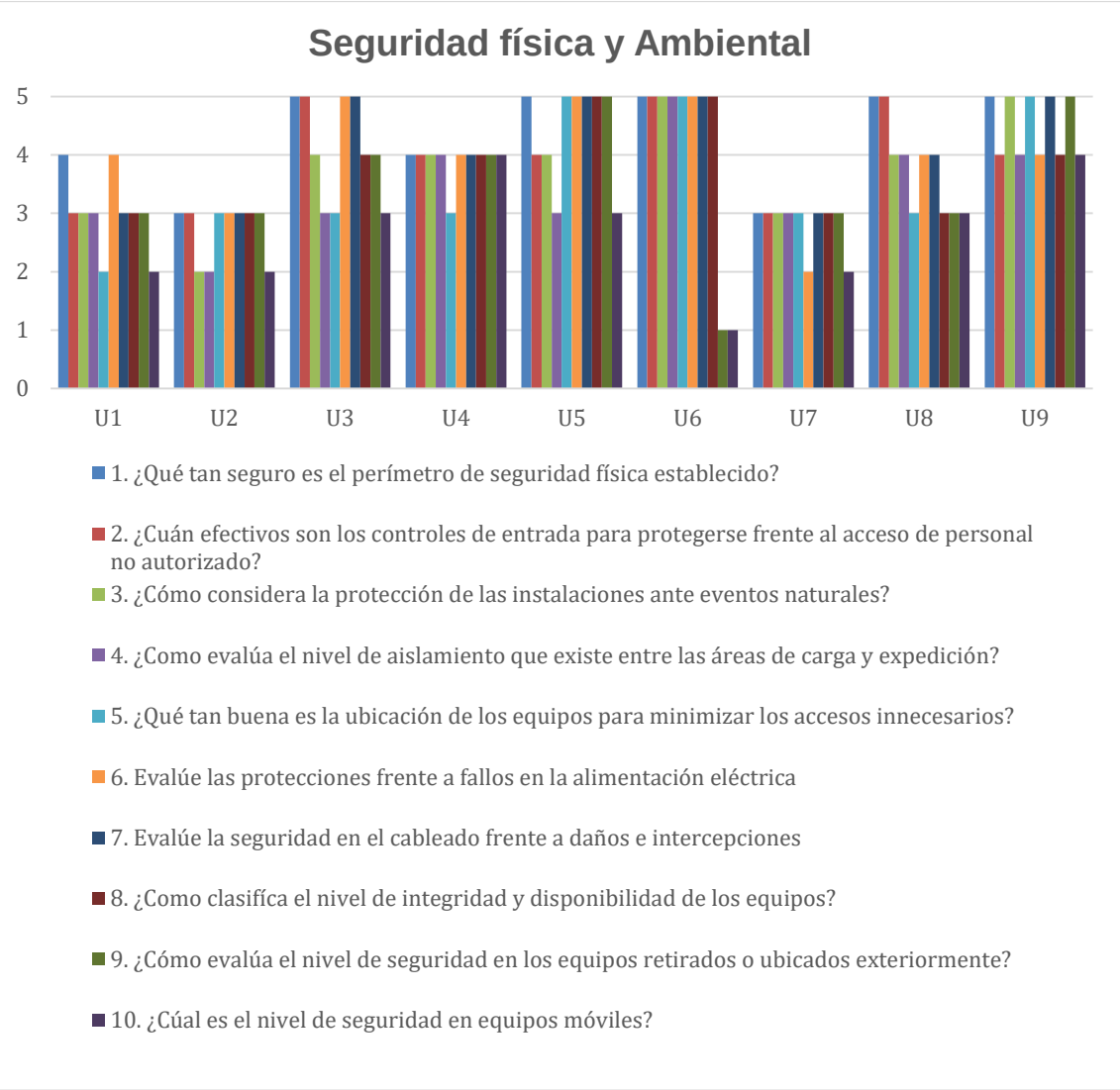
Seguridad física y Ambiental

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Seguridad Física y Ambiental	10	50	Nivel alto	]70% - 100%]	[36-50]
			Nivel medio	]40% - 70%]	[21-35]
			Nivel bajo	[0% - 40%]	[0 - 20]

Tabla 22- Resultados de sección Seguridad Física y Ambiental

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Qué tan seguro es el perímetro de seguridad física establecido?	A	M	O	A	O	O	M	O	O
2. ¿Cuán efectivos son los controles de entrada para protegerse frente al acceso de personal no autorizado?	M	M	O	A	A	O	M	O	A
3. ¿Cómo considera la protección de las instalaciones ante eventos naturales?	M	B	A	A	A	O	M	A	O
4. ¿Cómo evalúa el nivel de aislamiento que existe entre las áreas de carga y expedición?	M	B	M	A	M	O	M	A	A
5. ¿Qué tan buena es la ubicación de los equipos para minimizar los accesos innecesarios?	B	M	M	M	O	O	M	M	O
6. Evalúe las protecciones frente a fallos en la alimentación eléctrica	A	M	O	A	O	O	B	A	A
7. Evalúe la seguridad en el cableado frente a daños e intercepciones	M	M	O	A	O	O	M	A	O
8. ¿Cómo clasifica el nivel de integridad y disponibilidad de los equipos?	M	M	A	A	O	O	M	M	A
9. ¿Cómo evalúa el nivel de seguridad en los equipos retirados o ubicados exteriormente?	M	M	A	A	O	N	M	M	O
10. ¿Cuál es el nivel de seguridad en equipos móviles?	B	B	M	A	M	N	B	M	A
Total	30	27	41	39	44	42	28	38	45

Tabla 23- Resultados de respuesta Seguridad Física y Ambiental



No importando la ubicación geográfica de la universidad, antigüedad, cantidad de alumnos o ingresos mensuales, todas enfocan de una manera aceptable la necesidad de fortalecer la seguridad física de sus instalaciones, las cuales pueden incluir la entrada principal, aislamiento entre áreas de carga y expedición, protección contra fallos de electricidad y cableado lo cual puede ser por los altos índices de violencia que desafortunadamente sufre nuestro país ya que además muestran nivel alto en la integridad y disponibilidad de los equipos como en su seguridad cuando son retirados de las instalaciones. Solo muestran una tendencia baja en la seguridad móvil.

Seguridad en la Operativa

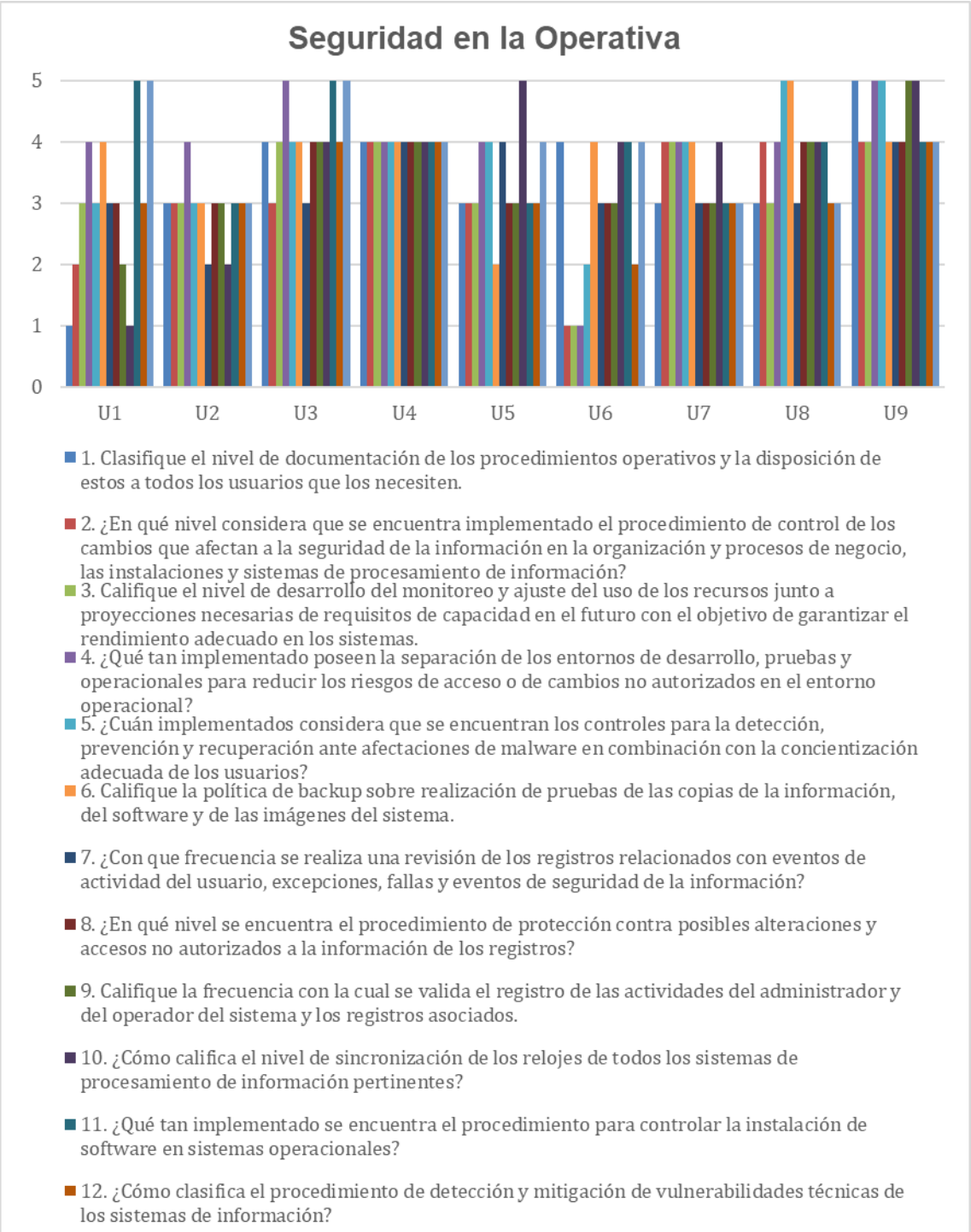
Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Seguridad en la Operativa	13	65	Nivel alto	]70% - 100%]	[47-65]
			Nivel medio	]40% - 70%]	[27-46]

		Nivel bajo	[0% - 40%]	[0 - 26]	

Tabla 24- Resultados de sección Seguridad en la Operativa

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. Clasifique el nivel de documentación de los procedimientos operativos y la disposición de estos a todos los usuarios que los necesiten.	N	M	A	A	M	A	M	M	O
2. ¿En qué nivel considera que se encuentra implementado el procedimiento de control de los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información?	B	M	M	A	M	N	A	A	A
3. Califique el nivel de desarrollo del monitoreo y ajuste del uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.	M	M	A	A	M	N	A	M	A
4. ¿Qué tan implementado poseen la separación de los entornos de desarrollo, pruebas y operacionales para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional?	A	A	O	A	A	N	A	A	O
5. ¿Cuán implementados considera que se encuentran los controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios?	M	M	A	A	A	B	A	O	O
6. Califique la política de backup sobre realización de pruebas de las copias de la información, del software y de las imágenes del sistema.	A	M	A	A	B	A	A	O	A
7. ¿Con que frecuencia se realiza una revisión de los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información?	M	B	M	A	A	M	M	M	A
8. ¿En qué nivel se encuentra el procedimiento de protección contra posibles alteraciones y accesos no autorizados a la información de los registros?	M	M	A	A	M	M	M	A	A
9. Califique la frecuencia con la cual se valida el registro de las actividades del administrador y del operador del sistema y los registros asociados.	B	M	A	A	M	M	M	A	O
10. ¿Cómo califica el nivel de sincronización de los relojes de todos los sistemas de procesamiento de información pertinentes?	N	B	A	A	O	A	A	A	O
11. ¿Qué tan implementado se encuentra el procedimiento para controlar la instalación de software en sistemas operacionales?	O	M	O	A	M	A	M	A	A
12. ¿Cómo clasifica el procedimiento de detección y mitigación de vulnerabilidades técnicas de los sistemas de información?	M	M	A	A	M	B	M	M	A
13. Indique el nivel en el cual se encuentra el procedimiento de control y restricción de instalación de software por parte de los usuarios.	O	M	O	A	A	A	M	M	A
Total	39	38	53	52	44	36	45	49	57

Tabla 25- Resultados de respuesta Seguridad en la Operativa



Una universidad del total encuestado indicó que no posee procedimientos operativos para su sistema de información esto conlleva a que no tiene implementado un control de cambios sobre sus sistemas críticos. Al contrario, el resto de las universidades al poseer un procedimiento operativo sí cuenta con controles que garanticen la revisión de los cambios en los sistemas y monitoreo de los mismos. En su mayoría las universidades poseen un nivel de separación de entornos de desarrollo, pruebas y operación de los sistemas bien definido, así como también la consideración de los controles para detección, prevención y recuperación ante afectaciones de malware

y la frecuencia de revisión de registros de eventos de seguridad excepciones y fallas. Además, poseen un nivel aceptable con su política de respaldo de datos, revisión de registros de los administradores y operadores del sistema, sincronización de relojes y las instalaciones de software en estos sistemas.

Finalmente clasifica de manera correcta los procedimientos que detectan y mitigan vulnerabilidades técnicas en los sistemas y los controles y restricciones del software por parte de los usuarios.

Según las respuestas obtenidas se puede visualizar que las universidades sin importar la cantidad de estudiantes, los ingresos económicos o la cantidad de años de estar en funcionamientos, han identificado la importancia de la seguridad de información en sus procesos operativos y han invertido recursos para tener niveles deseados de esta.

Seguridad en las Telecomunicaciones

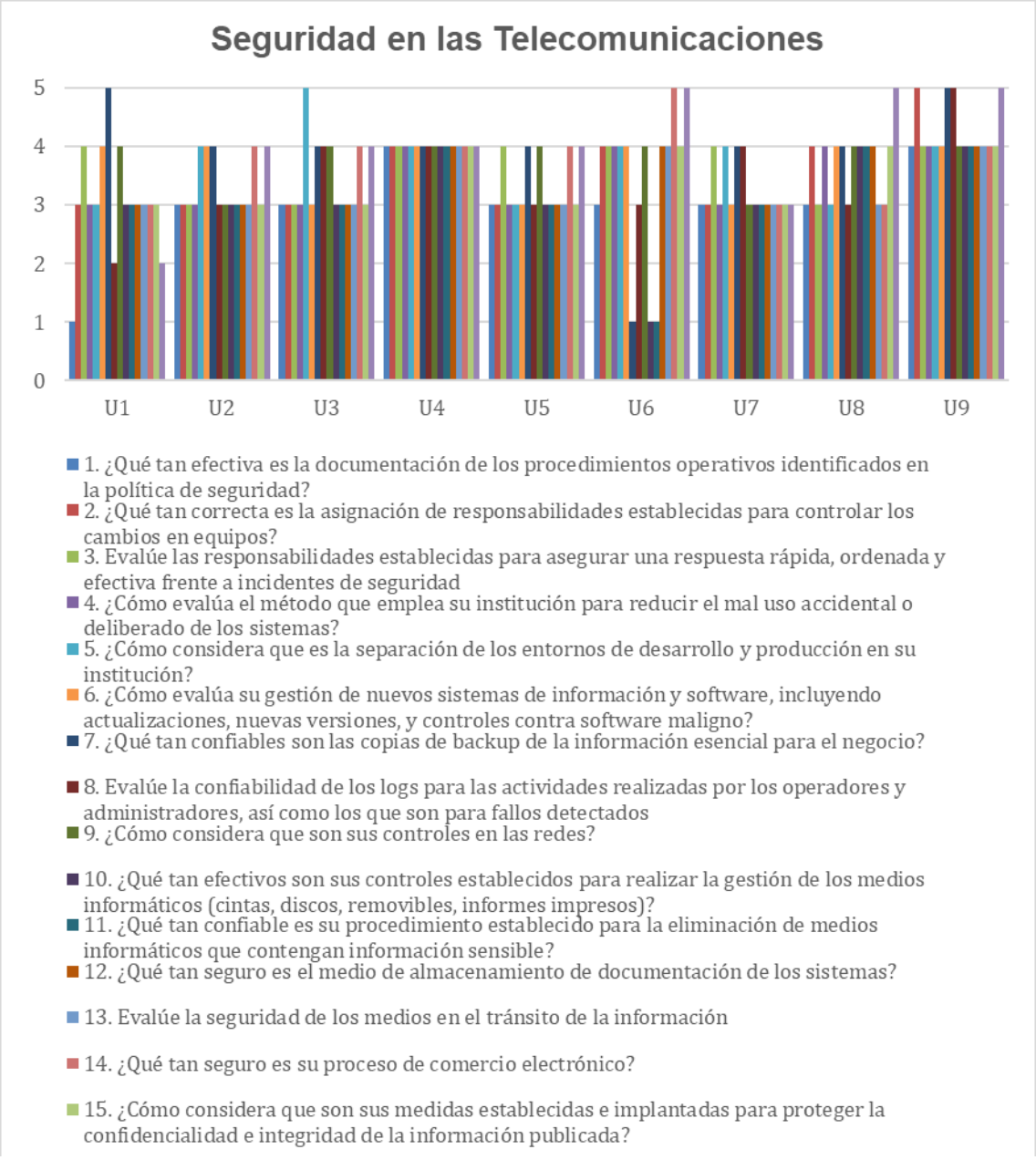
Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Seguridad en las Telecomunicaciones	16	80	Nivel alto	]70% - 100%]	[57-80]
			Nivel medio	]40% - 70%]	[33-56]
			Nivel bajo	[0% - 40%]	[0 - 32]

Tabla 26- Resultados de sección Seguridad en las Telecomunicaciones

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Qué tan efectiva es la documentación de los procedimientos operativos identificados en la política de seguridad?	N	M	M	A	M	M	M	M	A
2. ¿Qué tan correcta es la asignación de responsabilidades establecidas para controlar los cambios en equipos?	M	M	M	A	M	A	M	A	O
3. Evalúe las responsabilidades establecidas para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	A	M	M	A	A	A	A	M	A
4. ¿Cómo evalúa el método que emplea su institución para reducir el mal uso accidental o deliberado de los sistemas?	M	M	M	A	M	A	M	A	A
5. ¿Cómo considera que es la separación de los entornos de desarrollo y producción en su institución?	M	A	O	A	M	A	A	M	A
6. ¿Cómo evalúa su gestión de nuevos sistemas de información y software, incluyendo actualizaciones, nuevas versiones, y controles contra software maligno?	A	A	M	A	M	A	M	A	A
7. ¿Qué tan confiables son las copias de backup de la información esencial para el negocio?	O	A	A	A	A	N	A	A	O
8. Evalúe la confiabilidad de los logs para las actividades realizadas por los operadores y administradores, así como los que son para fallos detectados	B	M	A	A	M	M	A	M	O
9. ¿Cómo considera que son sus controles en las redes?	A	M	A	A	A	A	M	A	A
10. ¿Qué tan efectivos son sus controles establecidos para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	M	M	M	A	M	N	M	A	A

11. ¿Qué tan confiable es su procedimiento establecido para la eliminación de medios informáticos que contengan información sensible?	M	M	M	A	M	N	M	A	A
12. ¿Qué tan seguro es el medio de almacenamiento de documentación de los sistemas?	M	M	M	A	M	A	M	A	A
13. Evalúe la seguridad de los medios en el tránsito de la información	M	M	M	A	M	A	M	M	A
14. ¿Qué tan seguro es su proceso de comercio electrónico?	M	A	A	A	A	O	M	M	A
15. ¿Cómo considera que son sus medidas establecidas e implantadas para proteger la confidencialidad e integridad de la información publicada?	M	M	M	A	M	A	M	A	A
16. ¿Qué tan efectivas son las medidas de seguridad en las transacciones en línea?	B	A	A	A	A	O	M	O	O
Total	49	53	55	64	53	55	52	59	68

Tabla 27- Resultados de respuesta Seguridad en las Telecomunicaciones



Las universidades presenta una efectividad media en la documentación de los procedimientos operativos que se identifican en las política de seguridad que si bien se encuentran en niveles aceptables no son los niveles recomendados y deseables que deberían de tener las instituciones, esto debido a que si bien es importante poseer una política implementada también es de suma importancia que todos los procedimiento estén debidamente documentados para permitir que las asignación de las responsabilidades para el control de cambios en los equipos sea la más adecuada.

La correcta asignación de las responsabilidades de cada persona dentro de la institución permite minimizar el impacto ante cualquier incidente de seguridad que se presente y como se puede observar en las respuestas sin importar los puntos de diferenciación entre las universidades como son la cantidad de alumnos, el nivel económico y la cantidad de años que tiene en funcionamiento, estas poseen niveles adecuados en la asignación de las responsabilidades lo que les permite tener una reacción aceptable ante estos casos.

La mayoría de las universidades posee un nivel moderado en los métodos a través de los cuales reducen el mal uso de los sistemas mientras que poseen niveles deseables en la gestión de nuevos sistemas de información y en la confiabilidad de los backup y logs de las actividades realizadas por los operadores y administradores.

Las redes de comunicación son la vía de acceso y transmisión de información hacia los sistemas por lo que la implementación de controles de acceso a las mismas es de suma importancia y como se observa las universidades están conscientes de esto ya que la mayoría posee niveles altos para estos, de igual forma es muy importante que se posean nivel deseables de gestión y eliminación de medios informáticos que contengan información sensible, así como también en la seguridad de los medios de almacenamiento de los sistemas, sin embargo, si bien las universidades poseen niveles moderados para estos controles deben de invertir tiempo, dinero y recursos para mejorar estos controles y garantizar la confidencialidad de la información.

La confidencialidad e integridad son dos de los pilares fundamentales de la seguridad de información, por lo que si una organización se encuentra comprometida con la misma esta debe de dirigir sus esfuerzos a tener niveles altos en las medidas implementadas para garantizar los mismos, es por esta razón que aunque las universidades tengan en su mayoría un nivel moderado deben de

esforzarse más para mejorar sus niveles en este sentido.

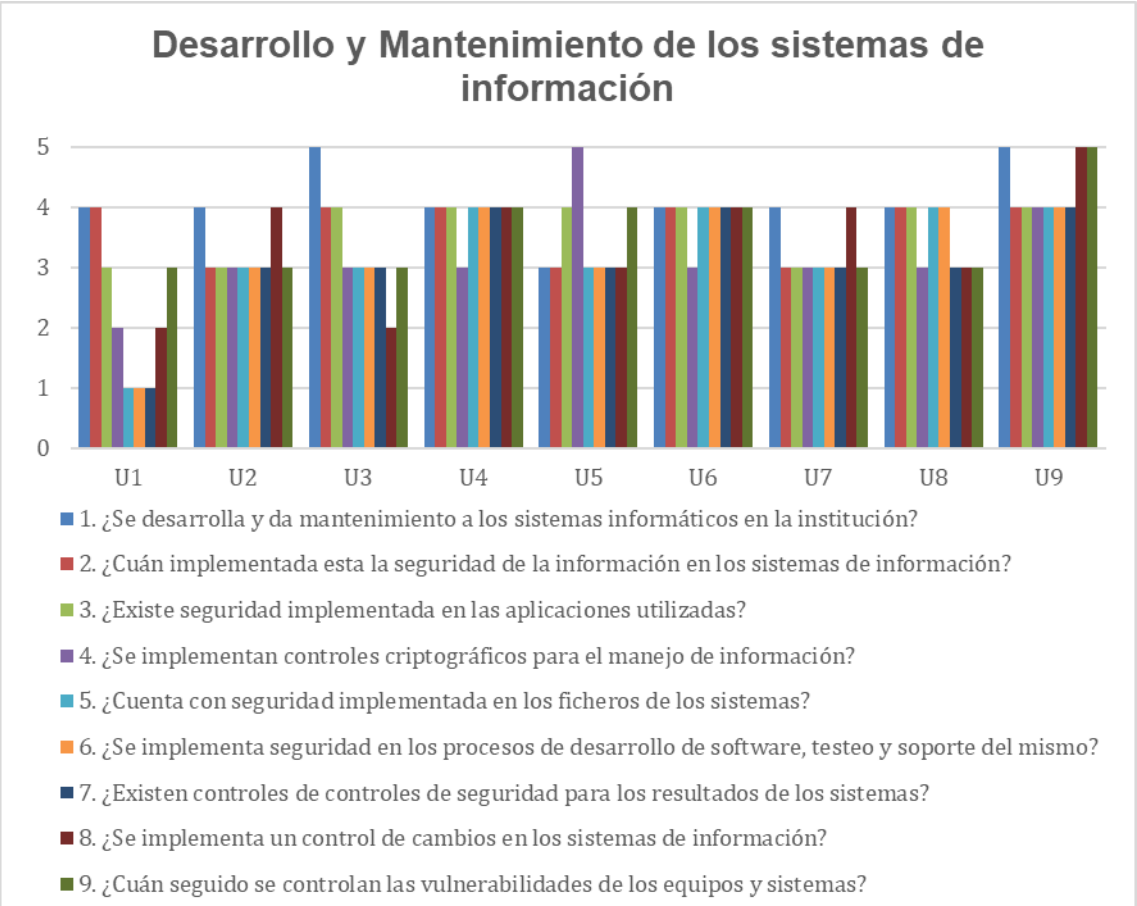
Desarrollo y Mantenimiento de los sistemas de información

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Desarrollo y Mantenimiento de los sistemas informáticos	9	45	Nivel alto	]70% - 100%]	[33-45]
			Nivel medio	]40% - 70%]	[19-32]
			Nivel bajo	[0% - 40%]	[0 - 18]

Tabla 28- Resultados de sección Desarrollo y Mantenimiento de los sistemas de información

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Se desarrolla y da mantenimiento a los sistemas informáticos en la institución?	A	A	O	A	M	A	A	A	O
2. ¿Cuán implementada esta la seguridad de la información en los sistemas de información?	A	M	A	A	M	A	M	A	A
3. ¿Existe seguridad implementada en las aplicaciones utilizadas?	M	M	A	A	A	A	M	A	A
4. ¿Se implementan controles criptográficos para el manejo de información?	B	M	M	M	O	M	M	M	A
5. ¿Cuenta con seguridad implementada en los ficheros de los sistemas?	N	M	M	A	M	A	M	A	A
6. ¿Se implementa seguridad en los procesos de desarrollo de software, testeo y soporte del mismo?	N	M	M	A	M	A	M	A	A
7. ¿Existen controles de controles de seguridad para los resultados de los sistemas?	N	M	M	A	M	A	M	M	A
8. ¿Se implementa un control de cambios en los sistemas de información?	B	A	B	A	M	A	A	M	O
9. ¿Cuán seguido se controlan las vulnerabilidades de los equipos y sistemas?	M	M	M	A	A	A	M	M	O
Total	21	29	30	35	31	35	29	32	39

Tabla 29- Resultados de respuesta Desarrollo y Mantenimiento de los sistemas de información



El desarrollo y mantenimiento en los sistemas muestra una tendencia alta en las universidades encuestadas, mostrando igualmente que aplican seguridad en estos procesos y en las aplicaciones que utilizan, sus ficheros, testing, soporte, resultados, control de cambios y el control de vulnerabilidades de los equipos.

Gestión de Incidentes de Seguridad

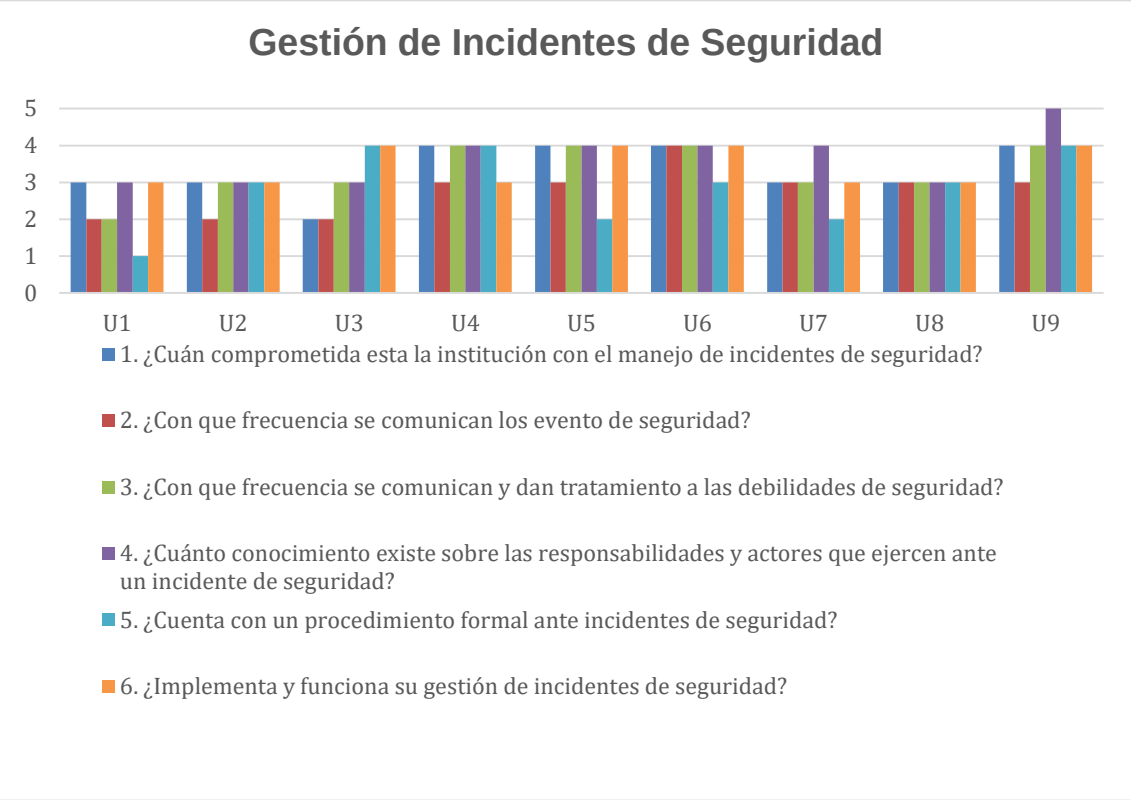
Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Gestión de Incidentes de Seguridad	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]

Tabla 30- Resultados de sección Gestión de Incidentes de Seguridad

Preguntas	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Cuán comprometida esta la institución con el manejo de incidentes de seguridad?	M	M	B	A	A	A	M	M	A
2. ¿Con que frecuencia se comunican los eventos de seguridad?	B	B	B	M	M	A	M	M	M
3. ¿Con que frecuencia se comunican y dan tratamiento a las debilidades de seguridad?	B	M	M	A	A	A	M	M	A
4. ¿Cuánto conocimiento existe sobre las responsabilidades y actores que ejercen ante un incidente de seguridad?	M	M	M	A	A	A	A	M	O
5. ¿Cuenta con un procedimiento formal ante incidentes de seguridad?	N	M	A	A	B	M	B	M	A

6. ¿Implementa y funciona su gestión de incidentes de seguridad?	M	M	A	M	A	A	M	M	A
Total	14	17	18	22	21	23	18	18	24

Tabla 31- Resultados de respuesta Gestión de Incidentes de Seguridad



En la encuesta, se evidencia que las universidades cuentan con basto conocimiento sobre la implementación de un plan de gestión de Incidentes de Seguridad, pero la mayoría de estas, no se ha implementado este plan, y al no tener un procedimiento o documento propiamente definido, no conocen que procesos o pasos se deben seguir para mitigar un escenario de riesgo. Esto hace que no exista un compromiso para el manejo de incidentes y por ende una correcta comunicación con el personal de cómo actuar ante un evento inesperado. Se evidencia que en la mayoría de las universidades no existe un plan de tratamiento de las debilidades y por esta razón, no se puede determinar si funciona su plan de gestión de incidentes de Seguridad.

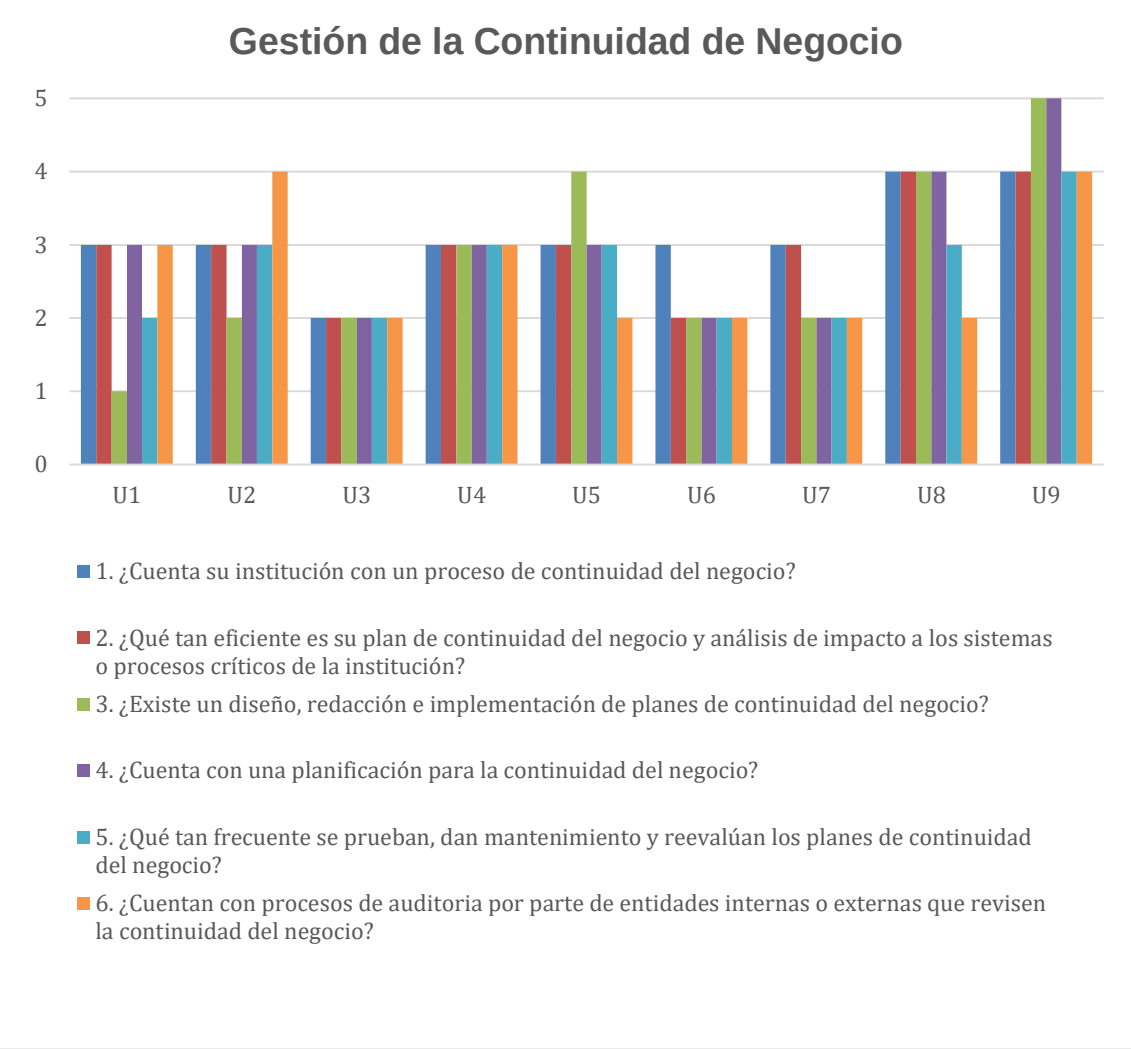
Gestión de la Continuidad de Negocio

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Gestión de la Continuidad del Negocio	6	30	Nivel alto	]70% - 100%]	[22-30]
			Nivel medio	]40% - 70%]	[13-21]
			Nivel bajo	[0% - 40%]	[0 - 12]

Tabla 32- Resultados de sección Continuidad del Negocio

Pregunta	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Cuenta su institución con un proceso de continuidad del negocio?	M	M	B	M	M	M	M	A	A
2. ¿Qué tan eficiente es su plan de continuidad del negocio y análisis de impacto a los sistemas o procesos críticos de la institución?	M	M	B	M	M	B	M	A	A
3. ¿Existe un diseño, redacción e implementación de planes de continuidad del negocio?	N	B	B	M	A	B	B	A	O
4. ¿Cuenta con una planificación para la continuidad del negocio?	M	M	B	M	M	B	B	A	O
5. ¿Qué tan frecuente se prueban, dan mantenimiento y reevalúan los planes de continuidad del negocio?	B	M	B	M	M	B	B	M	A
6. ¿Cuentan con procesos de auditoria por parte de entidades internas o externas que revisen la continuidad del negocio?	M	A	B	M	B	B	B	B	A
Total	15	18	12	18	18	13	14	21	26

Tabla 33- Resultados de respuesta Continuidad del Negocio



Logramos evidenciar que casi todas las universidades poseen un proceso de continuidad del negocio implementado. De estas, una universidad indica que su plan a pesar de estar implementado, no considera que sea eficiente para el análisis de los impactos en los sistemas y procesos críticos que operan en sus respectivas instituciones. Aunque la mayoría posee un plan de continuidad del negocio, estos

no cuentan con una planificación de levantamiento de procesos críticos, pruebas y ejecución de resultados con respecto a este análisis. Esto se debe, a que según lo indicado, estas instituciones no se les brinda un proceso de auditoría que revise esta tema tan importante, es por ello, que a pesar de tener un plan de continuidad implementado, no pueden garantizar que vaya a responder ante todos los posibles eventos que puedan llegar a pasar.

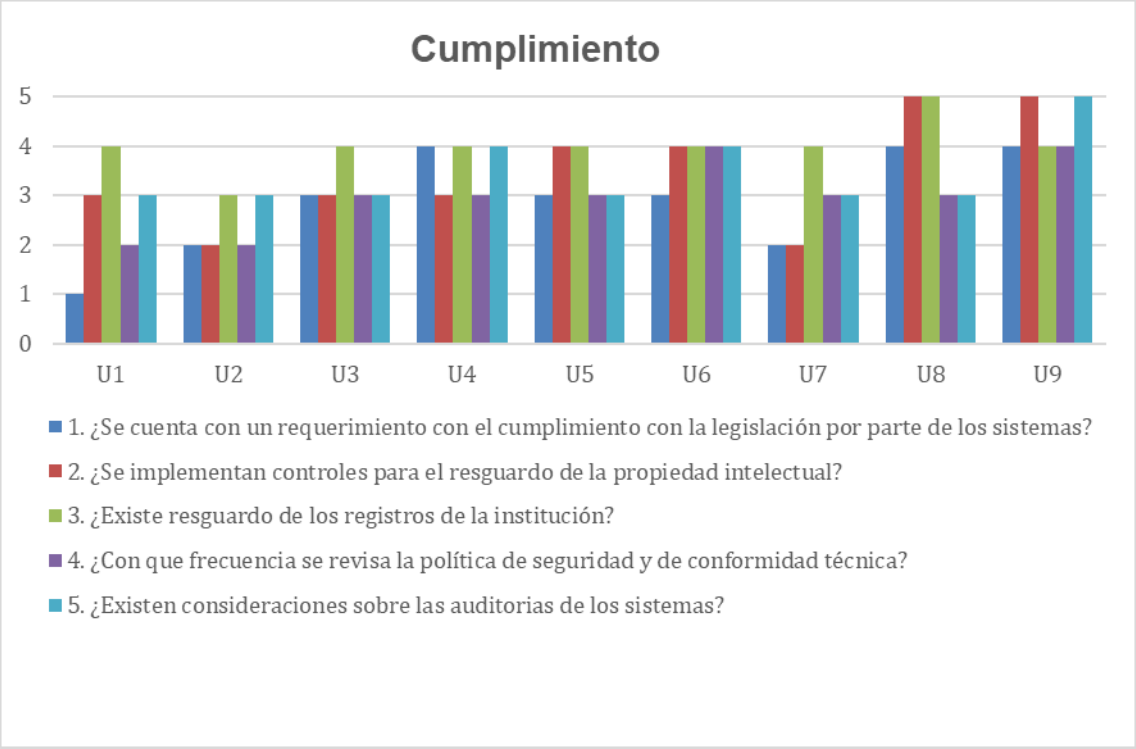
Cumplimiento

Sección de la encuesta	Número de preguntas	Puntos máximos	Nivel de implementación	Porcentaje	Rango de valores
Cumplimiento regulatorio	5	25	Nivel alto	]70% - 100%]	[19-25]
			Nivel medio	]40% - 70%]	[11-18]
			Nivel bajo	[0% - 40%]	[0 - 10]

Tabla 34- Resultados de sección Cumplimiento

Pregunta	U1	U2	U3	U4	U5	U6	U7	U8	U9
1. ¿Se cuenta con un requerimiento con el cumplimiento con la legislación por parte de los sistemas?	N	B	M	A	M	M	B	A	A
2. ¿Se implementan controles para el resguardo de la propiedad intelectual?	M	B	M	M	A	A	B	O	O
3. ¿Existe resguardo de los registros de la institución?	A	M	A	A	A	A	A	O	A
4. ¿Con que frecuencia se revisa la política de seguridad y de conformidad técnica?	B	B	M	M	M	A	M	M	A
5. ¿Existen consideraciones sobre las auditorias de los sistemas?	M	M	M	A	M	A	M	M	O
Total	13	12	16	18	17	19	14	20	22

Tabla 35- Resultados de respuesta Cumplimiento



Por lo general las universidades guardan de manera alta y óptima los registros de la información y consideran la importancia de las auditorías de los sistemas, además de revisar frecuentemente la política de seguridad y la conformidad técnica. Por otro lado, solo una de todas las universidades encuestadas mostró un nivel bajo en los controles para el resguardo de la propiedad intelectual, así como una mostró que no cuenta con un requerimiento de complimiento con las legislaciones con respecto a los sistemas, dos la tienen a un nivel bajo y el resto se encuentran en un nivel medio alto.

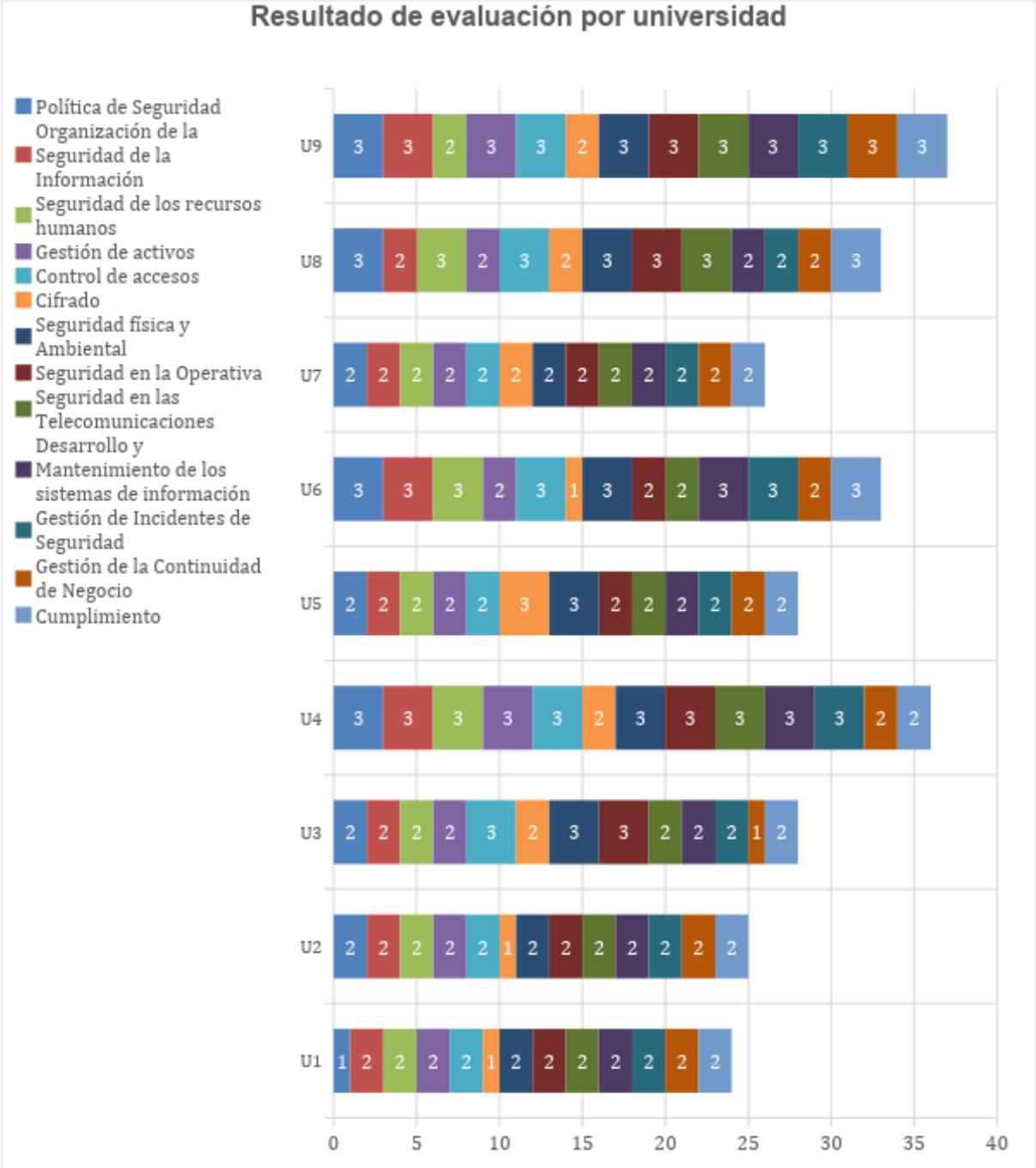
La mayoría de las universidades demostró que posee un resguardo de los registros de la institución. Por ser entidades reguladas por el Ministerio de Educación, estas poseen fuertes controles con el tema de cumplimiento legal, sin embargo, la mayoría no posee controles de o requerimientos para garantizar el cumplimiento de la legislación por parte de los sistemas. Por ser instituciones reguladas por un Ministerio, poseen altas consideraciones sobre el tema de revisión de auditorías en sus sistemas de información y el manejo de la propiedad intelectual. Se evidencia, que un alto porcentaje, revisa frecuentemente su política de seguridad y la acopla con los controles regulatorios necesarios, a pesar de esto, existen dos universidades que indicaron que tienen poco control sobre su actualización de la política.

4.3. Resumen de resultados

En la tabla y grafica presentadas a continuación se muestra el nivel de seguridad de la información que poseen las universidades por sección, basados en los niveles bajo, medio y alto según los porcentajes definidos en la escala de Likert.

Sección	U1	U2	U3	U4	U5	U6	U7	U8	U9
Política de Seguridad	B	M	M	A	M	A	M	A	A
Organización de la Seguridad de la Información	M	M	M	A	M	A	M	M	A
Seguridad de los recursos humanos	M	M	M	A	M	A	M	A	M
Gestión de activos	M	M	M	A	M	M	M	M	A
Control de accesos	M	M	A	A	M	A	M	A	A
Cifrado	B	B	M	M	A	B	M	M	M
Seguridad física y Ambiental	M	M	A	A	A	A	M	A	A
Seguridad en la Operativa	M	M	A	A	M	M	M	A	A
Seguridad en las Telecomunicaciones	M	M	M	A	M	M	M	A	A
Desarrollo y Mantenimiento de los sistemas de información	M	M	M	A	M	A	M	M	A
Gestión de Incidentes de Seguridad	M	M	M	A	M	A	M	M	A
Gestión de la Continuidad de Negocio	M	M	B	M	M	M	M	M	A
Cumplimiento	M	M	M	M	M	A	M	A	A

Tabla 36- Resumen de resultados



Como se observa en la tabla y en la gráfica la mayoría de las universidades posee un nivel medio de seguridad en gran parte de las secciones presentadas en la encuesta, las cuales representan la división de los requerimientos de la ISO 27001:2013. Las secciones en las que la mayoría presenta un nivel alto de seguridad de información son la Seguridad física y ambientes y el control de acceso lo que indica que son las áreas en las que la mayoría de universidades inviertes sus recursos de seguridad de información sin embargo esta inversión en seguridad no se ve definida por ninguno de los factores que caracterizan la funcionalidad de las

universidades definidos al inicio de esta sección por lo que se puede atribuir que la importancia y empeño que emplean para la seguridad se basa en el reconocimiento de la importancia de la seguridad de información por parte de los miembros de la organización.

Es importante aclarar que si bien en las demás áreas la mayoría posee un nivel medio de seguridad de la información el cual es aceptable e indica que estas instituciones ya se encuentran encaminadas a una visión de seguridad de información, no es el nivel deseable para garantizar la disponibilidad, confidencialidad e integridad de la información en todos los procesos de la institución por lo que es necesario que tengan procesos de mejora continua que les permitan elevar el nivel de seguridad de información que poseen, implementando procesos óptimos y confiables que permitan cumplir con los objetivos de negocio.

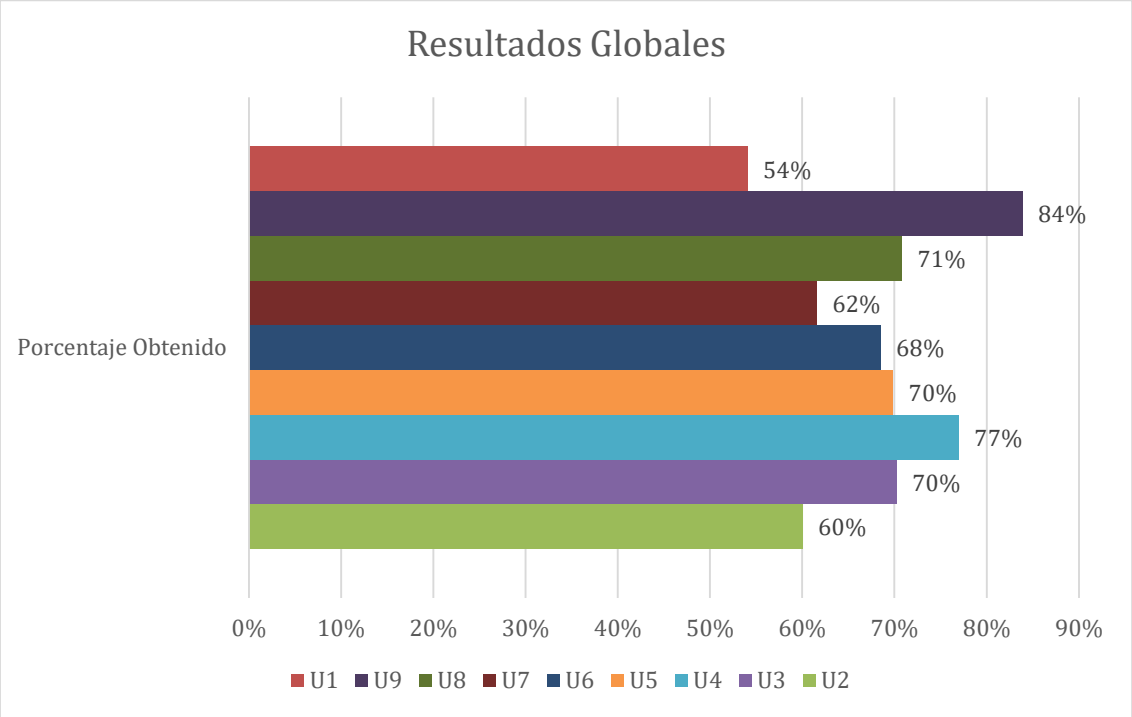
En los dos cuadros que se muestran a continuación se visualiza la cantidad respuestas y los puntos obtenidos en toda la encuesta según la escala de Likert para cada una de las universidades, con lo cual se determina el nivel en el que se encuentra cada universidad de forma global con respecto a todos los requerimientos de la ISO27001:2013.

Universidad	ÓPTIMO	ALTO	MODERADO	POCO	NULO	Total preguntas
U1	3	15	49	22	15	104
U2	0	21	62	21	0	104
U3	15	35	42	12	0	104
U4	0	88	16	0	0	104
U5	10	36	53	5	0	104
U6	14	52	16	8	14	104
U7	0	22	68	14	0	104
U8	9	46	41	8	0	104
U9	29	66	9	0	0	104

Tabla 37- Resultados por universidad

Universidad	ÓPTIMO (5 pts.)	ALTO (4 pts.)	MODERADO (3 pts.)	POCO (2 pts.)	NULO (1 pts.)	Total clasificación	Porcentaje Obtenido	Nivel de clasificación
U1	15	60	147	44	15	281	54%	Nivel Medio
U2	0	84	186	42	0	312	60%	Nivel Medio
U3	75	140	126	24	0	365	70%	Nivel Alto
U4	0	352	48	0	0	400	77%	Nivel Alto
U5	50	144	159	10	0	363	70%	Nivel Medio
U6	70	208	48	16	14	356	68%	Nivel Medio
U7	0	88	204	28	0	320	62%	Nivel Medio
U8	45	184	123	16	0	368	71%	Nivel Alto
U9	145	264	27	0	0	436	84%	Nivel Alto

Tabla 38- Nivel de Clasificación por Universidad



Como podemos observar en los resultados globales del total de las universidades la mayoría posee un nivel medio de seguridad de información lo cual indica que si no poseen un nivel desea y no tienen implementado de manera óptima un Sistema de Gestión de Seguridad de la Información, estas ya se encuentran encaminadas a la

seguridad de información y realizan la implementación de sus procesos en base a las necesidades no solo de la organización sino de la seguridad, lo que las lleva cada vez más cerca de garantizar de forma efectiva y optima la disponibilidad, confidencialidad e integridad de la información en todos los procesos de la institución por lo que es importante que se mantengan en constante mejora para lograr un nivel deseado de la seguridad de la información como lo es el cumplimiento de los requerimientos de la ISO27001.

4.4. CONCLUSIONES

No existe una tendencia identificada entre las universidades que mejor han implementado los requerimientos establecidos en la norma ISO27001:2013, ya que no se encuentran en la misma área de experticia con respecto a las carreras que ofrecen. Por otro lado, son opuestas en antigüedad de estar en el área de educación superior y su diferencia en la cantidad de estudiantes que poseen es grande, y tienen una cuota de mensualidad que difiere una con la otra, lo que muestra que ninguno de estos factos determina su disposición y compromiso ante la buena gestión de la seguridad de la información.

Se observó que la universidad con menor número de estudiantes y que posee una de las cuotas más altas no posee un compromiso sobre la implementación de controles de la seguridad de la información, sin embargo, el número de estudiantes y el ingreso económico no es un factor determinante que garantice de forma general la falta de compromiso con respecto a la seguridad de la información.

Viendo los resultados de todas las universidades se puede definir que no existe un patrón que determine a ciencia cierta qué es lo que afecte directamente que la seguridad de la información en estas instituciones tenga mayor o menor importancia, sino que son factores de compromisos propios de cada universidad que podrían partir de la alta gerencia en ellas y también de los equipos de soporte técnico como tal.

Por lo anteriormente mencionado se rechaza la hipótesis planteada al inicio de esta investigación la cual aseveraba que las universidades no cuentan con un sistema de gestión de la seguridad de la información o se encuentran en un nivel bajo, ya que partiendo que el documento que se tomó como base para realizar la encuesta muestra los requerimientos mínimos que se deben cumplir para implementar un sistema de gestión de la seguridad de la información, se ve reflejado que las universidades han obtenido una puntuación que los clasifica en un nivel medio alto.

5. Referencias

[1] J. G. Arévalo Ascanio, R. A. Bayona Trillos y D. W. Rico Bautista, «Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información,» *Tecnura,* 24 agosto 2015.

[2] A. D. Betancourt, «Diseño De Un Prototipo De Software Para Aplicar Análisis Gap A Los Controles Descritos En El Anexo A De La Norma ISO 27001:2013,» Universidad Tecnológica de Pereira, Pereira, Colombia, 2016.

[3] C. Rafael, G. Ellen y N. Tanya, «Propuesta de Implementación de un SGSI basado en la Norma ISO 27001,» Universidad Don Bosco, Antiguo Cuscatlán, El Salvador, 2016.

[4] D. Abbo, «Information Security Management Accounting,» *Intech,* 2012.

[5] J. Jones , «How to prove your value in information security,» Elsevier, 2014.

[6] V. De Freitas, «Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar,» *Acielo,* 17 Noviembre 2008.

[7] PricewaterhouseCoopers, «http://auditortraining.pwc.com.au/new-iso-high-level-structure-mean/,» [En línea].

[8] M. d. E. d. E. Salvador, «http://www.mined.gob.sv/cda/acreditacion_institucional.htm,» [En línea].

[9] CEGESTI, «Alta estructura y cambios previstos en ISO 9001, ISO 14001 e ISO 45001 para 2015.,» Costa Rica, 2015.

[10] I. O. f. Standardization., ISO/IEC Directives, Part 1 Consolidated ISO Supplement Procedures specific to ISO., Suiza, 2014.

[11] I. Barragán, I. Góngora y E. Martínez, Implementación de Políticas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002., Ecuador: http://www.dspace.espol.edu.ec/handle/123456789/21546, 2011.

[12] R. Linares , M. Patterson y L. Viciedo , «La información a través del tiempo,»

ACIMED , vol. 8, nº 3, 1999.

[13] International Organization For Standarization, «ISO 27001:2013 - Sistemas de Gestión de Seguridad de la Información – Requerimientos,» 2013.

[14] International Organization For Standarization, «ISO 27002:2013 - Código de Práctica para Controles de Seguridad de la Información,» 2013.

[15] International Organization For Standarization, «ISO 27003:2013 - Sistemas de Gestión de Seguridad de la Información - Guía de Implementación,» 2013.

[16] I. O. F. Standarization, «ISO/IEC 27007 - Guía para la auditoría de sistemas de gestión de la seguridad de la información,» 2017.

[17] A. H. Velasco Melo, «El Derecho Informático Y La Gestión De La Seguridad De La Información Una Perspectiva Con Base En La Norma Iso 27001,» *Scielo,* 29 Octubre 2007.

[18] M. I. Ladino A, P. A. Villas S y A. M. López E, «Fundamentos de ISO27001 y Su aplicación en las Empresas,» *Scientia Et Technica,* Abril 2011.

[19] M. V. S. Bajarlía, J. Eterovic y J. Ierache, «Modelo de Sistema Basado en Conocimiento para el Análisis de la Seguridad de la Información en el Contexto de los Sistemas de Gestión,» de *XVI Congreso Argentino de Ciencias de la Computación*, Argentina, 2010.

[20] J. Areitio, Seguridad de la información. Redes, Informática y Sistemas de Información., Editorial Paraninfo, 2008.