UNIVERSIDAD DE CIENCIAS COMERCIALES

CAMPUS LEÓN

COORDINACIÓN DE INGENIERÍA EN SISTEMAS

TITULO: DIAGNÓSTICO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013, EN LA UNIVERSIDAD DE CIENCIAS COMERCIALES UCC, CAMPUS LEÓN. NOVIEMBRE 2022 A JUNIO 2023.

ELABORADO POR:
MSc. Martha Elizabeth Aguinaga Mora.

Asesor:

MSc. Constantino Portocarrero

04 DE JUNIO 2023

Por nuestro Prestigio, Trayectoria y Calidad
Somos la Universidad para la Gente que Triunfa

ÍNDICE DE CONTENIDO

INTRODUCCIÓN:.....1
CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN.....3
1.1 Antecedentes y Contexto del Problema.....3
1.1.1 A nivel Local.....3
1.1.2 A nivel Nacional.....4
1.1.3 A nivel Internacional.....4
1.2 Objetivos.....6
1.2.1 Objetivo General:.....6
1.2.2 Objetivos Específicos:.....6
1.3 Descripción del Problema y Pregunta de Investigación.....7
1.3.1 Formulación de la pregunta de Investigación.....9
1.4 Justificación.....10
1.5 Limitaciones.....11
1.6 Hipótesis.....12
1.6.1 Hipótesis de Investigación.....12
1.6.2 Hipótesis Nula.....12
1.7 Variables.....12
1.7.1 Variable dependiente.....12
1.7.2 Variable Independiente.....12
CAPÍTULO II: MARCO REFERENCIAL.....13
2.1 Estado del Arte.....13
2.2 Teorías y Conceptualizaciones asumidas.....16
2.2.1 La información como activo estratégico de las organizaciones.....16
2.2.2 Los activos de apoyo.....16
2.2.3 Seguridad de información.....17
2.2.4 Sistema de Gestión de Seguridad de la información.....17
2.2.5 Principios de la seguridad de la Información.....18

a. Confidencialidad 18
b. Integridad 18
c. Disponibilidad 19
2.2.6 Políticas de Seguridad de la Información 19
2.2.7 Elementos de un SGSI 20
2.3 Marco Contextual Institucional 22
CAPÍTULO III: DISEÑO METODOLÓGICO 24
3.1 Tipo de Investigación 24
3.2 Área de Estudio 24
3.2.1 Macro y Microlocalización 25
3.3 Unidades de Análisis: Población y Muestra: tamaño de la muestra y muestreo. 27
3.3.1 Unidades de análisis: 27
3.3.2 Población: 27
3.3.3 Muestra: 28
3.3.4 Muestreo: 28
3.4 Técnicas e instrumentos de Recolección de Datos. 29
3.5 Confiabilidad y Validez de los instrumentos. 29
3.6 Procesamiento de datos y análisis de la información. 29
3.6.1 Fase I- Diagnóstico del SGSI. 30
3.6.2 Fase II- Preparación. 30
3.6.3 Fase III – Planificación. 31
3.7 Operacionalización de las variables. 32
CAPITULO IV. ANÁLISIS DE RESULTADOS. 33
4. 4 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA 43
4.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CIENCIAS COMERCIALES, CAMPUS-LEÓN 94
CAPITULO V. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN. 157
CAPITULO VI. RECOMENDACIONES. 159

REFERENCIAS BIBLIOGRÁFICAS 160
ANEXOS 161

ÍNDICE DE TABLAS

Tabla 1. Base de datos consultadas..... 13
Tabla 2. Principales teorías y aportes del tema de investigación 13
Tabla 3. Operacionalización de Variables 32
Tabla 4-Escala de Cumplimiento..... 42
Tabla 5-Controles de la Norma ISO 27001 43
Tabla 6. Cronograma de Actividades 164
Tabla 7. Presupuesto 165

ÍNDICE DE FIGURAS

Figura 1**.** Microlocalización 25
Figura 2. Mapa Satelital de León..... 25
Figura 3. Mapa Satelital de Nicaragua 26

ÍNDICE DE ANEXOS

Anexo 1-Entrevistas 161
Anexo 2-Cronograma de Actividades..... 164
Anexo 3-Presupuesto..... 165

RESUMEN

Un Sistema de Gestión de Seguridad de la Información, proporciona las mejores prácticas de seguridad de Información y permite a la organización desarrollar, implementar y medir la práctica eficaz de gestión de la seguridad en todas sus áreas unificadas en sus operaciones (comúnmente el día a día de la organización), con el fin de alinearse al cumplimiento de los objetivos de la misma y para minimizar los riesgos existentes.

Palabras claves: seguridad, gestión, información, riesgos.

ABSTRACT

An Information Security Management System provides information security best practices and enables an organization to develop, implement and measure effective security management practices across all of its unified areas of its operations (commonly on a day-to-day basis). day of the organization), to align with the fulfillment of its objectives and minimize the existing risks.

Keywords: security, management, information, risks

INTRODUCCIÓN:

En la actualidad, al hablar de información, se debe considerar que esta es uno de los activos más importantes dentro de cualquier tipo de organización, para mantener sus niveles de competitividad, por lo que es necesario tener en cuenta que la gestión de la misma debe ser adecuada con el fin de preservar su integridad, confidencialidad y disponibilidad; para lo cual es pertinente contar con un entorno que garantice cumplir con estas características.

Partiendo de lo mencionado anteriormente, dentro de la Universidad de Ciencias Comerciales, campus León, es importante considerar la necesidad de crear una cultura de seguridad de la información, mediante la adopción de mecanismos de control, que permitan incorporar un nivel de seguridad adecuado a los activos de información, que son gestionados por el área de Tecnologías de la Información y Comunicación, ya que actualmente existe desconocimiento de los riesgos a los que está expuesta la información por parte del personal de la institución responsable de los equipos, debido a que no existen políticas o planes de seguridad orientados a sensibilizar el manejo seguro de la información.

A partir de esto, se ha llevado a cabo la presente investigación, la cual consiste en proponer la implementación de un Sistema de Gestión de Seguridad de la Información para la Universidad de Ciencias Comerciales, campus León, que será gestionado por el área de Tecnología de Información y Comunicación (TIC), adaptando los requerimientos de la Norma ISO/IEC 27001:2013 a las actividades y funciones realizadas en la Unidad, para ello se establecerán tres fases de desarrollo, las mismas que permitirán, mediante el análisis de la situación actual del Campus en cuanto a seguridad de la información, valoración de los activos de información (bajo las dimensiones de: confidencialidad, disponibilidad e integridad), determinación de amenazas y vulnerabilidades asociadas a los activos de información, análisis de riesgos encontrados para los activos de información y determinación de los mecanismos de control necesarios para la mitigación

de dichos riesgos a partir del Anexo A - Objetivos de Control y Controles de Seguridad de la Información ISO/IEC 27001:2013, que contiene 114 controles, distribuidos en 11 secciones; esquematizar la propuesta de un Manual de Políticas de Seguridad de la Información, destinado a la mitigación de riesgos informáticos y creación de una cultura de seguridad de la información a nivel institucional, todo ello gestionado por el área de Ciberseguridad y Tecnología de la Información y Comunicación de la Institución.

En el capítulo I del presente documento se realiza el planteamiento de la Investigación, en el que se explica el contexto actual de la Universidad, se establece los objetivos e Hipótesis de la investigación.

En el capítulo II se abordan aspectos relacionados al marco referencial, teorías y conceptos bajo los que está sustentada esta investigación.

El capítulo III explica cada uno de los procedimientos, instrumentos y formas de procesamiento de los datos obtenidos para llevar a cabo esta investigación.

El capítulo IV muestra el análisis de los resultados, en el que se explica y demuestra los resultados que se obtuvieron al aplicar los instrumentos, la interpretación de las entrevistas realizadas y el porcentaje de cumplimiento de los controles aplicados en la UCC que corresponden a la Norma ISO/IEC 27001 mediante una lista de cotejo.

El capítulo V, refleja los aspectos administrativos que se tomaron en cuenta para el desarrollo de esta investigación, tales como el presupuesto y el cronograma de actividades.

El capítulo VI, describe las conclusiones y futuras líneas de investigación que se podrían continuar desarrollando tomando como bases este estudio.

Y por último en el capítulo VII se brindan las recomendaciones para mejorar el proceso de gestión de seguridad de la información en la UCC.

CAPÍTULO I: PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Antecedentes y Contexto del Problema

Las grandes y medianas empresas están tomando conciencia de la seguridad de la información, ya que, con el pasar de los años, la importancia de las TICs, han determinado la continuidad y existencia del negocio. Por lo que todos los procesos existentes se manejan desde las TICS.
Pero también existe su contraparte ya que la empresa nacional no toma en cuenta el uso y desarrollo de las TICs, no invierten en ello, no lo mejoran porque sienten que no es parte de su negocio y solo lo toman como una necesidad obligada, por lo que la inversión es mínima y realizan lo posible para no generar más inversión.

La implementación de un SGSI en la Universidad de Ciencias Comerciales Campus León, es muy importante pues las soluciones se basan en la informática y el nivel cultural de seguridad, la cual crece muy lentamente.

Para el desarrollo de esta investigación se consultaron estudios previos relacionados a la temática:

1.1.1 A nivel Local

"Diseño del modelo de Seguridad del Sistema de Información de la UNÁN-León". Este trabajo Monográfico fue desarrollado por Lidia López y Martha Carmona en el año 2003. Con la implementación de dicho diseño del Sistema de Información propuesto se garantizó una mayor confiabilidad en la red, lográndose un mayor Tiempo Medio Operacional y un menor Tiempo Medio de Recuperación; pues la anteriormente el Sistema no lograba controlar los ataques que recibía por parte de intrusos internos o

externos, además la red informática de la Universidad, no lograba dar una máxima confiabilidad en lo que se refería a la seguridad y disponibilidad de servicios.

1.1.2 A nivel Nacional

"Procedimientos de Gestión de Incidentes de Seguridad de la Información, para la División de Informática y Sistemas de la Dirección General de Ingresos de Nicaragua". Trabajo monográfico por el Ingeniero Eddy Cardoza, para obtener el grado de Máster en Gestión de la Seguridad de la Información en el año 2020. El objetivo era establecer un manual de procedimientos para la gestión de incidentes de seguridad de la información de la División de Informática y Sistemas de la Dirección General de Ingresos. Se realizó una propuesta de roles y responsabilidades del grupo de respuesta a incidentes, se identificaron los incidentes principales y se establecieron formas de reporte y escalamiento.

"Auditoria de Seguridad basado en el Standard ISO 27001.2013 SGSI" (Sistema de Gestión de Seguridad de la Información). Proyecto desarrollo por Marcel Enrique Diaz Otero, estudiante de la Universidad Nacional de Ingeniería (UNI), en el año 2021. El objetivo principal del mismo era realizar una auditoría de seguridad de la información en la empresa AKROSERV basada en la norma internacional ISO 27001:2013 SGSI (Sistema de Gestión de Seguridad de la Información) a fin de identificar el estado actual y emitir recomendaciones necesarias para la implementación de un PGSI (Plan de Gestión de la Seguridad de la Información).

1.1.3 A nivel Internacional

"Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca". Tesis desarrollada por Roberto Carlos Fuentes Serrate en Lambayeque, Perú en el año 2020. En la misma se propone un SGSI

para dar seguridad a la información que se gestiona en los procesos críticos de la Universidad Nacional de Cajamarca (UNC), específicamente, en aquellos procesos que son la razón de ser de la entidad, como son; la gestión académica y la investigación.

“Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001”. Esta tesis la desarrolló María Gabriela Pardo Cuenca en Loja, Ecuador en el año 2015. Dicho proyecto, se llevó a cabo bajo las consideraciones la de Norma ISO/IEC 27001, para la planificación de un Sistema de Gestión de Seguridad de la Información, para lo cual, se tomó en cuenta la situación de la Unidad de Telecomunicaciones e Información, donde, a través de entrevistas al personal técnico se pudo identificar las necesidades en cuanto a seguridad para la gestión de la información, manejada en los activos informáticos bajo responsabilidad de la UTI, con ello, se consideró la metodología MAGERIT v3 para la gestión de los riegos informáticos identificados en el análisis, permitiendo con ello determinar mecanismos de control para la mitigación de riesgos, estableciendo de esta forma los primeros pasos en la creación de cultura de seguridad de la información a nivel institucional.

“Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac, 2018”. Esta tesis fue desarrollada por Jessica Noralina Huallpa Laguna en el año 2020 en la ciudad de Abancay, Perú. El objetivo principal de dicha tesis era contribuir al mejoramiento del nivel de la seguridad de la información en la Dirección de Tecnologías de Información de la Universidad Nacional Micaela Bastidas de Apurímac implementando el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013.

1.2 Objetivos

1.2.1 Objetivo General:

Diagnosticar el Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Internacional ISO/IEC 27001, para la Universidad de Ciencias Comerciales UCC, campus León.

1.2.2 Objetivos Específicos:

- Analizar la situación actual de los controles de seguridad de la información en el área TIC y área de Registro Académico.

- Determinar el nivel de cumplimiento de los controles de seguridad de la información que implementa actualmente la UCC- Campus León, en base a los objetivos de control establecidos en la Norma ISO/IEC 27001.

- Definir las políticas de seguridad de la información en cada uno de los dominios de seguridad de la ISO/IEC 27001.

1.3 Descripción del Problema y Pregunta de Investigación

La mayoría de organizaciones manejan una gran cantidad de información en todos sus procesos, y de ocurrir algún incidente relacionado con la confidencialidad, integridad o disponibilidad de ésta, puede afectar de manera muy significativa las diferentes áreas existentes, ocasionando riesgos inmediatos que afectan el desarrollo óptimo de cada una de ellas.

Riesgos como pérdida, alteración o lectura no permitida de información. Accesos no autorizados, sobrecalentamiento de servidores, presencia de software malicioso, etc. son solo algunos de los riesgos existentes, ocasionados muchas veces por la falta del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) que luego sea implementado en la organización.

“Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados”

En un Sistema de Información (SI) existen también las amenazas de carácter técnico e influyendo a la vez las de carácter humano; casos como equipos conectados a la red que son usados para uso personal y no institucional, colaboradores que no protegen la confiabilidad de sus credenciales de acceso a su área, uso de correos electrónicos personales para la comunicación institucional, uso de múltiples contraseñas para acceder a diferentes servicios ocasionando varias veces el olvido de sus datos de acceso, el no contar con un sistema automático de recuperación de contraseñas son solo algunos ejemplos de las diferentes amenazas existentes.

Por todo lo mencionado anteriormente es necesaria la implantación de políticas, procedimientos, herramientas, controles, pruebas que salvaguarden los tres principios básicos de la Seguridad de la Información: confiabilidad, integridad y disponibilidad.

“El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TIC, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados” (Solarte, Enríquez, & Benavides Ruano, 2015).

En el caso específico del sector educativo no existen leyes o normas establecidas por el Ministerio de Educación que regulen la SI en todas las instituciones de este rubro.

La Universidad de Ciencias Comerciales, campus León, no es ajena como muchas otras universidades nacionales a este gran problema, la falta de un SGSI. La Universidad, no cuenta con controles, políticas o procedimientos oficiales que ayuden a proteger de manera correcta toda la información de dicha casa de estudios. Empezando por la falta de presupuesto e inversión en la Seguridad de la Información, existe también la falta de políticas, procedimientos, normas establecidas relacionadas con la seguridad, la gestión y tratamiento de riesgos, falta de diagramas acerca de los procesos que se desarrollan, falta de un inventario de los activos tecnológicos existentes y la relación que existe con cada uno de sus procesos, falta de controles para la seguridad de equipos y así evitar pérdida, daño o robo de los mismos, falta de documentación oficial de todas las incidencias y la atención de problemas, falta de una definición formal de los deberes y funciones dentro de cada sub-área existente, falta de políticas sobre el uso de la red, falta de documentación de los sistemas utilizados en la oficina, entre otros.

Considerando la problemática anteriormente identificada, surge la necesidad de diseñar un Sistema de Gestión de la Seguridad de la Información en la UCC que se ajuste a sus necesidades actuales, utilizando la norma ISO/IEC 27001, con el objetivo de cumplir los requerimientos en materia de seguridad de la información, tales como la identificación y valoración de activos, identificación, análisis y evaluación de riesgos y amenazas, elaboración de un documento de Políticas de Seguridad, etc.

1.3.1 Formulación de la pregunta de Investigación

¿La Gestión actual de la seguridad de la información en la Universidad de Ciencias Comerciales UCC-Campus León, cumple con los controles y políticas establecidos en la Norma ISO/IEC 27001 para su implementación, en el período de Noviembre de 2022 a Junio de 2023?

1.4 Justificación

La implementación de un Sistema de Gestión de Seguridad de la Información basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial, como es la norma ISO/IEC 27001:2013, proveerá las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivos estratégicos de la Universidad, mediante la protección y aseguramiento de su información que es fundamental para garantizar la debida gestión académica, financiera y administrativa y con ello asegurar el cumplimiento de su Misión.

Un Sistema de Gestión de Seguridad de la Información, demuestra el compromiso de la Universidad hacia la Seguridad de la Información y provee los elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar en contra de la seguridad de su información, lo cual genera confianza en sus partes interesadas que es fundamental para el crecimiento y la sostenibilidad de la Institución. El Sistema de Gestión de Seguridad de la Información (SGSI), aportará grandes beneficios no solo a la Universidad, sino que también servirá de referente a otras instituciones educativas que deseen implementar un SGSI y a las instituciones en general tanto del sector público como privado.

Un Sistema de Gestión de Seguridad de la Información, le permitirá a la Universidad gestionar de manera efectiva los riesgos asociados a la seguridad de la información mediante la identificación de amenazas que puedan llegar a comprometer la integridad, disponibilidad y confidencialidad de sus activos de información y con esto poder establecer los mecanismos para minimizar el impacto en caso de presentarse la materialización de una vulnerabilidad.

1.5 Limitaciones

La presente investigación abarca a nivel de propuesta de Implementación del Sistema de Gestión de Seguridad de la Información para la Universidad de Ciencias Comerciales, campus León, basado en la norma Internacional ISO/IEC 27001:2013; pero no incluye la revisión, mantenimiento y mejora del SGSI.

Algunas limitantes presentadas para el desarrollo de la investigación es el factor tiempo, debido a que se tiene un corto período de tiempo establecido para llevar a cabo el estudio.

Otra limitante es la poca información existente en cuanto a los controles de seguridad de la información implementados en la UCC, no existe un registro oficial o personal encargado de llevar el control de las incidencias presentadas en lo que respecta a la seguridad de los activos informáticos.

1.6 Hipótesis

1.6.1 Hipótesis de Investigación.

La Gestión actual de la seguridad de la información en la Universidad de Ciencias Comerciales UCC-Campus León, cumple en un 30% con los controles y políticas establecidos en la Norma ISO/IEC 27001 para su implementación, en el período de Noviembre de 2022 a Junio de 2023.

1.6.2 Hipótesis Nula.

La Gestión actual de la seguridad de la información en la Universidad de Ciencias Comerciales UCC-Campus León, no cumple con los controles y políticas establecidos en la Norma ISO/IEC 27001 para su implementación, en el período de Noviembre de 2022 a Junio de 2023.

1.7 Variables

1.7.1 Variable dependiente.

La variable dependiente en este caso es el Sistema de Gestión de Seguridad de la Información.

1.7.2 Variable Independiente.

Las variables independientes son todos los dominios de la Norma ISO 27001:2013.

CAPÍTULO II: MARCO REFERENCIAL

2.1 Estado del Arte

Tabla 1. *Bases de datos consultadas*

Base de Datos Científicas Utilizadas	No. de publicaciones relacionadas con la investigación de acuerdo a la base de datos	No. de publicaciones con mayor reconocimiento científico	Tipos de publicaciones identificadas
Dialnet	1	1	Tesis de Grado
Google Académico	15,700	1	Artículo Científico

Fuente: Elaboración propia.

Tabla 2. *Principales teorías y aportes del tema de investigación*

Año	Tema	Contribución	Conclusión
(Montaño Orrego, 2011)	La gestión en la seguridad de la información según Cobit, Itil e Iso 27000	Relación tienen Cobit, ITIL e ISO 27000 en la seguridad informática	La experiencia demuestra que resulta algo complicado implementar un Sistema de Gestión de Seguridad de la Información SGSI sin tocar aunque sea tangencialmente este tipo de modelos en los aspectos de seguridad de la información que existe en una Organización. Por ende, usted puede estar implementando su SGSI pudiendo mejorar este sistema mediante la inclusión de áreas de aplicación ISO 27000, o midiendo el estado de maduración de su SGSI a través de Cobit o ITIL

(Ramos, Urrutia, & Bravo, 2013)	Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca	La adopción e implementación de políticas de seguridad de la información teniendo en cuenta la norma 27002:2013, las cuales servirán como guía para proporcionar herramientas que contribuyan a mejorar la gestión de la información obtenida, generada o procesada en CODELCAUCA	La política de seguridad facilita la adopción de lineamientos necesarios para garantizar la seguridad de la información teniendo las directrices establecidas en los objetivos de control 5.1.1 y 5.1.2 relacionados con políticas de seguridad y sustentados en los objetivos de la empresa
(Valencia-Duque, 2017)	Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000	implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la familia de normas de la ISO/IEC 27000, con énfasis en la interrelación de cuatro normas fundamentales a través de las cuales se desarrollan las actividades requeridas para cumplir con lo establecido en la ISO/IEC 27001	Los controles de seguridad presentados en la ISO/ IEC 27002, el esquema de riesgos de la ISO/IEC 27005 y los pasos recomendados en la ISO/IEC 27003. Se genera como resultado un proceso metodológico que da respuesta al cómo abordar un proyecto de este nivel de importancia en el contexto actual de las organizaciones y basado en estándares internacionales. Este proceso metodológico representa un aporte a los profesionales que emprenden esta labor, y que buscan un método para una implementación exitosa de un SGSI
(Ochoa Arévalos, 2015)	Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio	La Información es un asunto corporativo y es la forma como la deben percibir las Instituciones Financieras de manera que pueda encarar un entorno altamente competitivo y regulado. Este enfoque se ve desde el punto de vista de Gobierno.	Tratar las actividad regulatorias desde un enfoque de Gobierno, el cual es transversal en toda la organización no solamente un enfoque hacia los Sistemas de Información; bajo este contexto la aplicación de mejores prácticas tales como Cobit 5 e ISO 27000 nos dan los lineamientos claros para establecer el alcance de la implementación, objetivos de mejora, planificar soluciones y proyectos, definir las mediciones y una operación sostenible de los catalizadores que permitan un Gobierno y Gestión Empresarial de Seguridad de la Información
(Bertrán & Francisco, 2014)	Implementación del modelo de gestión de	La implementación de un Modelo de Gestión de la	Considerar que la seguridad de la información no se lo gestiona adquiriendo herramientas de

	la seguridad de la información aplicando ISO 27000 en la empresa Coka Tours, Ambato - Ecuador.	Seguridad de la Información contribuye a fomentar las actividades de protección y seguridad de la información en las organizaciones, mejorando su imagen y generando confianza frente a terceros	software o hardware. Cada organización debe establecer su normativa de seguridad que contiene políticas, procedimientos y roles los mismo que deben estar definidos en la organización. La implementación de la NTE INEN – ISO 2700 en la estandarización de la normativa de seguridad, es esencial para ejecución del Modelo de Seguridad de la Información y para el cumplimiento de adecuados niveles de seguridad. El objetivo principal es implementar un Modelo de Gestión de la Seguridad de la Información utilizando como base la Norma Técnica Ecuatoriana NTE INEN - ISO 27000 en la empresa COKA TOURS, satisfaciendo las necesidades de seguridad de la información y para utilizar una adecuada normativa seguridad, a través de una guía de implementación, con adecuados niveles seguridad y cumplimiento
(Rodríguez, 2016)	Diseño y creación de una política de seguridad de la información (SGSI) basado en la normativa ISO 27000 para la cooperativa construcción, comercio y producción	Se evidenció que no existe un manejo apropiado de la información lo que crea complicaciones en el cumplimiento de las actividades que se realizan dentro de todas las áreas que la componen la cooperativa estudiada	Se creo una política de seguridad de la información que ayude a cumplir con los objetivos organizacionales, administrativos y técnicos que consten en cada planificación anual. Se hizo el levantamiento de procesos, trabajo conjunto con cada líder de proceso para poder formular un ERM y de esta manera identificar de una forma específica las necesidades que tiene la empresa en función del criterio profesional de los encargados de cada área, extrayendo así un diccionario de controles que fue la base fundamental para escribir la política de seguridad.
(Sangoluisa, 2015)	Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000	Se definieron políticas de seguridad de la información a nivel de red y de usuario para el servicio de correo electrónico y de videoconferencia de la Presidencia de la República basadas en un análisis de riesgo previo. Para realizar el análisis previamente se estudió	Se definió áreas de impacto, es decir áreas inherentes a la misión de la institución que podrían verse afectadas si una de las posibles amenazas llegase a realizarse. Una vez definidas las áreas de impacto se definieron los activos críticos de información, así como los contenedores donde la información es almacenada, procesada y transmitida y poder definir los distintos escenarios de amenazas de estos. Finalmente se define las amenazas con las posibles consecuencias y seriedad que no es más que la multiplicación de las áreas de

		algunas metodologías de análisis de riesgo de la seguridad de la información como, MAGERIT, ISO 27005, FRAAP, OCTAVE-ALLEGRO	impacto y la probabilidad de ocurrencia de amenaza, una vez obtenidos estos valores de suman, de cada área de impacto, para conformar el nivel de riesgo.

Fuente: Elaboración propia.

2.2 Teorías y Conceptualizaciones asumidas

2.2.1 La información como activo estratégico de las organizaciones

Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Estos son necesarios para que la organización funcione y alcance los objetivos que propone su dirección (Espinoza, 2013).

Así entonces la información se ha convertido en un recurso clave para las empresas a todos los niveles jerárquicos y para todos los departamentos ya que las organizaciones deben conseguir, procesar, usar y comunicar información, tanto interna como externa, en sus procesos de planificación, dirección y toma de decisiones (Carrasco, 2010).

La NTP-ISO/IEC 27005 (2009) clasifica el activo en dos tipos:

Los activos primarios: Son usualmente los procesos e información centrales de la actividad en cuestión. Otros activos primarios como los procesos de la organización también pueden considerarse, lo cual será más apropiado para diseñar una política de seguridad de la información o un plan de continuidad del negocio.

-Procesos y actividades de negocio

-Información.

2.2.2 Los activos de apoyo

Estos activos tienen vulnerabilidades que son explotables por amenazas que tienen como objetivo desactivar los activos primarios del alcance (proceso e información). Son de varios tipos:

- Hardware o Software o Red
- Personal
- Sitio
- Estructura de la Organización

2.2.3 Seguridad de información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (Aguirre Freire & Palacios Cruz, 2014).

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener a acceso a cierta información, ésta se clasifica como (Talavera Álvarez, 2015):

a. Crítica: Es indispensable para la operación de la empresa.

b. Valiosa: Es un activo de la empresa y muy valioso.

c. Sensible: Debe ser conocida por las personas autorizadas.

2.2.4 Sistema de Gestión de Seguridad de la información

Un Sistema de Gestión de Seguridad de Información (SGSI) es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección

con el propósito de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la empresa (ISO 17799:2005; Alexander, 2007).

2.2.5 Principios de la seguridad de la Información

Los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se provocan daños irreparables (Montesino Perurena, Baluja Garcia, & Porven Rubier, 2013).

Estos últimos tres términos constituyen la base de la seguridad de la información, de donde se resume la explicación que se da a continuación.

a. Confidencialidad

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, como durante su procesamiento y tránsito, hasta llegar a su destino final (Condori Alejo, 2012).

b. Integridad

Este principio permite garantizar que la información no sea modificada o alterada en su contenido por personas no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos.

c. Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes. (Condori Alejo, 2012).

2.2.6 Políticas de Seguridad de la Información

Una política de seguridad de la información es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen (Hernández Pinto, 2006).

Tiene como objetivo de dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones. La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización (NTP ISO/IEC 17799, 2007).

Peltier, considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo (Peltier, Peltier, & Blackley, 2005).

Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.

Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

Según Hernández Pinto (2006) una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

- Seguridad Física
- Seguridad Lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el Outsourcing
- Planes de Contingencia

2.2.7 Elementos de un SGSI

La ISO/IEC 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio) (ISO 27000.es, 2005):

a. Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
b. Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

c. Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

d. Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

e. Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

f. Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

g. Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

h. Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

i. Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

2.3 Marco Contextual Institucional

Actualmente en Nicaragua existe una Ley, la cual se aprobó el 27 de octubre del año 2020, conocida como Ley especial de Ciberdelito o Ley 1042, la cual tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.

La Ley de Ciberdelitos define y castiga una serie de delitos cibernéticos, como el acceso no autorizado a sistemas informáticos, la interceptación ilegal de comunicaciones electrónicas, la difusión de virus informáticos, el acoso cibernético, el robo de identidad y el fraude electrónico, entre otros.

Algunas disposiciones de la Ley de Ciberdelitos de Nicaragua podrían considerarse restrictivas a la libertad de las personas, dependiendo de cómo se apliquen y se interpreten en la práctica.

Por ejemplo, la ley establece penas para delitos como el acceso no autorizado a sistemas informáticos y la difusión de virus informáticos. Si bien estas disposiciones están destinadas a proteger la seguridad informática y la privacidad de las personas, su aplicación podría ser objeto de controversia si se utilizan de manera excesiva o para restringir la libertad de expresión o de acceso a la información.

En general, es importante equilibrar la necesidad de proteger la seguridad informática y la privacidad de las personas con la protección de los derechos y libertades fundamentales, como la libertad de expresión y de acceso a la información.

Además, la Ley de Ciberdelitos de Nicaragua establece que la recolección y procesamiento de información personal solo se puede realizar en los casos y en la forma

permitidos por la ley, y se deben seguir los procedimientos legales establecidos para la investigación y enjuiciamiento de delitos informáticos.

CAPÍTULO III: DISEÑO METODOLÓGICO

En este capítulo se describe la metodología que fue utilizada para la realización de esta investigación, se detallan el tipo de estudio según su enfoque, alcance, diseño, medios de recolección de datos. Así como área de estudio, población, muestra y métodos de recolección de datos.

3.1 Tipo de Investigación

El tipo de investigación presentada es de carácter cuantitativo, de corte transversal, descriptiva, no experimental.

El enfoque cuantitativo en este estudio se aplicará debido a que para su realización será necesaria la recolección de información sobre los diferentes elementos que luego serán transformados en datos porcentuales para su posterior análisis, logrando medir el nivel de cumplimiento en la Universidad de Ciencias Comerciales UCC, Campus León, de los controles establecidos en la Norma ISO/IEC 27001:2013.

Este estudio es de corte transversal porque las variables en este caso, los dominios de la Norma ISO 27001, serán analizados durante un determinado período de tiempo. Es descriptiva porque describe cada una de las políticas de seguridad de la información que se aplican en la UCC, campus León en base a criterios establecidos en la Norma antes mencionada.

El estudio es no experimental porque se observará el estado actual en cuanto a niveles de seguridad de la información de la UCC, campus León, para después analizarlos.

3.2 Área de Estudio

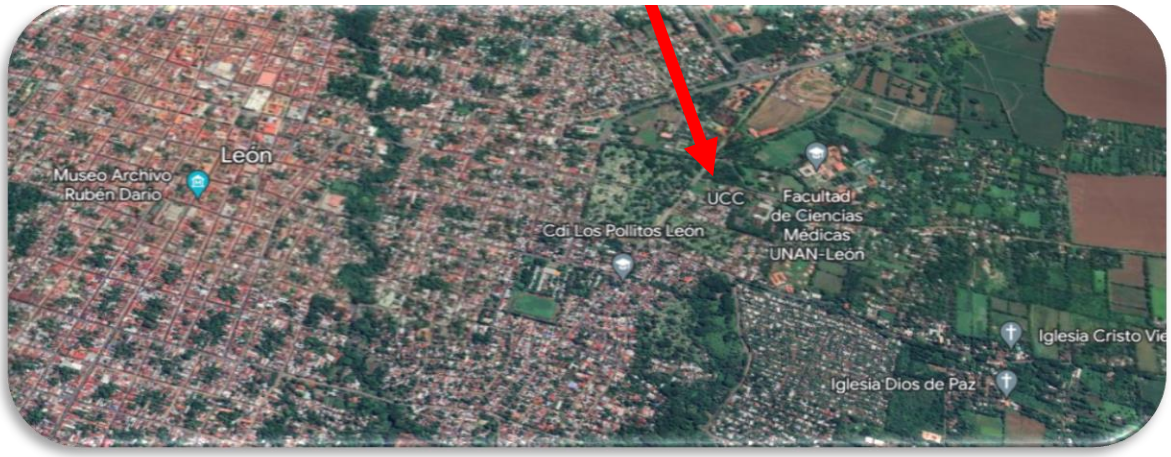
El área de estudio es la Universidad de Ciencias Comerciales, UCC, en el campus León, ubicado al costado Oeste del Campus Médico, UNÁN León.

3.2.1 Macro y Microlocalización

Figura 1. Microlocalización

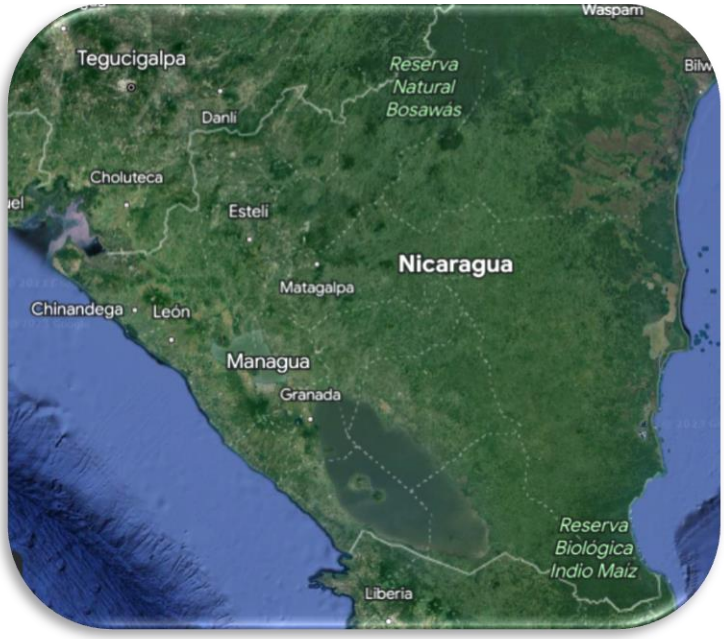
Fuente: Google Earth

Figura 2. Mapa Satelital de León



Fuente: Google Earth

Figura 3. Mapa Satelital de Nicaragua



Fuente: Google Earth

3.3 Unidades de Análisis: Población y Muestra: tamaño de la muestra y muestreo.

3.3.1 Unidades de análisis:

Son los activos informáticos del Campus León, los cuales se detallan a continuación:

- Computadoras de escritorio.
- Laptops.
- Dispositivos de Red: Router, Switch, Path Panel, Router inalámbricos.
- Página Web de la Universidad. (https://ucc.edu.ni/)
- Campus Virtual UCC. (https://campusvirtual.ucc.edu.ni/).
- Sistema Integrado de Registro Académico y Control de Ingresos (SIRACI).
- Sistema de Administración y Gestión de Educación Superior (SIAGES).
- Sistema de contabilidad (SysContab).
- Sistema de Nómina (SysNomina)

3.3.2 Población:

Son todos aquellos colaboradores que de manera directa o indirecta tengan acceso a información sensible o sistemas informáticos implementados en la Institución. La población está compuesta por 19 personas:

El responsable de la administración de toda la Red informática de la UCC, así como el encargado de Soporte Técnico, quien tiene bajo su responsabilidad el cuido de los equipos informáticos. Son 2 personas.

-Los colaboradores del Área de Registro Académico, quienes tienen bajo su responsabilidad el resguardo de la información académica de manera digital y física de los estudiantes del Campus. En esta área trabajan 2 personas.

-Los colaboradores del área de Dirección Académica, quienes tienen acceso a la información de docentes y estudiantes. Son 2 personas.

-El coordinador y asistente de la Coordinación de Arquitectura, Diseño Gráfico y Publicitario e Ingeniería de Sistemas, los cuales tienen acceso a la información académica de los estudiantes. Son 2 personas.

-Coordinación de Recursos Humanos, en la cual se manipulan datos del personal de la Universidad. Es 1 colaborador.

-El coordinador y asistente de la Coordinación de Ciencias Económicas, los cuales tienen acceso a la información académica de los estudiantes. Son 2 colaboradores.

-El coordinador y asistente de la Coordinación de Ingenierías, los cuales tienen acceso a la información académica de los estudiantes. Son 2 colaboradores.

-Los colaboradores del área de contabilidad, quienes hacen uso de los sistemas contables. Son 3 personas.

-Los colaboradores del área de caja, quienes hacen uso de los sistemas contables y tienen acceso a la información de los estudiantes. Son 3 personas.

3.3.3 Muestra:

En este caso la muestra está compuesta por 2 personas.

3.3.4 Muestreo: No probabilístico, por conveniencia debido a que el investigador decidió conforme a su criterio la cantidad de personas a entrevistar.

Se han seleccionado a 2 colaboradores para aplicarle entrevista. En este caso al Director de TIC de la Universidad de Ciencias Comerciales, pues es quien maneja la información de manera global sobre las normas o políticas asociadas a la seguridad de la información, que actualmente se implementan en la Universidad y la Coordinadora de

Registro Académico, por ser un área clave en la institución, pues en ella se manejan los datos personales y académicos de los estudiantes.

3.4 Técnicas e instrumentos de Recolección de Datos.

Dada las características del tema a investigar, la información será recolectada mediante fuentes primarias, ya que la obtención de los datos será a través del contacto directo con los sujetos en estudio y los instrumentos por el cual se registrará la información serán entrevistas y lista de cotejo.

Se realizará entrevista a 2 colaboradores por los que está compuesta la muestra para este estudio.

En la lista de cotejo se encontrará el conjunto de variables que se analizarán en este estudio, las cuales se detallan en el acápite de la operacionalización de las variables. Esta lista de cotejo contiene una escala que permite medir o cuantificar el nivel de cumplimiento de la Norma ISO 27001:2013.

3.5 Confiabilidad y Validez de los instrumentos.

Se hará una escala de Likert para medir el nivel de cumplimiento de cada uno de los controles de seguridad de la información que son aplicados en el campus León, y que están establecidos en la Norma ISO 27001:2013.

3.6 Procesamiento de datos y análisis de la información.

Teniendo en cuenta los requerimientos establecidos en la norma ISO/IEC 27001:2013 para el diseño del Sistema de Gestión de Seguridad de la Información, se establecieron las siguientes fases para el desarrollo del proyecto:

3.6.1 Fase I- Diagnóstico del SGSI.

Corresponde a las actividades para identificar el nivel de madurez inicial de la entidad con respecto al modelo de seguridad de la información que plantea la norma ISO/IEC 27001:2013.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

• Aplicación de listas de cotejo con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.

• Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

3.6.2 Fase II- Preparación.

Corresponde a las actividades que se desarrollaran para establecer el Sistema de Gestión de Seguridad de la Información, las cuales corresponde a:

• Analizar el contexto de la organización, que de acuerdo a los requerimientos establecidos en el “Capítulo 4.1 – Conocimiento de la organización y de su contexto”, de la norma ISO/IEC 27001:2013, corresponde a determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.

• Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.

• Definir la política del Sistema de Gestión de Seguridad de la Información.

• Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.

3.6.3 Fase III – Planificación.

Esta fase contempla las actividades relacionadas con:

• Identificar los activos de información del proceso de gestión de tecnología y clasificarlos de acuerdo a su criticidad y protección.

• Realizar la valoración de riesgos de seguridad de la información de acuerdo al alcance del SGSI.

• Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.

• Elaborar la declaración de aplicabilidad, que corresponde a un documento que contiene los objetivos de control y controles seleccionados del anexo A de la norma ISO/IEC 27001:2013, su nivel de cumplimiento y los motivos para su elección o exclusión.

• Elaborar el manual de política de seguridad de la información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información.

• Elaborar el procedimiento para la gestión de incidentes de seguridad, el cual se incluye en el documento del manual de política de seguridad de la información, esto corresponde a el proceso para el reporte, atención y respuesta a incidencias de seguridad.

3.7 Operacionalización de las variables.

Tabla 3. *Operacionalización de Variables*

Variable	Dimensión	Indicador	Instrumento para la evaluación	Escala
Sistema de Gestión de la Seguridad de la Información, basado en la ISO/IEC 27003	Contexto organización de la	Grado de adecuamiento del modelo de SGSI planteado a la estructura organizativa, a la normativa interna y a los procesos académicos de la UCC.	CheckList (Lista de Cotejo)	Escala Likert
		Nivel de satisfacción de las necesidades y expectativas de las partes interesadas		
		Nivel de conformidad del alcance del SGSI		
		Nivel de cumplimiento de los requisitos de la Norma ISO/IEC 27003		
	Liderazgo	Nivel de compromiso de la alta dirección	CheckList (Lista de Cotejo)	Escala Likert
		Nivel Efectividad de las políticas de TI		
		Nivel de consistencia de los roles, responsabilidades y autoridades organizacionales del SGSI propuesto.		
	Planificación	Nivel de efectividad de las acciones para tratar los riesgos de TI	CheckList (Lista de Cotejo)	Escala Likert
		Nivel de consistencia en los objetivos de seguridad y su planificación para conseguirlos.		
Gestión de riesgos de TI	Grado de satisfacción de la identificación, análisis y tratamiento de los riesgos identificados		CheckList (Lista de Cotejo)	Escala Likert

Fuente: Elaboración Propia.

CAPITULO IV. ANÁLISIS DE RESULTADOS.

4.1 Entrevistas:

Con el objetivo de analizar la situación actual de los controles de seguridad de la información se realizó entrevista al director del área de Tecnologías de Información y Comunicaciones y a la Coordinación de Registro Académico. Se obtuvieron los siguientes resultados:

4.1.1 Entrevista a director de TIC:

El Máster Ulises Rivera, considera que es de mucha importancia que en la Institución exista un conjunto de políticas para la seguridad de la información, porque esto permitirá que se minimicen los diferentes riesgos de seguridad a la cual están expuestos los sistemas de información, tales como la privacidad de la información, y su protección frente a accesos por parte de personas no autorizadas como hackers. También manifestó que los datos hoy en día son los activos más importantes de una institución.

En relación a los recursos que se tienen para el tratamiento de la información, el máster mencionó, que existe un inventario actualizado de cada uno de los activos informáticos que posee la institución, así como el registro del responsable al cual se le ha asignado cada activo.

Respecto al registro de usuarios a los sistemas informáticos y a la red, cada dirección o coordinación de la institución juega un papel fundamental en esta función, si hay que dar de alta o baja un usuario por ejemplo de cualquiera de los Sistemas Informáticos, la Dirección de RRHH o la Vicerrectoría

Administrativa Financiera, lo notifica, si es nuevo mandan los roles que debe tener dentro del Sistema y solo podrá acceder a la información que le corresponde. En cuanto al uso de las redes informáticas, algunos locales tienen acceso inalámbrico libre, sin contraseña, la mayoría está controlado tanto en ancho de banda como en el acceso con contraseñas, en algunos lugares tienen políticas de acceso.

En relación a las computadoras que se conectan vía cable, se lleva un control por parte de Soporte Informático.

Existe un doble control de acceso a los Sistemas Informáticos de la Institución, se debe tener primeramente un usuario y contraseña en el sistema, la computadora desde la que se conecta el usuario debe estar registrada en los Servidores correspondientes, si la computadora no está autentificada no podrá conectarse.

Las contraseñas no tienen periodo de caducidad, se cambia a petición del usuario. Cada usuario es dueño y se hace responsable del uso de sus credenciales, tanto de sus equipos como de los Sistemas de Información.

En cuanto a la protección del sistema de cableado estructurado, la mayor parte se hace a través de canaletas, sin embargo, muchos lugares no cumplen con esta protección y están expuestos.

En relación al mantenimiento preventivo y correctivo de los equipos informáticos, se planifica en el POA, pero por lo general, se aprovecha si un equipo es reportado con problemas, en dar su mantenimiento respectivo. Muchas veces no se cumple lo planificado por falta de personal del área de soporte informático.

El director de TIC, también manifestó que, en cuanto a los controles de detección, prevención y recuperación para la protección contra malware, la institución no cuenta con muchos recursos, pues solo se cuenta con cortafuegos físicos, Fortinet ubicados en cada sede, solo los servidores centrales cuentan con antivirus profesionales pagados, por otro lado, la concienciación a los usuarios sobre el peligro de los códigos maliciosos no se realiza de una manera formal.

En lo que respecta a copias de seguridad se realizan respaldo de las Bases de datos y de los sistemas a diario.

Por último, el director de TIC, señaló que en la institución actualmente no existe un plan de contingencia para dar respuesta a incidentes relacionados con la seguridad de la información y tampoco existen políticas de seguridad establecidas.

4.1.2 Interpretación entrevista a director de TIC:

De la entrevista realizada al Máster Ulises Rivera, director del área de Tecnologías de la Información y Comunicación, se ha logrado interpretar que:

-En la Universidad de Ciencias Comerciales, campus León, no existe una política de seguridad de la información como tal, sino que existen normas de uso de los servicios tecnológicos, pero de manera general.

- No se han realizado capacitaciones de concienciación al personal sobre el uso de buenas prácticas para proteger la información frente amenazas internas y externas.

- No se cuenta con muchos recursos (equipos tecnológicos, software) que ayuden a garantizar la seguridad de la información.

-Se debe mejorar el sistema de cableado estructurado en la institución para prevenir las interferencias en la transmisión de los datos y uso de la red informática.

- Se tiene un doble control de acceso a los sistemas que tiene que ver con la autenticación del equipo desde el cual se hace la conexión a los servidores y la autenticación de los usuarios a los sistemas informáticos con sus respectivas credenciales personales.

- Se realizan respaldos de la información ingresada en los sistemas de manera diaria.

-Se cuenta con poco personal en el área de soporte informático para dar respuesta a la demanda de servicios que deben de darse a las áreas en lo que respecta a mantenimiento de equipos informáticos y acceso a la red.

4.2 Entrevista a coordinadora de Registro Académico:

Otra de las áreas seleccionadas para realizar entrevista fue la Coordinación de Registro Académico, por ser esta una de la más importantes de la institución y donde se manejan datos sensibles pertenecientes a estudiantes, tales como datos personales, datos académicos, calificaciones, etc.

En este caso, la coordinadora de Registro Académico, la Lic. Grethel Hernández indicó que anteriormente no conocía lo que es un Sistema de Gestión de Seguridad de la información. También mencionó las políticas de seguridad de la información que se implementan actualmente en registro académico, de las cuáles tenemos.

a) Existencia de un documento que establece Normativas para los Procesos de Registro Académico.

b) A los datos registrales de los estudiantes ingresados al sistema únicamente tienen acceso el personal de UCC previamente autorizados y se brindan a personas externas autorizadas por el estudiante, los cuales brindan su nombre al momento de aplicar matrícula. Si por algún motivo no se encuentra la persona detallada en sistema como autorizada para realizar gestiones a nombre del estudiante, debe presentar carta poder o documento legal que le de potestad para actuar en nombre del alumno.

c) Uso de credenciales personales.

d) Los ID y credenciales deben encontrarse registrados en los servidores para poder acceder a los sistemas SIRACI y SIAGES.

En cuanto a la clasificación de la información en Registro Académico, la licenciada detalló dicha clasificación:

a) Los expedientes: Activos grado, activo posgrado, inactivos grados, inactivos posgrados, traslados de sucursal de egresados, egresados y titulados.

b) Ampos de notas de oferta general: Clasificados por turno, año, cuatrimestre y carrera.

c) Ampos de notas de cursos académicos: Clasificados por año y tipo de curso.

d) Ampos de Educación Continua: Contienen aperturas, notas e inscripciones en cursos y seminarios, con detalle de número de oferta.

e) Ampos de beca: Clasificado por año.

f) Ampo Cronológico de convalidaciones: Contiene actas de dictaminación de asignaturas convalidadas por cada estudiante.

g) Ampos Administrativos: Correspondencia y soportes de procesos administrativos.

En relación a los que tienen acceso a la información de Registro Académico, indicó:

a) Acceso directo:
   - Coordinación de Registro Académico, con acceso a ingresar, eliminar, modificar y aprobar en opciones académicas y administrativas.
   - Asistentes de Registro Académico, con acceso a ingresar y modificar.

b) Acceso indirecto:
   - Coordinación de Carreras: con acceso a visualizar, ingresar y eliminación (bajo supervisión).
   - Secretaría Académica: con acceso a visualizar, ingresar, modificar, eliminar y aprobar notas y ciertos procesos académicos.
   - Asistente de Posgrado y Educación continua: Visualizar, ingreso de notas y creación de ofertas.

Durante el traslado de la información fuera de los límites físicos de la institución:

a) Se utilizan medios institucionales como vehículos y personal autorizado (conductores).
b) Para el envío de la documentación enviada fuera de los límites de UCC-Campus León, el embalaje utilizado son cajas de cartón resistente.
c) Se lleva un registro físico y digital que detalla la documentación enviada entre sede y campus.

También expresó que para proteger las áreas que contienen información sensible

a) Se tiene establecido un área de atención para público interno y externo.
b) Se acondicionó un área para la emisión de carné estudiantil.
c) Existencia de dos espacios como áreas de archivo, en las cuales el acceso es restringido.

En cuanto a la identificación de los activos de información de Registro Académico señaló:

a) Información física: Se da un tratamiento de información documental o inactiva, que son soportes de las actividades pasadas ya ejecutadas, también se encuentra información activa de los que se encuentra en proceso, vigente, en ejecución o más actual. La más sensible y relevante son los ampos de notas que son soportes en original de la vida académica del estudiante.

b) Información digital: Es resguardada en carpetas que se crean por año de ejecución y tipo de información que contienen.

Respecto a la protección de la información física, dijo que esta se encuentra ordenada en muebles y archivadores, que se encuentra elaborados a base de madera y/o metal; sin embargo, existe cierto riesgo contra desastres naturales, tales como inundaciones.

A los equipos informáticos se les realiza mantenimiento correctivo y preventivo, por parte del área de soporte técnico con una frecuencia media.

Y por último indicó que respecto a los controles de acceso a los sistemas de información que se aplican en la coordinación de registro académico están:

a) Credenciales únicas que son creadas por el área TIC, proporcionadas por medios confidenciales y personales.
b) Para sistemas SIRACI Y SIAGES, se establece un mismo usuario y contraseña, en lo que respecta a correo institucional puede diferir en ocasiones.

4.2.1 Interpretación entrevista a Coordinadora de Registro Académico:

De la entrevista realizada a la Lic. Grethel Hernández, coordinadora de Registro Académico del campus León, se pudo interpretar que:

-En registro académico existe una normativa interna, sin embargo, no es específicamente para la seguridad de la información, sino que trata de la descripción de los procesos académicos del área.

-A la información que se maneja en Registro Académico, únicamente tiene acceso el personal autorizado.

-No se tiene clasificada la información por grado de criticidad, sin embargo, la información más sensible se tiene resguardada en áreas de acceso restringido.

- La información que se traslada fuera del campus es resguardada en cajas de cartón resistente y es transportada por personal autorizado únicamente.

- Se maneja información física como digital correspondiente a la vida académica de los estudiantes.

- Hay un perímetro de seguridad entre el área a la que puede acceder el público y el área a la que puede acceder solamente personal autorizado.

-A los equipos informáticos se les brinda mantenimiento preventivo y correctivo con cierta frecuencia, pero podría mejorar.

4.3 Lista de Cotejo.

Para determinar el nivel de cumplimiento de los controles de seguridad de la información que implementa actualmente la UCC-Campus León, en base a los objetivos de control establecidos en la Norma ISO/IEC 27001, se ha elaborado una lista de cotejo o de verificación. La siguiente tabla, refleja las equivalencias de los valores en el campo nivel de cumplimiento.

Tabla 4. *Escala de Cumplimiento*

Cumplimiento	Escala (0-0.5-1)
Si cumple	1
Nivel medio de cumplimiento	0.5
No cumple	0

Fuente: Elaboración propia.

El nivel o porcentaje de cumplimiento global será obtenido de la sumatoria de los valores correspondientes a cada uno de los controles dividido entre el número de ellos y posteriormente se multiplicará por 100.

4. 4 OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Tabla 5. *Controles de la Norma ISO 27001*

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN				
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
A.5.1.1	Políticas para la seguridad de información.	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	**% Cumplimiento**	**Justificación**
			0	No existe una política de seguridad de la Información, las políticas generales de la Universidad de Ciencias Comerciales, solo generaliza la seguridad.
A.5.1.2	Revisión de las políticas para la	*Control* Las políticas para la	**% Cumplimiento**	**Justificación**

	seguridad de información	seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	**0**	No existe una Política de seguridad de la Información, solo existe una política y normas generales de Tecnologías de información que no profundiza la seguridad de información.
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1. Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de a seguridad de la información dentro de la organización.				
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	**% Cumplimiento**	**Justificación**
			0	Las designaciones de roles y responsabilidades se dan de manera intuitiva, hay encargados generales.
A.6.1.2	Separación de deberes	*Control* Los deberes y las áreas de	**% Cumplimiento**	**Justificación**

		Responsabilidad en conflictos se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	**0**	Las principales funciones están segregadas en diversos roles de manera intuitiva.
A.6.1.3	Contacto con las autoridades	*Control* Se deben tener contactos apropiados con las autoridades pertinentes.	**% Cumplimiento**	**Justificación**
			0	No los tiene
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben tener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	**% Cumplimiento**	**Justificación**
			0	No los tiene
A.6.1.5	Seguridad de la información en la	*Control* La seguridad de la	**% Cumplimiento**	**Justificación**

	gestión de proyectos	información se debe tratar en la gestión de proyectos independientemente del tipo de proyecto.	**0**	Para cada proyecto se trata la seguridad de la información de manera diversa, ajustándose según las circunstancias.
A.6.2 Dispositivos móviles y teletrabajo				
Objetivos: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles				
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de los dispositivos móviles.	**% Cumplimiento**	**Justificación**
			0	No existe una política para la gestión de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se deben implementar	**% Cumplimiento**	**Justificación**

		una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares donde se realiza el teletrabajo.	**0**	No aplica porque usualmente solo los docentes trabajan de manera virtual y no acceden o manipulan información confidencial de la Universidad.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS				
A.7.1 Antes de asumir el empleo				
Objetivo: Asegurar que los empleados y contratistas comprendan sus responsabilidades y son idóneos en los roles para los que se consideran.				
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va	**% Cumplimiento**	**Justificación**
			1	Se verifica de manera detallada los antecedentes y documentos presentados por los postulantes a los diversos puestos de trabajo. Esto queda documentado y es aprobado por los jefes de las áreas respectivas.

		a tener acceso, y a los riesgos percibidos.		
A.7.1.2	Términos y Condiciones del empleo	*Control* Los acuerdos Contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	**% Cumplimiento** **0**	**Justificación** No se estipulan las condiciones respecto a la seguridad de la información en las condiciones contractuales.
A.7.2 Durante la ejecución del empleo				
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A.7.2.1	Responsabilidade	*Control* La dirección debe exigir	**% Cumplimiento**	**Justificación**

	s de la dirección	a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	**0**	Debido a que no existe una política como tal, sobre la seguridad de la información en la Institución, la Dirección no exige su cumplimiento a los contratistas y empleados.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	**% Cumplimiento**	**Justificación**
			0	Hasta el momento no se han realizado capacitaciones al personal.

A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**% Cumplimiento**	**Justificación**
			0	Existe definido un proceso disciplinario contra aquellos empleados que comenten una falta a las normas que no tienen que ver con la seguridad de la información, este se comunica.
A.7.3 Terminación y cambio de empleo				
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A.7.3.1	Terminación o Cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**% Cumplimiento**	**Justificación**
			0	Aún, no existe definido un proceso disciplinario contra aquellos empleados que comenten una falta contra la seguridad de la información.
A.8 GESTIÓN DE ACTIVOS				
A.8.1 Responsabilidad por los activos				
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas				

A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con la información e instalaciones de procesamiento e información, y se debe elaborar y mantener un inventario de estos activos.	**% Cumplimiento**	**Justificación**
			0.5	Se tiene un inventario de activos de información, pero está actualizado.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.	**% Cumplimiento**	**Justificación**
			0	Cada activo está asociado con el dueño de este, sin embargo, solo se documentan en algunos casos la asociación activo-responsable.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de activos asociados con información e instalaciones de procesamiento de información.	**% Cumplimiento** **0**	**Justificación** No se ha reglas para el uso aceptable de la información.

A.8.1.4	Devolución de activos	*Control* Todos los empleados y terceras partes deben devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.	**% Cumplimiento** **1**	**Justificación** Los empleados al finalizar su empleo devuelven los activos que les fueron asignados para sus funciones laborales.
A.8.2	**Clasificación de la información**			
Objetivo: Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de la importancia de su revelación o modificación no autorizadas.	**% Cumplimiento** **0.5**	**Justificación** La información es clasificada de forma diferente en cada área. Algunas áreas la clasifican según si importancia, otras áreas emplean otros criterios.
A.8.2.2	Etiquetado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.	**% Cumplimiento** **0.5**	**Justificación** No todas las áreas tienen etiquetada la información

A.8.2.3	Manipulado de la información	*Control* Debe desarrollarse e implantarse un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	**% Cumplimiento** **0**	**Justificación** No existe un conjunto adecuado de procedimientos para la manipulación de la información.
A.8.3 Manipulación de los soportes				
A.8.3.1	Gestión de soportes extraíbles	procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	**% Cumplimiento** **0**	**Justificación** No existe algún procedimiento definido para el manejo de los medios removibles en la organización
A.8.3.2	Disposición de los medios	*Control* Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	**% Cumplimiento** **0**	**Justificación** No existe un procedimiento para la disposición final de los medios de manera segura, se realiza de manera repetible
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que	**% Cumplimiento**	**Justificación**

		contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	**1**	La información que es trasladada fuera de los límites de la institución es bien resguardada.
A.9 CONTROL DE ACCESO				
A.9.1 Requisitos del negocio para controlar el acceso				
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A.9.1.1	Política de control de acceso	*Control* Se debe establecer,	**% Cumplimiento**	**Justificación**
		documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**1**	Existe una política de control de acceso ya definida, documentada, aprobada y comunicada
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de la red para los que hayan sido autorizados específicamente.	**% Cumplimiento**	**Justificación**
			1	Existe un procedimiento definido de acceso a la red y servicios en base a una clasificación de usuarios.
A.9.2 Gestión de acceso de usuarios				

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	**% Cumplimiento**	**Justificación**
			1	Existe un procedimiento manual documentado a través de correo electrónico, se realiza en base se soliciten.
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un	**% Cumplimiento**	**Justificación**
		proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	**1**	El cambio de permisos del acceso del usuario se realiza manual y con confirmación vía correo electrónico.
A.9.2.3	Gestión de derecho de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**% Cumplimiento**	**Justificación**
			1	Los accesos privilegiados están controlados detalladamente y son siempre aprobados y comunicados para su área respectiva
A.9.2.4	Gestión de Información de	*Control* La asignación de	**% Cumplimiento**	**Justificación**

	autenticación secreta de usuarios	Información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	**1**	Se controla la autentificación secreta a través de un proceso formal de gestión de autentificación de usuarios.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	**% Cumplimiento**	**Justificación**
			0	Se realiza una revisión solo en casos que se genere un incidente o se solicite explícitamente esto.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de Procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	**% Cumplimiento**	**Justificación**
			1	Los ajustes, cambios y remoción de derechos de acceso son documentados y pedidos mediante un procedimiento formal a los responsables de cada área.
A.9.3 Responsabilidades de los usuarios				
Objetivo: Hacer que los usuarios rindan cuentas por las salvaguardas de su información de autenticación.				

A.9.3.1	Uso de Información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	**% Cumplimiento** **1**	**Justificación** Se le informa y exige al usuario a que siga las buenas prácticas de la organización. No existe un proceso de concientización hacia los usuarios.
A.9.4 Control de acceso a sistemas y aplicaciones				
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A.9.4.1	Restricciones de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	**% Cumplimiento** **1**	**Justificación** Se restringe el acceso a las funciones del sistema y a los aplicativos en base a los requerimientos de diversas áreas
A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar	**% Cumplimiento** **1**	**Justificación**

		mediante un proceso de ingreso seguro.		Se controla de manera segura el acceso a los diversos sistemas y aplicaciones.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	**% Cumplimiento**	**Justificación**
			0	No existe un sistema de gestión de contraseñas ni de apoyo a los usuarios para que generen contraseñas seguras. Las contraseñas son asignadas por el administrador de los sistemas.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	**% Cumplimiento**	**Justificación**
			0	No se tiene control
A.9.4.5	Control de acceso a códigos fuentes de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas	**% Cumplimiento**	**Justificación**
			1	Se restringe el acceso al código fuente de las aplicaciones desarrollados solamente a los usuarios que tienen permiso

				explícito
A.10 CRIPTOGRAFÍA				
A.10.1 Controles criptográficos				
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y la integridad de la información.				
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	**% Cumplimiento**	**Justificación**
			0	No existe una política para el uso de controles criptográficos.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	**% Cumplimiento**	**Justificación**
			0	No existe una política para el uso de claves criptográficas.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO				
A.11.1 Áreas seguras				
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				

A.11.1.1	Perímetro de seguridad física	*Control* Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**% Cumplimiento**	**Justificación**
			1	Se protege con acceso con llave, vigilancia con personal de seguridad y cámaras de video
A.11.1.2	Controles de acceso físico	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	**% Cumplimiento**	**Justificación**
			1	Se cuenta con controles y procedimientos definidos para el acceso a áreas seguras.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**% Cumplimiento**	**Justificación**
			0.5	Los controles de seguridad son ligeros, puertas con llave y vigilancia por cámaras de seguridad; pero falta más seguridad en el área de soporte técnico del campus León.
A.11.1.4	Protección	*Control* Se debe diseñar y	**% Cumplimiento**	**Justificación**

	contra amenazas externas y ambientales	aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**0**	No se han definido y documentado controles para la protección contra amenazas físicas y ambientales
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	**% Cumplimiento**	**Justificación**
			0	No existen procedimientos documentados para el acceso a las áreas seguras.
A.11.1.6	Áreas de despacho y carga	*Control* Se debe controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**% Cumplimiento**	**Justificación**
			1	Las áreas de despacho y carga están alejadas de las instalaciones de procesamiento de información, además se realizan de manera minuciosa en base a las prácticas que se mantienen.
A.11.2 Equipos				
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar	**% Cumplimiento**	**Justificación**

		ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	**1**	Los equipos están ubicados correctamente en base las buenas prácticas que se siguen en cada área respectiva.
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	**% Cumplimiento**	**Justificación**
			0	No se cuenta con protección para todos los equipos en caso que suceda una falla o corte del servicio de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	**% Cumplimiento**	**Justificación**
			0.5	El cableado no se encuentra debidamente protegido contra el daño, interceptación e interferencia, puesto que en su mayoría están a la intemperie y no dentro de canaletas.
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben	**% Cumplimiento**	**Justificación**

		mantener correctamente para asegurar su disponibilidad e integridad continuas.	**0.5**	Se conserva un programa para la revisión periódica de los equipos en base a un procedimiento ya definido; sin embargo muchas veces no se cumple.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin actualización previa.	**% Cumplimiento**	**Justificación**
			1	El retiro de los equipos se realiza con autorización previa del área respectiva.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	**% Cumplimiento**	**Justificación**
			1	Se mantiene un esquema de protección para los activos fuera de las instalaciones, pero se hace de manera independiente para cada caso según se requiera
A.11.2.7	Disposición segura o reutilización de	*Control* Se deben verificar todos	**% Cumplimiento**	**Justificación**

	equipos	los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición de reuso.	**0.5**	Se realizan tareas determinadas para la disposición y reutilización de los equipos, sin embargo, estas no están documentadas y se realizan siguiendo la intuición
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que los equipos desatendidos se les dan protección apropiada.	**% Cumplimiento**	**Justificación**
			0.5	Algunas veces se verifica que los equipos desatendidos se conserven bajo una protección adecuada; pero no hay procedimientos definidos.
A.11.2.9	Políticas de escritorio limpio y	*Control* Se debe adoptar una	**% Cumplimiento**	**Justificación**

	pantalla limpia	política de escritorio limpio para los papeles y medios de almacenamientos removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	**0.5**	Se mantiene un comportamiento intuitivo de escritorio limpio y pantalla limpia para los usuarios, pero esta no se documenta.
A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1 Procedimientos operacionales y responsabilidades				
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que se necesitan.	**% Cumplimiento**	**Justificación**
			0	Solo están documentados algunos procedimientos, los que se consideran en base a cada encargado del área
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los	**% Cumplimiento**	**Justificación**

		cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	**0**	No se controlan los cambios.
A.12.1.3	Gestión de capacidad	Control Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	**% Cumplimiento**	**Justificación**
			0	No se gestiona
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Control Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**% Cumplimiento**	**Justificación**
			1	Los entornos están separados física y lógicamente pero no tienen control.
A.12.2 Protección contra códigos maliciosos				

<table>
<tr><td colspan="5">Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos</td></tr>
<tr><td rowspan="2">A.12.2.1</td><td rowspan="2">Controles contra códigos maliciosos</td><td rowspan="2">Control
Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos</td><td>% Cumplimiento</td><td>Justificación</td></tr>
<tr><td>0.5</td><td>Se tiene una protección contra el código malicioso básica, pero no se ha realizado una concientización a los usuarios sobre este.</td></tr>
<tr><td colspan="5">A.12.3 Copias de respaldo</td></tr>
<tr><td colspan="5">Objetivo: Evitar la pérdida de datos</td></tr>
<tr><td rowspan="2">A.12.3.1</td><td rowspan="2">Respaldo de la información</td><td rowspan="2">Control
Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de</td><td>% Cumplimiento</td><td>Justificación</td></tr>
<tr><td>1</td><td>Se realizan respaldos diario de la información de los sistemas.</td></tr>
</table>

		acuerdo con una política de copias de respaldo acordadas		
A.12.4 Registro y seguimiento				
Objetivo: Registrar eventos y generar evidencia				
A.12.4.1	Registro de eventos	Control Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	**% Cumplimiento**	**Justificación**
			0	No se registran los eventos de los usuarios en navegación, los eventos de seguridad no están monitoreados.
A.12.4.2	Protección de la información de registro	Control Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	**% Cumplimiento**	**Justificación**
			1	El acceso a los registros de eventos está protegido por las políticas a nivel técnico de la organización.
A.12.4.3	Registros del administrador y del operador	Control Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad	**% Cumplimiento**	**Justificación**
			0	Los eventos del administrador no son monitoreados ni respaldados.

A.12.4.4	Sincronización de relojes	Control Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo	**% Cumplimiento** **1**	**Justificación** Los relojes están sincronizados en base a una fuente de referencia única.
A.12.5 Control de software operacional				
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A.12.5.1	Instalación de software en sistemas operativos	Control Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos	**% Cumplimiento** **1**	**Justificación** Se han implementado procedimientos para evitar la instalación de software sin autorización de los administradores.
A.12.6 Gestión de la vulnerabilidad técnica				
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control Se deben obtener oportunamente información	**% Cumplimiento**	**Justificación**
				No existe ningún procedimiento ni

		acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	**0**	iniciativa para el manejo de las vulnerabilidades técnicas de los sistemas de información.
A.12.6.2	Restricciones sobre la instalación de software	Control Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios	**% Cumplimiento**	**Justificación**
			1	Existen reglas que impiden que un usuario estándar pueda instalar software. El enfoque es un proceso estándar documentado y comunicado, apoyado por controles técnicos.
A.12.7 Consideraciones sobre auditorias de sistemas de información				
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos				
A.12.7.1	Controles de	Control Los requisitos y	**% Cumplimiento**	**Justificación**

	auditorías de sistemas de informaci ón	actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio	**1**	Se planifican y acuerdan las actividades de auditoría de un enfoque intuitivo en base a las experiencias los administradores de cada servidor
A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 Gestión de la seguridad de las redes				
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte				
A.13.1.1	Controles de redes	Control Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	**% Cumplimiento**	**Justificación**
			0.5	Existen gestión y controles para la protección de la información, pero se necesita mejora la seguridad de la red.
A.13.1.2	Seguridad de los servicios de red	Control Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes, ya sea que los servicios se presten internamente o se contraten	**% Cumplimiento**	**Justificación**
			0	No existen acuerdos de servicio para los servicios de red.

		externamente		
A.13.1.3	Separación en las redes	Control Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes	**% Cumplimiento**	**Justificación**
			0.5	Las redes están segregadas en base a las buenas prácticas de la organización. No existe documentación detallada sobre la segregación de la red.
A.13.2 Transferencia de información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa				
A.13.2.1	Políticas y procedimientos de transferencia de información	Control Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones	**% Cumplimiento**	**Justificación**
			0.5	Existen controles técnicos para controlar la transferencia de información dentro de la organización; pero no existen procedimientos definidos ni detallados para esto.

A.13.2.2	Acuerdos sobre transferencia de información	Control Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas	**% Cumplimiento**	**Justificación**
			0	No existen acuerdos de transferencia de información.
A.13.2.3	Mensajería electrónica	Control Se debe proteger adecuadamente la información incluida en la mensajería electrónica	**% Cumplimiento**	**Justificación**
			0	No existen políticas y controles técnicos para el control de la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información	**% Cumplimiento**	**Justificación**
			0	No existen acuerdos de confidencialidad
A.14 Adquisición, desarrollo y mantenimiento de sistemas				
A.14.1 Requisitos de seguridad de los sistemas de información				

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes	**% Cumplimiento**	**Justificación**
			1	Los requisitos de seguridad de la información son tomados en cuenta bajo enfoques de acuerdo al escenario en desarrollo o mejora de los sistemas de información
A.14.1.2	Seguridad de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	**% Cumplimiento**	**Justificación**
			0	No se han establecido controles sobre eso.

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	**% Cumplimiento**	**Justificación**
			0	Existen controles técnicos para las transacciones de los servicios de aplicación. Estos se dan de manera intuitiva.
A.14.2 Seguridad en los procesos de desarrollo y de soporte				
Objetivo: Asegurar que la seguridad de la información esté diseñada o implementada dentro del ciclo de vida de desarrollo de los sistemas de información				
A.14.2.1	Política de desarrollo seguro	Control Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización	**% Cumplimiento**	**Justificación**
			0	No existe una política de desarrollo seguro de las aplicaciones.

A.14.2.2	Procedimientos de control de cambios en sistemas	Control Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios	**% Cumplimiento**	**Justificación**
			1	Se manejan procedimientos formales de control de cambios de los sistemas. Pero no están documentados.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización	**% Cumplimiento**	**Justificación**
			0.5	Existen revisiones técnicas de las aplicaciones después de cambios de plataforma, pero son procedimientos informales y repetitivos en muchos de los casos.
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente	**% Cumplimiento**	**Justificación**
			0.5	Hay procedimientos determinados e informales sobre los cambios a los paquetes de software de la organización.

A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información	**% Cumplimiento**	**Justificación**
			0.5	Los principios de ingeniería de sistemas seguros se aplican bajo un enfoque en base al momento y escenario, no existen procedimientos formales.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas	**% Cumplimiento**	**Justificación**
			0.5	Se mantiene y conserva un ambiente de desarrollo seguro en base a algunos controles técnicos y procedimientos informales.
A.14.2.7	Desarrollo contratado	*Control* La organización debe	**% Cumplimiento**	**Justificación**

	externamente	supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente	**1**	Se da seguimiento y supervisión al desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad	**% Cumplimiento**	**Justificación**
			1	Se realizan pruebas bajo enfoques intuitivos para el desarrollo de aplicaciones.
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados	**% Cumplimiento**	**Justificación**
			0.5	Se realizan pruebas de aceptación de los sistemas bajo enfoques informales sin documentación detallada
A.14.3 Datos de prueba				
Objetivo: Asegurar la protección de los datos usados para pruebas				
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se	**% Cumplimiento**	**Justificación**

		deben seleccionar, proteger y controlar cuidadosamente	**1**	Los datos de prueba son seleccionados aleatoriamente, en algunos casos aislados si se tienen en cuenta algunos criterios.
A.15 RELACIONES CON LOS PROVEEDORES				
A.15.1 Seguridad de la información en las relaciones con los proveedores				
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar	**% Cumplimiento**	**Justificación**
			0.5	No existen procedimientos ni documentos definidos para la seguridad de la información en las relaciones con los proveedores. En algunos casos solo se menciona que no se debe revelar la información.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda	**% Cumplimiento**	**Justificación**

		tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización	**0.5**	Solo para algunos acuerdos con proveedores se tienen en cuenta la seguridad de la información
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación	**% Cumplimiento**	**Justificación**
			0	No se aplica
A.15.2 Gestión de la prestación de servicios de proveedores				
Objetivo: mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A.15.2.1	Seguimiento y revisión de los	*Control* Las organizaciones	**% Cumplimiento**	**Justificación**

	servicios de los proveedores	deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores	**0**	No se revisa ni audita regularmente los servicios con los proveedores, solamente en caso se pida explícitamente la realización de estas tareas.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos	**% Cumplimiento**	**Justificación**
			0	No existe un enfoque de gestión de cambios a los servicios de proveedores.
A.16 Gestión de incidentes de seguridad de la información				
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información				
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades				
A.16.1.1	Responsabilidades y	*Control* Se deben establecer	**% Cumplimiento**	**Justificación**

	procedimientos	las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	**0.5**	Se han establecido responsabilidades para la gestión de incidentes bajo un enfoque repetitivo y no formal.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible	**% Cumplimiento**	**Justificación**
			0	No existe un reporte formal y periódico de los eventos de seguridad de la información, solamente se realiza este cuando es requerido explícitamente.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los	**% Cumplimiento**	**Justificación**
			0.5	Se mantiene un enfoque informal para reportar la debilidad en seguridad de la información.

		sistemas o servicios		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	*Control* Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información	**% Cumplimiento**	**Justificación**
			0	No se realiza una evaluación para los incidentes de seguridad de la información y no se toma en cuenta ninguna clasificación.
			% Cumplimiento	**Justificación**
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	**0.5**	Se responden los incidentes de seguridad bajo un enfoque informal sin un procedimiento determinado.

A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros	**% Cumplimiento**	**Justificación**
			0.5	Se utiliza el conocimiento adquirido, pero sin manejar algún documento formal.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	**% Cumplimiento**	**Justificación**
			0	No existen enfoques para la recolección de evidencia sobre los incidentes de seguridad de la información
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO				
A.17.1 Continuidad de seguridad de la información				
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización				
			% Cumplimiento	**Justificación**

A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre	**0**	No tiene planes ni sistemas de restauración de servicios de información. Solo gestión de backups internos.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	**% Cumplimiento**	**Justificación**
			0	No posee procesos, procedimientos ni controles de seguridad de la información.
A.17.1.3	Implementación de la continuidad	*Control* La organización debe	**% Cumplimiento**	**Justificación**

	de la seguridad de la información	verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas	**0**	No posee procesos, procedimientos ni controles de seguridad de la información.
A.17.2 Redundancias				
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	**% Cumplimiento**	**Justificación**
			0	No posee sistemas de redundancia
A.18 CUMPLIMIENTO				
A.18.1 Cumplimiento de requisitos legales y contractuales				
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad				
A.18.1.1	Identificación de la legislación	*Control* Todos los requisitos	**% Cumplimiento**	**Justificación**

	aplicable y de los requisitos contractuales	estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización	**1**	Se han identificado, documentado y mantenido todos los requisitos contractuales y de legislación aplicables para la organización y cada sistema de información.
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos	**% Cumplimiento**	**Justificación**
			1	Se han establecido los procedimientos para asegurar los derechos de propiedad intelectual en la organización.

		de software patentados		
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio	**% Cumplimiento**	**Justificación**
			1	Se han implementado controles para la protección de registros importantes en la organización.
A.18.1.3	Protección de registros	*Control* Se deben asegurar la	**% Cumplimiento**	**Justificación**

		privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable	**1**	Se han implementado controles para la protección de registros importantes en la organización.
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable	**% Cumplimiento**	**Justificación**
			1	Se han implementado controles de acuerdo a la legislación vigente para asegurar la privacidad y la protección de datos personales.
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	**% Cumplimiento**	**Justificación**
			0	No se aplican
A.18.2 Revisiones de seguridad de la información				

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales				
A.18.2.1	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos	**% Cumplimiento**	**Justificación**
			0.5	Solo se revisan algunas políticas generales cuando se realizan cambios significativos
A.18.2.2	Cumplimiento con las políticas y	Control Los directores deben	**% Cumplimiento**	**Justificación**

	normas de seguridad	revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad	**0.5**	Solo se revisa el cumplimiento de las políticas y normas de seguridad cuando se van a realizar cambios o durante las auditorías. No existe un enfoque periódico ni un procedimiento definido.
A.18.2.3	Revisión del cumplimiento técnico	Control Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	**% Cumplimiento**	**Justificación**
			0.5	Solo se revisa el cumplimiento de las políticas y normas de seguridad cuando se van a realizar cambios o durante las auditorías. No existe un enfoque periódico ni un procedimiento definido

Fuente: Norma ISO 27001.

Para determinar el porcentaje de cumplimiento de los controles se utilizará la siguiente fórmula:

PC=(SC/NC) *100

Donde:

PC= Porcentaje de Cumplimiento

SC= Sumatoria de los controles.

NC= Número de controles

PC= (50.5/114) *100

PC=44.3%

El porcentaje de cumplimiento de los controles que se aplican en la Universidad de Ciencias Comerciales, campus León, basado en Norma ISO/IEC 27001, es del 44.3%.

4.5 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CIENCIAS COMERCIALES, CAMPUS-LEÓN

1. PRESENTACIÓN

Un aspecto fundamental en el proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) es la definición de una Política de Seguridad de la Información que establezca los objetivos e identifique responsabilidades de la adecuada protección de los activos de información de la Universidad de Ciencias Comerciales, Campus León. La presente política se sustenta en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y se orienta al desarrollo de mejores prácticas de gestión de los activos de información.

La Institución, reconoce que la información generada en sus procesos, es un activo de alto valor e importancia para el eficaz desempeño organizacional y por tanto requiere de una adecuada protección.

Una Política de Seguridad de la Información es un grupo de principios y lineamientos generales, que regula el manejo de los activos de información de una organización y establece los objetivos y responsabilidades para la adecuada protección de los mismos, en este sentido, se debe asumir el compromiso de establecer, implementar, mantener y mejorar continuamente un SGSI, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información, de conformidad con la normatividad vigente.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

2.1 Objetivo General

La Política de Seguridad de la Información de la Universidad de Ciencias Comerciales, campus León, tiene como objetivo establecer el marco general para gestionar de manera adecuada la seguridad de la información en la Institución.

2.2 Objetivos Específicos

a) Garantizar niveles adecuados de confidencialidad, integridad y disponibilidad para la información que se maneja en la Universidad de Ciencias Comerciales, campus León.

b) Controlar, prevenir y mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas, para garantizar la continuidad de los procesos de información y servicios de la Institución.

c) Sensibilizar y capacitar al personal indistintamente de su régimen laboral o modalidad de contratación al que se encuentre sujeto, en relación a la seguridad de la información y su adecuado uso.

4. BASE LEGAL

a) Ley N° 29733, Ley de protección de datos personales.

5. PRINCIPIOS

Los siguientes principios constituyen los fundamentos sobre los que se basa cualquier acción acerca de seguridad de la información en la Universidad de Ciencias Comerciales, campus León.

5.1 Confidencialidad

Sólo quienes estén autorizados puedan tener acceso a la información que se produzca, procese, transmita y almacene, con lo cual se resguarda la información del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

5.2 Integridad

La información no debe de ser alterada por cambios no autorizados o accidentales, garantizando la precisión y validez de información en todas las transacciones de acuerdo con los valores y expectativas de la Institución, así como evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

5.3 Disponibilidad

Asegurar que usuarios autorizados puedan acceder a la información y a sus activos asociados cuando lo requieran, garantizando el acceso oportuno a la información y a los recursos relacionados con la misma, para ello se debe asegurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.

5.4 Propiedad

Toda la información producida, procesada y almacenada, es de propiedad de la Universidad de Ciencias Comerciales, campus León, salvo que, en una relación contractual de la institución, se establezca lo contrario.

5.5 Auditabilidad

Asegurar que los sistemas informáticos, de acuerdo a su criticidad, registren y documenten todo evento relacionado con la seguridad de la información, e identifiquen a sus usuarios, a fin de generar las evidencias para su control posterior.

5.6 Autenticación

Todos los usuarios de los sistemas de información, deben ser identificados individualmente y sus permisos de acceso deben concederse en forma específica de acuerdo a su rol y responsabilidades y cumplir los requisitos de autenticación.

6. LINEAMIENTOS

Los siguientes lineamientos constituyen las medidas de seguridad a implementar acerca de seguridad de la información de la Universidad de Ciencias Comerciales, Campus León.

6.1 Sobre el control de accesos a los sistemas de información.

a) Se deberá establecer las medidas de seguridad informáticas necesarias para asegurar que todo acceso a los sistemas de información, servicios de red y plataformas de tecnología informática, sean solo para los usuarios autorizados.

b) Se deberá establecer procedimientos para asignar los permisos de acceso a los sistemas informáticos, plataformas virtuales y conexiones de red que se encuentren bajo su administración.

c) Los administradores de los recursos informáticos son los encargados de autorizar los perfiles y privilegios para los usuarios que necesiten acceder a la información que estos contengan, los mismos que serán controlados y evaluados.

d) Los accesos a los recursos informáticos deben tener un medio de autenticación.

e) Los accesos a los recursos informáticos deben tener un medio de autenticación como clave secreta de acceso y otros, que permitan el acceso solo al usuario autorizado.

6.2 Sobre el uso del servicio de internet.

El acceso de los usuarios al servicio de internet, debe ser otorgado solo para llevar a cabo actividades directamente relacionadas con las responsabilidades laborales, pudiendo ser monitoreada toda la navegación web y restringido el acceso a ciertas páginas web.

a.3 Sobre el uso del correo electrónico.

a) Se deberá establecer los controles necesarios para proteger la información de los correos electrónicos de posibles ataques de virus, intercepción de correos, phishing, entre otros.

b) La cuenta de correo electrónico será asignada a un usuario y deberá ser utilizada solo para fines laborales.

c) El usuario asignado a la cuenta de correo electrónico será el responsable de toda la información enviada y almacenada en dicha cuenta.

a.4 Sobre la seguridad física

a) Todas las áreas donde se produzca, procesen, transmita y almacene información, deben contar con medidas de seguridad física apropiadas, para prevenir su daño o pérdida.

b) Todo el personal, indistintamente de su régimen laboral o modalidad de contratación de la institución, deberán portar de forma permanente, mientras se encuentre en las instalaciones de la Institución, su carnet que lo identifique.

c) Todo visitante que ingrese a las instalaciones de la Institución, se le deberá asignar un pase de visita, el cual deberá de portar en todo momento hasta su salida de la Universidad.

d) Se deberá establecer las medidas necesarias para mantener en condiciones óptimas la limpieza, seguridad, mantenimiento y funcionalidad de los equipos de procesamiento de la información, a fin de asegurar su continua disponibilidad e integridad.

a.5 Sobre la seguridad en los recursos humanos

a) Se deberá establecer las medidas de seguridad adecuadas para comprobar y asegurar la idoneidad, ética y conducta profesional en la selección del personal para cualquier modalidad de contratación.

b) Se deberá establecer acuerdos de confidencialidad de seguridad de la información para cualquier modalidad de contratación de personal que brinde servicios a la Universidad.

c) Se deberá tener un plan de inducción o capacitación sobre aspectos de la política, las directivas y los procedimientos de seguridad de la información.

6.6 Sobre la continuidad operativa

Se deberá establecer un plan de contingencia informático para actuar de manera efectiva ante algún posible evento que pudiera afectar la continuidad informática y disponibilidad de la información.

a.7 **Sobre la gestión de incidentes.**

a) Se deberá de disponer de canales de comunicación adecuados que permita que el personal indistintamente de su régimen laboral, modalidad de contratación o nivel jerárquico, reporte, ocurrencias de seguridad, incidente sospechoso y el inadecuado uso de los recursos informáticos.

b) Los responsables de la seguridad de la información de la Institución, deberán reportar periódicamente toda ocurrencia de seguridad de la información al Área de Tecnologías de Información y Comunicaciones de la Institución.

7. RESPONSABILIDADES

Para el cumplimiento de la presente Política de Seguridad de la Información, se establece las siguientes responsabilidades:

a) Gerencia de la Universidad: Aprobar la Política de Seguridad de la Información y sus actualizaciones.

b) Comité de Gestión de Seguridad de la información: Aprobar, dirigir y gestionar la puesta en práctica de la seguridad de la información, comprometiendo el apoyo de Gerencia y el de Dirección.

c) Coordinador de Seguridad de la Información: Supervisar y ejecutar el cumplimiento de la presente Política y liderar el establecimiento, implementación y mantenimiento del SGSI.

d) Direcciones y coordinaciones: Aplicar las políticas de seguridad de la información al interior de cada órgano, unidad orgánica o área a su cargo, en el ámbito funcional, técnico y administrativo, según corresponda.

e) Personal y usuarios en general: Tomar conocimiento y cumplir con la presente política y el marco normativo que lo sustenta, e informar de eventos o incidentes de seguridad de la información al jefe inmediato superior o encargado.

8. DIFUSIÓN

La comunicación de los documentos que componen la seguridad de la información se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todo el personal comprendido en esta Política.

9. REVISIONES

La Política de Seguridad de la Información es revisada, y de ser necesario actualizada anualmente por el Comité de Gestión de Seguridad de la Información de la Institución y es aprobada con Gerencia.

10.SANCIONES

El no cumplimiento del contenido en la presente Política, Directivas, Procedimientos, u otros documentos que se deriven de estas; incurrirán en falta disciplinaria que se sancionará de acuerdo al reglamento interno de la Universidad.

A5. DIRECTIVA DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE CIENCIAS COMERCIALES, CAMPUS LEÓN.

I. OBJETIVO

Establecer los lineamientos de la Seguridad de la Información necesarios para asegurar y mantener la confidencialidad, integridad y disponibilidad de la información de la Universidad de Ciencias Comerciales, campus León.

II. FINALIDAD

Brindar el marco normativo de cumplimiento de los controles de Seguridad de la Información alineados ISO/IEC 27001.

III. ALCANCE

Los lineamientos comprendidos en la presente directiva son de obligatoriedad de cumplimiento para todo el personal que labore en la Institución incluido los servicios externos.

IV. BASE LEGAL

a) Ley N° 29733, Ley de protección de datos personales.

V. DISPOSICIONES GENERALES

a) La Coordinación de Ciberseguridad es responsable de la implementación del SGSI, en la Institución y por ende del cumplimiento de los presentes lineamientos de Seguridad de la Información.

b) Los lineamientos de la presente directiva se basan en el ISO/IEC 27001.

VI. DISPOSICIONES ESPECIFICAS

6.1. Lineamientos para las directivas y/o políticas de seguridad de la información.
6.1.1. Directivas y/o Políticas de seguridad de la Información.
Las directivas y/o políticas que estén afectas al ISO/IEC 27001, deben establecer los lineamientos y requerimientos necesarios para implementar un razonable nivel de protección de los activos de información Política de Seguridad de la Información y Manual de Políticas del SGSI.

• Las políticas de Seguridad deben ser aprobadas, publicadas y comunicadas según lo definido en el Procedimiento de Creación y Actualización de Información Documentada del SGSI y Plan de Concientización del SGSI.

6.1.2. Revisión de las Políticas de Seguridad de Información [ISO 27001 Cl A.5.1.2]
• Se deben realizar revisiones y mantenimiento de las políticas de seguridad de información, según lo definido en el documento Procedimiento de Creación y Actualización de Información Documentada del SGSI.

6.2. Organización de Seguridad de Información (ISO 27001-A.6)

6.2.1. Funciones de seguridad de información y responsabilidades [ISO 27001 Cl A.6.1.1]

• La Institución debe de crear un comité de Seguridad de la Información, que es quien debe tener autoridad y responsabilidad sobre la gestión del SGSI de la UCC.

• El Comité de Gestión de Seguridad de la Información debe designar al Coordinador de Seguridad de la Información, el cual debe ser responsable de la rendición de cuentas sobre el funcionamiento del SGSI al Comité de Gestión de Seguridad de la Información.

• El Comité de Gestión de Seguridad de la Información debe estar conformado por:

➢ El Rector de la Universidad.

➢ El Director de TIC.

➢ El Vicerrector General.

➢ Vicerrectoría de Administración y Finanzas.

➢ La Dirección de Recursos Humanos.

➢ La coordinación de Ciberseguridad.

El comité deberá ser presidido por el Director de TIC.

Para las reuniones del comité, no deberá ser necesario que se encuentren presentes todos los integrantes. En ausencia del presidente del comité este debe ser presidido por quien él haya designado.

La frecuencia de reuniones del comité debe ser 2 veces al año.

El comité deberá poder invitar a otros trabajadores de la Institución, en función de los temas a tratar en la agenda.

• Las funciones y responsabilidades del personal de la Institución, se deben registrar en el documento Manual de Organización y Funciones de la UCC.

• Las funciones y responsabilidades del personal de la Institución con respecto al SGSI se deben registrar en los documentos de registro del SGSI, Manual de Funciones y Responsabilidades del SGSI y, en actas de reunión (cuando corresponda).

Asimismo, las responsabilidades y funciones de seguridad de la información y sus funciones de los terceros con respecto al SGSI se deben registrar en el documento de registro del SGSI, Manual de Funciones y Responsabilidades del SGSI.

6.2.2. Separación de deberes [ISO 27001 Cl A.6.1.2]

• El directorio de accionistas debe asegurar que los roles y responsabilidades definidos para la operación de la Institución deben estar registrados en el documento Manual de Organización y Funciones (MOF) de la UCC y los roles y responsabilidades de seguridad de la información en el documento Manual de Funciones y Responsabilidades del SGSI.

La Responsabilidad de los propietarios de los activos de información, debe ser, dar acceso a la información considerando una adecuada definición y manejo de funciones, en relación a su actividad y función operativa que debe de cumplir, la sensibilidad de los datos y el interés entre las áreas afectadas. A tal efecto es necesario una declaración de perfiles de usuarios y los mismos estarán determinados por grupos específicos para cada sistema de información.

6.2.3. Contacto con autoridades [ISO 27001 Cl A.6.1.3]

• Las áreas con la asesoría del Coordinador de Seguridad de la Información deben establecer internamente la mecánica para recurrir a una instancia técnica de apoyo o asesoría en actividades relacionadas con la seguridad de la información.
El contacto con Bomberos, Policía, Hospitales lo deben gestionar Servicios Generales y el Proveedor de Seguridad Física.

6.2.4. Contacto con grupos de interés especial [ISO 27001 Cl A.6.1.4]

• El personal involucrado en la gestión de seguridad de la información deberá registrarse en foros que le envíen actualizaciones respecto a seguridad de información y; deberán mantener constante relación con las empresas externas que puedan prestar apoyo en caso de incidentes de seguridad de la información, la relación deberá mantenerse a un nivel tal que asegure el apoyo, pero sin generar obligaciones de entregar información confidencial.

6.2.5. Seguridad de información en gerencia de proyectos [ISO 27001 Cl A.6.1.5]

• La seguridad de la información debe integrarse en el método de gestión de proyectos de la Universidad de Ciencias Comerciales para que los riesgos de seguridad de la información sean identificados y tratados como parte de un proyecto.

6.2.6. Política de dispositivo móvil [ISO 27001 Cl A.6.2.1]

• La Universidad de Ciencias Comerciales, campus León, deberá establecer la presente Política de Dispositivo Móvil:

➢ Las características en las capacidades de los equipos deberán ser definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la Institución.

➢ Todos los usuarios de dispositivos móviles que contengan información confidencial o de uso interno deben usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.

➢ Los usuarios que utilicen dispositivos móviles como computadores portátiles, en su puesto de trabajo, para el cumplimiento de las funciones asignadas deberán mantener el equipo asegurado.

➢ Los usuarios de dispositivos móviles deben mantener actualizado el software antivirus del dispositivo.

➢ El Propietario del Activo de Información y el Coordinador de Seguridad de la Información deberán precisar el tipo de información que se puede mantener en los computadores personales que son utilizados fuera de la Universidad. El acceso a estos dispositivos deberá estar protegido mediante controles como claves de acceso de BIOS, software de protección y nunca deberá quedar el computador desatendido sin ningún bloqueo de acceso.

6.2.7. Teletrabajo [ISO 27001 Cl A.6.2.2]

• El servicio de acceso remoto debe permitir el acceso a la red de datos a aquellos usuarios externos e internos expresamente autorizados por el jefe inmediato o el usuario del servicio (en el caso de terceros) y el Coordinador de Seguridad de la Información, para que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.

• Solo los equipos de procesamiento de datos tipo servidor y de comunicación deberán tener habilitado el servicio de conexión de acceso remoto. Los clientes para acceder a estos recursos serán previamente identificados y autorizados.

Cualquier usuario que requiera acceso a la red desde el exterior, sea por Internet o por acceso telefónico deberá estar debidamente autenticado y sus conexiones deberán estar encriptados.

6.3. Seguridad de Recursos Humanos (ISO 27001-A.7)

6.3.1. Evaluación [ISO 27001 Cl A.7.1.1]

• El Sistema Administrativo de Personal y los Usuarios del Servicio (en el caso de terceros) deben mantener listas de verificación de todos los candidatos a trabajadores y terceros, en concordancia con las leyes, regulaciones, ética y requerimientos de la Institución. Dichas listas deben tomar en consideración la privacidad y la protección de los datos del trabajador y/o personal y deben incluir lo siguiente:

➢ La disponibilidad de referencias suficientes.

➢ La comprobación de los documentos de identificación, por ejemplo: currículo vitae, certificados académicos y profesionales.

➢ Comprobaciones más detalladas, por ejemplo: antecedentes penales y/o, policiales y/o de crédito.

6.3.2. Términos y Condiciones de Empleo [ISO 27001 Cl A.7.1.2]

• Los contratos laborales deben incluir una sección en la cual se especifiquen las responsabilidades del empleado por la seguridad de la información.

• La definición debe incluir el tipo de sanciones cuando no se cumpla este requerimiento. Además, deberán estar acordados las responsabilidades y derechos de ley del empleado en cuanto a aspectos de propiedad intelectual, protección de la información y leyes aplicables.

• El Sistema Administrativo de Personal debe definir los términos y condiciones del empleo de los trabajadores de la Universidad.

6.3.4. Conciencia de seguridad de información, educación y capacitación [ISO 27001 Cl A.7.2.2]

Se deben realizar charlas de inducción y sensibilización al personal de la Universidad, donde se deben difundir los temas de Seguridad de la Información, su contribución a la eficacia del SGSI incluyendo los beneficios de un mejor desempeño de seguridad de la información y, las consecuencias del incumplimiento de los requisitos del SGSI, la asistencia por parte de los trabajadores debe ser registrada en el documento Formato de Lista de Asistencia del SGSI.

• La concientización, educación y capacitación del SGSI debe ser administrada por el Coordinador de Seguridad de la Información de acuerdo al documento Plan de Concientización del SGSI y en coordinación con la Coordinación de Recursos Humanos.

6.3.5. Procesos Disciplinarios [ISO 27001 Cl A.7.2.3]

• La Institución deberá establecer que se procederán a sanciones disciplinarias en caso de identificarse violaciones a las políticas y procedimientos relacionados con la seguridad de la información de la Institución, según lo estipulado en el Reglamento Interno de Trabajo.

6.3.6. Término o cambio de las responsabilidades de empleo [ISO 27001 Cl A.7.3.1]

• Las responsabilidades para realizar el cese del empleo de un trabajador o el reemplazo de éste, deben ser bien definidas, asignadas y comunicadas por la Coordinación de Recursos Humanos. En el caso de los terceros, la responsabilidad de finalización o cambio es tomada por el Usuario del Servicio.

La Coordinación de Recursos Humanos, debe ser responsable del proceso de finalización del empleo del trabajador para lo cual debe trabajar conjuntamente con el

jefe del trabajador cesante y, de ser requerido con el Coordinador de Seguridad de la Información.

La comunicación de la finalización de las responsabilidades debe incluir requisitos de seguridad de la información, responsabilidades legales y donde sea apropiado, responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad; asimismo las responsabilidades y tareas que son todavía válidas después de la finalización del empleo deben ser contenidas en dicha comunicación.

La Coordinación de Recursos Humanos debe ser responsable del proceso de cambio del empleo del trabajador para lo cual debe trabajar conjuntamente con el jefe anterior y jefe nuevo del trabajador que cambia de responsabilidades del empleo y, de ser requerido con el Coordinador de Seguridad de la Información.

• Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la Universidad, deben realizarse de acuerdo a los lineamientos definidos en un documento formal.

6.4. Gestión de Activos (ISO 27001-A.8)

6.4.1. Inventarios de Activos [ISO 27001 Cl A.8.1.1]

• La Universidad debe registrar los activos de información que están involucrados en el proceso parte del alcance del SGSI en el documento Formato de Inventario de Activos de Información.

• Para el desarrollo del Inventario de Activos de Información se debe seguir lo especificado en el documento Metodología de Gestión de Riesgos.

6.4.2. Propiedad de activos [ISO 27001 Cl A.8.1.2]

• Todo activo de información debe tener un “Propietario” quien debe ser responsable de asegurar la apropiada clasificación y protección de los mismos; para lo cual, debe definir y revisar periódicamente las restricciones de acceso y las clasificaciones.

El propietario del activo de información se debe registrar en el Inventario de Activos de Información, según lo detallado en el documento Metodología de Gestión de Riesgos.

6.4.3. Uso aceptable de activos [ISO 27001 Cl A.8.1.3]

• El uso de todos los recursos informáticos es de uso exclusivo a tareas relacionadas a las actividades de la Institución.

• Los activos de información deben ser utilizados dentro de un adecuado entorno de seguridad de acuerdo a lo definido en el documento Política de Seguridad de la Información, cualquiera sea el medio que los soportes y el ambiente tecnológico en que se procesen.

6.4.4. Retorno de activos [ISO 27001 Cl A.8.1.4]

• La finalización del empleo debe incluir el retorno previo de los activos de información proporcionados por la Universidad al trabajador para el desempeño de las funciones asignadas.

• En los casos donde los trabajadores compren los equipos de la Universidad o empleen sus propios equipos, se deben seguir procedimientos para asegurar que toda la información de la Institución sea transferida y luego sea borrada con seguridad del equipo.

6.4.5. Clasificación de Información [ISO 27001 Cl A.8.2.1]

• Los colaboradores de la Universidad, deben conocer la clasificación de la información y asegurar la protección de la misma.

• La información debe clasificarse según su sensibilidad o grado de impacto en el negocio, según los siguientes niveles:

➢ Confidencial: Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en la empresa entre ellas: pérdida económica, sanción legal o pérdida de imagen.

➢ Uso Interno: Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la empresa y que solo podrán ser divulgados a terceras partes teniendo firmado un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la Universidad.

➢ Público: Activos de información cuyo contenido no es sensible, de acceso público y que su divulgación no genera impacto en la Institución.

• Los usuarios propietarios de los activos de información deben ser responsables de la clasificación de la información.

6.4.6. Etiquetado de información [ISO 27001 Cl A.8.2.2]

• Teniendo en consideración los niveles mencionados en el punto anterior, la Universidad debe asegurarse que los activos de información lleven un rótulo que identifique en qué nivel de clasificación se encuentran.

6.4.7. Manejo de activos [ISO 27001 Cl A.8.2.3]

• Todo activo de información de la Universidad, deberá tener un “propietario” quien será el encargado de establecer los niveles de protección que le aplique. Estos controles estarán soportados por procedimientos específicos de manejo y control de activos de información.

• Toda información documentada del SGSI deberá ser de uso exclusivo dentro de la Institución. Su entrega total o parcial a terceros deberá ser autorizada por el Coordinador de Seguridad de la Información.

Cualquier documento impreso, y cualquier archivo electrónico que no se encuentre en el repositorio de documentos designado para tal fin, deberán ser considerados fuera del SGSI de la Institución.

6.4.8. Gestión de medios removibles [ISO 27001 Cl A.8.3.1]

• Toda la información almacenada en medios magnéticos removibles de la Institución deberá estar debidamente controlada en cuanto a su uso, transporte y almacenamiento.

6.4.9. Desecho de los medios [ISO 27001 Cl A.8.3.2]

• En el caso de desechar cualquier medio magnético, deberá eliminarse de manera segura cualquier tipo de información contenida en los mismos.

6.4.10. Transferencia de medios físicos [ISO 27001 Cl A.8.3.3]

• Cualquier información que deba ser trasladada desde la Institución a un sitio externo deberá ser transportada en forma segura y controlada previa a su salida. Esto debe aplicar también para el almacenamiento de las copias de respaldo en sitios externos a la Universidad.

• El tratamiento que se les debe dar a los medios que almacenan activos de información de la Institución y que se trasladan fuera del ámbito de la misma se debe realizar según lo especificado en documentos formales de la Universidad.

Control de Acceso (ISO 27001-A.9)

6.5.1. Política de control de acceso [ISO 27001 Cl A.9.1.1]

• La Universidad deberá establecer la presente Política de Control de Acceso:

➢ El control de acceso a los sistemas de información debe realizarse por medio de códigos de identificación y contraseñas únicos para cada usuario.

➢ El acceso a cualquier servicio o recurso de información debe de ser permitido previa identificación y por requerimiento a la Universidad, definido por los propietarios de los activos de información, según norma ley de protección de acceso a la información.

➢ Todos y cada uno de los equipos de cómputo deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

• La presente política debe estar soportada por procedimientos formales y responsabilidades definidas.

6.5.2. Acceso a redes y servicios de red [ISO 27001 Cl A.9.1.2]

• Es obligatorio que los trabajadores que cuenten con equipos informáticos de la Universidad, deberán autenticarse en dichos sistemas. Los usuarios estarán definidos en grupos con perfiles específicos y solo podrán acceder a sistemas que están autorizados.

• Se deberán establecer las acciones y controles para monitorear el uso de los servicios de TI, detectar posibles fallas y analizarlas para tomar las acciones apropiadas.

• Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la Institución, se deben realizar según lo establecido en documentos formales.

6.5.3. Registro y cancelación de registro de usuarios [ISO 27001 Cl A.9.2.1], Provisión del acceso de usuario [ISO 27001 Cl A.9.2.2], Gestión de la información de autenticación secreta de los usuarios [ISO 27001 Cl A.9.2.4], Eliminación o ajuste de derechos de acceso [ISO 27001 Cl A.9.2.6]

• La Universidad, debe establecer un conjunto de controles y procedimientos con el fin de obtener un alto nivel de seguridad en la gestión de contraseñas y usuarios de los sistemas informáticos de la Institución.

• Los trabajadores se deben comprometer a responsabilizarse por toda acción que se realice mediante el usuario y contraseña que le sean asignados. Ningún trabajador deberá compartir sus credenciales por ningún motivo. Todos los usuarios tendrán un único identificador de acceso de modo tal de poder identificar cualquier actividad no autorizada en la red o sistemas informáticos.

• Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la Institución se deben realizar según lo establecido en documentos formales.

6.5.4. Gestión de derechos de acceso privilegiados [ISO 27001 Cl A.9.2.3]

• El control del correcto uso y disposición de contraseñas de los diversos sistemas informáticos considerados críticos para el negocio y en particular sobre el control de acceso lógico a plataformas y sistemas de red que involucran al proceso en el alcance del SGSI se deben realizar según lo establecido en documentos formales.

6.5.5. Revisión de derechos de acceso de usuarios [ISO 27001 Cl A.9.2.5]

• Los administradores propietarios de los activos de información de la Universidad deben revisar periódicamente los derechos de acceso, revocando los que hayan caducado o ya no correspondan.

6.5.6. Uso de información de autenticación secreta [ISO 27001 Cl A.9.3.1], Sistema de gestión de contraseña [ISO 27001 Cl A.9.4.3]

• Se prohíbe bajo responsabilidad compartir las contraseñas bajo ningún tipo de medio ya sea electrónico o de voz.

6.5.7. Restricción de acceso a la información [ISO 27001 Cl A.9.4.1].

• La Institución debe establecer que los usuarios tendrán derecho a acceder a la información según el perfil de usuario asignado y el nivel de clasificación de dicha información.

• Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la Universidad, se deben realizar según lo establecido en documentos formales.

6.5.8. Procedimientos Seguros de inicio de sesión [ISO 27001 Cl A.9.4.2]

• El trabajador será responsable de su cuenta de usuario y quedará constatado bajo formulario de entrega de cuentas. Adicionalmente, los usuarios deben proteger el

acceso a su máquina activando el protector de pantalla o bien haciendo un logout del sistema.

6.5.9. Uso de programas de utilidad privilegiada [ISO 27001 Cl A.9.4.4]

• En la Institución debe restringirse y controlarse estrechamente el uso de aplicaciones que pudieran ser capaces de anular los controles del sistema y las aplicaciones.

6.5.10. Control de acceso al código fuente del programa [ISO 27001 Cl A.9.4.5]

• Se debe restringir y controlar el acceso al código fuente de los programas únicamente al personal autorizado para su edición y/o modificación.

• Se debe de implementar un proceso automático y/o manual que permita controlar el versionamiento del código fuente.

• Si se trata de una aplicación desarrolla por un proveedor externo, se deben revisar las condiciones del contrato.

6.6. Criptografía (ISO 27001-A.10)

6.6.1. Política sobre el uso de controles criptográficos [ISO 27001 Cl A.10.1.1]

• La Universidad deberá establecer la presente Política sobre el Uso de Controles Criptográficos:

➢ Se deberán utilizar controles criptográficos en los siguientes casos:

✓ Para compartir información secreta, fuera de la Institución.

✓ Para la protección y resguardo de la información, demostrada en la evaluación de riesgos realizada por el administrador propietario de Activo de Información.

➢ Se deberán desarrollar lineamientos acerca de la administración de claves, de recuperación de información cifrada, compromiso o daño de las contraseñas y el reemplazo de las claves de cifrado.

6.6.2. Gestión de claves [ISO 27001 Cl A.10.1.2]

• Las llaves criptográficas utilizadas para el cifrado de los datos deben estar clasificadas como Confidencial y ser protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.

• Para minimizar la probabilidad de compromiso, las llaves deberán tener fechas de inicio y caducidad de vigencia.

6.7. Seguridad Física y Ambiental (ISO 27001-A.11)

6.7.1. Perímetro de seguridad física [ISO 27001 Cl A.11.1.1], Control de Entrada Física [ISO 27001 Cl A.11.1.2], Control de Entrada Física [ISO 27001 Cl A.11.1.2], Seguridad de oficinas, salas e instalaciones [ISO 27001 Cl A.11.1.3]

- La Universidad debe establecer que se registrará todo ingreso y egreso del personal interno y visitantes que deban acceder a diferentes sitios de la Institución.

- El acceso a las diferentes áreas de la Institución deberá estar controlado con diferentes medidas de seguridad de control de acceso y salida, así como las autorizaciones de ingreso correspondientes. No se deberá permitir el ingreso de personas internas, tercero y/o visitante, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado.

6.7.2. Protección contra amenazas externas y ambientales [ISO 27001 Cl A.11.1.4]

• Las áreas deberán contar con equipos apropiados de seguridad física para evitar en la Institución el daño ocasionado por desastres naturales o causados por el hombre.

• La Universidad deberá contar con un Certificado de Protocolo de Prueba de Puesta de Tierra actualizado.

6.7.3. Trabajo en zonas seguras [ISO 27001 Cl A.11.1.5]

• Los elementos críticos de la Institución, deberán estar protegidos en áreas seguras para su operación, a través del uso de controles de acceso físico, reglamentos y sanciones; para lo cual se deberá cumplir con las normas y procedimientos utilizados para asegurar la infraestructura y los activos de información que esta contiene.

Como mecanismo de prevención todos los trabajadores, terceros y visitantes no deberán comer, fumar o beber en el Centro de Procesamiento de Datos o en instalaciones donde haya equipos tecnológicos.
• No se debe proveer información sobre la ubicación del Centro de Procesamiento de Datos o de los lugares críticos, como mecanismo de seguridad.

6.7.4. Zonas de entrega y de carga [ISO 27001 Cl A.11.1.6]
• Se deberá establecer un área especial para recepción de material, equipos, correspondencia, etc., la cual deberá estar, aislada de las áreas restringidas que solo deberá tener acceso personal interno autorizado.

6.7.5. Situar los equipos y protección [ISO 27001 Cl A.11.2.1]
Se deberán instalar sistemas de protección eléctrica en el Centro de Procesamiento de Datos, y en otras áreas por determinar, de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Los dispositivos y mecanismos de protección deberán estar alineados con base en el análisis de riesgos.
• La Institución deberá establecer que todos los equipos de hardware y software que se utilice para el tratamiento de información de la Universidad, deberán contar con las medidas de protección eléctrica y de comunicaciones para evitar daños a la información procesada.
6.7.6. Servicios públicos de apoyo [ISO 27001 Cl A.11.2.2]

• La Institución deberá contar con un conjunto de UPS's que asegure el tiempo necesario para que los equipos de cómputo cierren sus actividades para evitar daños y perdida de información.

6.7.7. Seguridad del cableado [ISO 27001 Cl A.11.2.3]

• La Universidad deberá asegurar que todos los equipos de comunicaciones y cableado para el transporte de información, estarán protegidos de daños o interferencias que puedan afectar la integridad y disponibilidad de la información.

6.7.8. Mantenimiento de los equipos [ISO 27001 Cl A.11.2.4]

• Los equipos informáticos deberán mantenerse según el plan de mantenimiento asignado, teniendo en cuenta las especificaciones recomendadas por el proveedor y que sólo el personal de soporte autorizado puede brindarlo para llevar a cabo reparaciones, y por otra parte se debe de tener una bitácora de eventos de los equipos informáticos. Además, cuando se retiran equipos de la Institución para su mantenimiento se debe cumplir con todos los requisitos impuestos por las pólizas de seguro en cuanto a la seguridad del equipamiento fuera del ámbito de la Institución.

6.7.9. Retiro de los activos [ISO 27001 Cl A.11.2.5]

• La Institución deberá establecer que los usuarios que requieran retirar información fuera de las oficinas de trabajo habitual, deberán estar autorizados por el responsable del área al que pertenecen dichos usuarios.

• El retiro de los activos deberá realizarse según los lineamientos formalmente definidos en la Institución.

6.7.10. Seguridad de los equipos y de los activos fuera de las instalaciones [ISO 27001 Cl A.11.2.6]

• Todo equipo de cómputo o medios de almacenamiento que son utilizados fuera de la Institución, (computadores portátiles, etc.), no deberán salir de la misma sin una autorización escrita previa.
• El Propietario de Activo de Información en coordinación con el responsable de Seguridad de la Información deberá precisar el tipo de información que se puede mantener en este tipo de equipamiento, aún si estos no son propiedad de la Universidad.

Cuando un equipo de computación deba repararse, éste no saldrá del edificio sin tener una notificación firmada por el responsable del mismo, donde se detalle la información de la maquina (marca, modelo y serie).
• Se registrará los datos de la Universidad y la persona que se lleva dicho equipo. Para el traslado de equipos o dispositivos que contengan información y archivos de la Universidad.

6.7.11. Eliminación segura o reúso de equipos [ISO 27001 Cl A.11.2.7]
• Todo equipamiento que contenga medios de almacenamiento debe revisarse para asegurar que todos los datos sensibles y software licenciado se haya eliminado de forma segura antes de su eliminación o reutilización.

El borrado de información y destrucción de medios de información, exclusivo para cualquier documento que contenga información confidencial, dispositivos de almacenamiento como cintas magnéticas, medios de almacenamiento óptico o para los equipos que son operados en la Institución, cuando estos deban ser entregados o retirados por terceros del sitio de instalación por motivo de cambios, reparación o destrucción se debe realizar según lo especificado en los documentos formales de la Universidad.

6.7.12. Equipos de usuarios no atendidos [ISO 27001 Cl A.11.2.8]

• Los usuarios deberán bloquear sus computadores personales y los servidores al retirarse de las mismas independientemente del tiempo que permanezcan alejados.

6.7.13. Política de escritorio y pantalla limpia [ISO 27001 Cl A.11.2.9]

• La Universidad deberá establecer la presente Política de Escritorio y Pantalla Limpia:

➢ No se permitirá que los usuarios dejen papeles impresos sobre el escritorio fuera de las horas laborales. Asimismo, no deberán dejar ningún medio de almacenamiento portátil al alcance. Todos estos dispositivos se dejarán bajo llave.

➢ Se deberá tener especial cuidado con el uso de dispositivos como fotocopias e impresoras de manera que el material con información sensible no permanezca en ellas sin atención, y que no se use papel reciclado que contenga información confidencial.

La presente política debe estar soportada por procedimientos formales y responsabilidades definidas.

6.8. Seguridad de Operaciones (ISO 27001-A.12)

6.8.1. Procedimientos de operación documentados [ISO 27001 Cl A.12.1.1]

• La Universidad deberá establecer que deberán existir procedimientos, registros y guías documentadas para mantener el SGSI.

• Para la creación y actualización de la información documentada contenida en el SGSI se deberá coordinar con los responsables de los activos y presentar los cambios al comité de seguridad de información.

6.8.2. Gestión de cambio [ISO 27001 Cl A.12.1.2]

• Todo cambio en los sistemas de información de la Institución deberán ser actualizados bajo los procedimientos formales de control de cambios y estos no deben de afectar la continuidad, ni la disponibilidad ni la integridad de la información.

• La gestión de cambio deberá realizarse según los lineamientos formales definidos por la Universidad.

6.8.3. Gestión de capacidad [ISO 27001 Cl A.12.1.3]

• En la Institución se deberá proyectar y asegurar las demandas de capacidad de almacenamiento y procesamiento de información para evitar bajo desempeño de los sistemas o perder información por el mal uso de los recursos informáticos actuales.

• La gestión de la capacidad deberá realizarse según los lineamientos formales definidos por la Universidad.

6.8.4. Separación de evaluaciones de desarrollo y entornos operacionales [ISO 27001 Cl A.12.1.4]

• La Institución deberá establecer que no deberán realizarse pruebas, instalaciones o desarrollos sobre el entorno de producción, se deberá contar con ambientes separados para efectuar el desarrollo y mantenimiento de los sistemas de información y que se deberá utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas; con el fin de evitar errores de integridad de la información utilizada en la Institución.

6.8.5. Control contra malware [ISO 27001 Cl A.12.2.1]

• La Universidad deberá establecer que todo equipo informático deberá estar protegido mediante un software Antivirus y antimalware. Deberá ser responsabilidad del usuario y personal del área de Tecnologías de la Información correspondiente prever que el software instalado no sea deshabilitado.

Para el control contra códigos maliciosos se deben seguir los lineamientos formales definidos por la Institución.

6.8.6. Backup [ISO 27001 Cl A.12.3.1]

• La Universidad deberá asegurar que toda la información almacenada en los equipos de respaldo sea respaldada de manera diaria usando los procedimientos que indiquen su identificación, protección y la disponibilidad en cuanto sea requerida.

Toda información resguardada en medios magnéticos deberá almacenarse en lugares que cumplan con máximas medidas de protección. Tales medidas deberán incluir su resguardo en una ubicación física adecuada, la cual deberá contar con mecanismos de detección de humo, calor y humedad y control de acceso físico.

• La información crítica que deba ser almacenada en medios magnéticos serán almacenadas fuera de las instalaciones de la Universidad, este sitio deberá tener disponibilidad inmediata y que cuenten con los mecanismos de protección contra incendios, control de humedad y acceso físico.

La Universidad deberá establecer los períodos de retención de la información magnética respaldada, así como la recuperación de la información almacenada

• La Universidad deberá establecer la existencia de sistemas manuales o automáticos de inventario de los medios magnéticos que contengan la información resguardada. Estos sistemas deberán permitir la identificación unívoca de los medios de almacenamiento, la identificación de la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a la información resguardada.

6.8.7. Registro de eventos [ISO 27001 Cl A.12.4.1]

• Todos los sistemas informáticos de la Institución, contaran con un registro de eventos de seguridad y ser monitoreado y consultado cuando se requiera. La información sensible deberá ser registrada mediante logs de acceso.

• La Universidad deberá establecer que todos los logs que se registren serán mantenidos en forma confidencial y de acceso privilegiado de solo lectura. Se deberán poder revisar estos logs cada vez que un incidente de seguridad de la información lo requiera o bien dentro de los procesos de revisión periódica de auditoría.

• Para la generación y formato de los registros de auditoría deberá seguirse los lineamientos formalmente definidos por la Institución.

6.8.8. Protección de información de registro [ISO 27001 Cl A.12.4.2]

Los registros de auditoría deberán protegerse contra su alteración y uso no autorizado según los lineamientos formalmente definidos por la Universidad.

6.8.9. Registros de administrador y operador [ISO 27001 Cl A.12.4.3]

• Todas las actividades de administración realizadas por el personal de la Institución deberán estar debidamente registradas y revisadas periódicamente por el Coordinador de Seguridad de la Información.

• Para la generación y formato de los registros de auditoría deberán seguirse los lineamientos formales definidos por la Institución.

6.8.10. Sincronización de reloj [ISO 27001 Cl A.12.4.4]

• Todos los relojes de los sistemas informáticos de la Universidad, deberán estar sincronizados para obtener un control apropiado para la determinación exacta de eventos no deseados en la infraestructura de red o para la investigación efectiva de incidentes de seguridad de la información.

• Para la sincronización de relojes deberán seguirse los lineamientos formales definidos por la Universidad.

6.8.11. Instalación de software en sistemas operacionales [ISO 27001 Cl A.12.5.1]

• La Universidad deberá establecer que existirán controles para asegurar que los cambios o actualizaciones de los sistemas informáticos no provoquen errores de procesamiento de información y evitar la pérdida de integridad de los datos.

La instalación de software en sistemas operacionales deberá realizarse según los lineamientos formales definidos por la Institución.

6.8.12. Gestión de vulnerabilidades técnicas [ISO 27001 Cl A.12.6.1]

• La Universidad debe obtener de forma periódica información sobre las vulnerabilidades técnicas de los sistemas de información, evaluar su exposición a tales vulnerabilidades y debería tomar medidas para abordar el riesgo asociado.

6.8.13. Restricciones en la instalación de software [ISO 27001 Cl A.12.6.2]

• Para todos los equipos de cómputo propiedad de la Institución, se deberá instalar únicamente el software que cuente con licencia autorizada para uso en la Universidad. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley sobre el Derecho de Autor.

• Las restricciones para la instalación de software deberán realizarse según los lineamientos definidos formalmente por la Institución.

6.8.14. Controles de auditoría de sistemas de información [ISO 2700 1 Cl A.12.7.1]

• Las auditorías y controles de seguridad se realizarán por lo menos 1 vez al año, dentro del plan de auditoría interna, a efectos de mejorar la efectividad de los controles. Estas auditorías contemplarán la plataforma tecnológica y los procesos de gestión de la Seguridad de la Información de la Universidad.

Las auditorias serán coordinadas con el Coordinador de Seguridad Información, su ejecución no debe de interrumpir las operaciones diarias de los sistemas de información.

• Los auditores tendrán toda la información que necesite con permisos de solo lectura.

• Las auditorías deberán realizarse según los lineamientos definidos en el documento Procedimiento de Auditoría Interna del SGSI.

6.9. Seguridad de Comunicaciones (ISO 27001-A.13)

6.9.1. Controles de redes [ISO 27001 Cl A.13.1.1]

• La Institución deberá establecer un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos según los resultados del análisis de riesgos sobre los activos de información.

El servicio de internet y su infraestructura de red será usado exclusivamente para las actividades de interés de la Universidad.

• El servicio de internet no debe de ser utilizado para interferir con la labor diaria del usuario en la Institución.

• Los controles de redes deberán realizarse según los lineamientos formales definidos por la UCC.

6.9.2. Seguridad de los servicios de redes [ISO 27001 Cl A.13.1.2]

• La UCC deberá establecer que todos los sistemas y servicios de red estarán actualizados con los parches y recomendaciones de los fabricantes para asegurar los niveles óptimos de control y seguridad.

• La seguridad de los servicios de redes deberá implementarse según los lineamientos formales definidos por la UCC.

6.9.3. Separación en redes [ISO 27001 Cl A.13.1.3]

• La UCC deberá controlar la seguridad de la red dividiéndola en dominios de red separados, lo cual deberá implementar siguiendo los lineamientos formalmente definidos por la UCC.

6.9.4. Procedimientos y políticas de transferencia de información [ISO 27001 Cl A.13.2.1], Acuerdos sobre transferencia de información [ISO 27001 Cl A.13.2.2]

• La UCC deberá establecer la presente Política de Transferencia de Información:

➢ Toda la información en formato impreso o electrónico que sea utilizada entre organizaciones o usuarios externos y la UCC, deberá estar bajo normativas de un Acuerdo de Confidencialidad mutuo (Formato de Acuerdos de Confidencialidad para Terceros), donde quedarán especificadas las responsabilidades para cada una de las partes.

El intercambio de información manual, solo debe utilizar los servicios de correos autorizados en la UCC. Debe ser entregada personalmente al destinatario en sobre sellado y su entrega debe quedar registrada.

➢ Toda información enviada a través del correo de la UCC, debe incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información.

Todos los medios de información, con datos pertenecientes a la UCC que deban ser trasladados fuera de la UCC o ingresados desde algún lugar hacia la UCC, deben seguir los lineamientos formalmente definidos por la UCC.

6.9.5. Mensajería electrónica [ISO 27001 Cl A.13.2.3]

• El Comité de Gestión de Seguridad de la Información de la Institución deberá ser quien vele por el cumplimiento de la cultura en UCC acerca del buen uso del correo

electrónico. Los usuarios serán responsables de toda la actividad que se realice en su cuenta de correo electrónico de la Universidad.

6.9.6. Acuerdo de confidencialidad o de no divulgación [ISO 27001 Cl A.13.2.4]

• Para todo tipo de contratación (a plazo fijo o indeterminado), la UCC debe asegurar que el nuevo trabajador firme el documento Formato de Acuerdos de Confidencialidad para Trabajadores para proteger los activos de información que este maneje. Con respecto a los proveedores y terceros que contraten con la UCC se deberán establecer acuerdos de servicios de carácter preventivo para que exista una previsión sobre la calidad del servicio recibida además de firmar el documento Formato de Acuerdos de Confidencialidad para Terceros.

6.10. Adquisición, Desarrollo y Mantenimiento de Sistemas (ISO 27001-A.14)

6.10.1. Análisis y especificaciones de los requisitos de seguridad de la información [ISO 27001 Cl A.14.1.1]

• Siempre que se establezca un requerimiento nuevo para un sistema, se deberán especificar los controles o requerimientos de seguridad asociados a él y a su implantación, además del análisis de riesgo y de impacto derivado en una posible falla.

• El análisis y especificaciones de los requisitos de seguridad de la información se deben realizar según los lineamientos formalmente definidos por la UCC.

6.10.2. Asegurar los servicios de aplicaciones en redes públicas [ISO 27001 Cl A.14.1.2]

• Se deberán realizar evaluaciones de riesgos y seleccionar los controles adecuados para proteger la información involucrada en las aplicaciones gratuitas en las redes públicas.

• Para asegurar los servicios de aplicaciones en redes públicas se deben seguir los lineamientos formales definidos por la UCC.

6.10.3. Política de desarrollo de seguridad [ISO 27001 Cl A.14.2.1]

• La UCC deberá establecer la presente Política de Desarrollo de Seguridad:

➢ El software debe poder ser adquirido a través de terceras partes o desarrollado por personal propio de la UCC.

➢ Se debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.

Los productos de software adquiridos a través de terceras partes deben cumplir con los lineamientos formales de incorporación de sistemas de información establecidos por la UCC.

6.10.4. Procedimientos de control de cambios de sistema [ISO 27001 Cl A.14.2.2]

• Los sistemas que procesen información de la UCC, serán modificados y autorizados según los procedimientos de control de cambios, estos asegurarán que solo se cambiara lo aprobado. Las áreas funcionales y de riesgos deberán formar parte de la aprobación. Estos cambios deberán ser registrados en una bitácora.

6.10.5. Revisión técnica de las aplicaciones después de los cambios de la plataforma de operación [ISO 27001 Cl A.14.2.3]

• Cuando se realicen cambios o actualizaciones a los sistemas operativos, se deberán realizar pruebas para garantizar que no se afecta la seguridad de los mismos. El Coordinador de Seguridad de la Información deberá supervisar los cambios y la evaluación de su impacto en las aplicaciones.

6.10.6. Restricciones a los cambios en los paquetes de software [ISO 27001 Cl A.14.2.4]

Los cambios en el software deberán limitarse a los necesarios y estos deberán ser estrictamente controlados, siguiendo los lineamientos formalmente definidos en la UCC.

6.10.7. Principios de ingeniería de sistemas seguros [ISO 27001 Cl A.14.2.5]

• El desarrollo de software debe aplicar técnicas seguras de ingeniería, las cuales deben estar documentadas y deben revisarse periódicamente.

6.10.8. Entorno de desarrollo seguro [ISO 27001 Cl A.14.2.6]

• Se debe contar con control de acceso al ambiente de desarrollo de software.

6.10.9. Desarrollo de externalización [ISO 27001 Cl A.14.2.7]

• Deberá realizarse estrictamente la supervisión de los contratos y seguimiento de las actividades de desarrollo de software desarrollado por terceros.

6.10.10. Pruebas de seguridad del sistema [ISO 27001 Cl A.14.2.8]

• Se deben realizar pruebas de las funcionalidades de seguridad, tanto para el software desarrollado internamente como el software desarrollado por terceros.

6.10.11. Pruebas de aceptación del sistema [ISO 27001 Cl A.14.2.9]

• Para el caso de actualizaciones y cambios de versiones de los sistemas de procesamiento de información críticos, deberá existir una autorización formal de aceptación por parte del responsable del sistema, luego de haber realizado las pruebas necesarias de funcionamiento apropiado de los nuevos sistemas a implantar.

• Los cambios se deben regir por los lineamientos formalmente definidos en la UCC.

6.10.12. Protección de datos de prueba [ISO 27001 Cl A.14.3.1]

• Las pruebas de aceptación se deben realizar en un ambiente de pruebas separado del ambiente de producción.

• Las pruebas que usen los datos de producción deberán ser filtradas para no exponer información crítica. Se deben definir los procedimientos para el uso de la información requerida. Los ambientes de prueba deberán tener implementados los mismos mecanismos de control de acceso que los sistemas de producción.

6.11. Relación de Proveedores (ISO 27001-A.15)

6.11.1. Política de seguridad de información para la relación con los proveedores [ISO 27001 Cl A.15.1.1]

• La UCC deberá establecer la presente Política de Seguridad de Información para la Relación con los proveedores:

Los terceros deben firmar el documento Formato de Acuerdos de Confidencialidad para Terceros al momento de realizar la legalización de sus contratos, en los cuales se comprometen a no exponer o divulgar, copiar y explotar la información de la UCC a la cual tengan acceso.

➢ La información de la empresa administrada, manejada o creada por los terceros deberá ser de la UCC, al igual que los Sistemas de Información desarrollados por personal tercero; por lo anterior, la UCC deberá ser propietaria de los derechos de esta información.

-Deberá estar prohibido por la UCC, debido a la Ley sobre el Derecho de Autor, realizar copias no autorizadas de software.

-El correo electrónico de la empresa deberá ser usada solo con fines de interés dentro de la UCC.

Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como confidencial, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.

El servicio de acceso remoto deberá permitir el acceso a la red de datos a aquellos usuarios externos expresamente autorizados por el usuario del servicio y el Coordinador de Seguridad de la Información, para que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.

Los terceros no deben comer, fumar o beber en el Centro de Procesamiento de Datos o en instalaciones donde haya equipos tecnológicos.

➢ No se debe proveer información sobre la ubicación del Centro de Procesamiento de Datos o de los lugares críticos, como mecanismo de seguridad.

➢ Los terceros deberán registrar al momento de su entrada en el puesto de control, el ingreso de equipos de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la UCC.

➢ Los terceros deben portar en un lugar visible el elemento que los identifica como tales, mientras permanezcan dentro de las instalaciones de la UCC.

• La presente política debe estar soportada por procedimientos formales y responsabilidades definidas.

6.11.2. Abordar la seguridad dentro de acuerdos con proveedores [ISO 27001 Cl A.15.1.2] y Cadena de suministro de tecnología de información y comunicaciones [ISO 27001 Cl A.15.1.3]

• Los Usuarios del Servicio deben definir los requisitos de seguridad con terceros los cuales se deben incluir en los Términos de Referencia del Servicio y también deberán incluirse en el documento Formato de Acuerdos de Confidencialidad para Terceros.

6.11.3. Monitoreo y revisión de los servicios de proveedores [ISO 27001 Cl A.15.2.1]

• Los servicios de terceros se deberán monitorear y revisar de acuerdo al pliego técnico especificado en los Términos de Referencia del servicio.

• Este monitoreo y revisión se deberá realizar siguiendo los lineamientos definidos en la UCC.

6.11.4. Gestión de cambios de los servicios del proveedor [ISO 27001 Cl A.15.2.2]

• Se deberá mantener la operación de la UCC controlando el impacto de los servicios de terceros ante cambios.

Los terceros deberán gestionar los cambios siguiendo los lineamientos definidos en los documentos correspondientes.

6.12. Gestión de Incidentes de Seguridad de la Información (ISO 27001-A.16).

6.12.1. Responsabilidades y procedimientos [ISO 27001 Cl A.16.1.1] y Informe de eventos de seguridad de información [ISO 27001 Cl A.16.1.2].

La UCC deberá establecer un conjunto de procedimientos y responsabilidades para el manejo de eventos e incidentes de seguridad de la información con el fin de asegurar una respuesta efectiva, restablecer la operación del negocio y analizar las causas con fines de auditoría.

• Todo evento e incidente de seguridad de la información detectado, debe ser reportado inmediatamente al Coordinador de Seguridad de la Información y al responsable de la plataforma afectada, siguiendo el procedimiento específico de manejo de incidentes denominado Procedimiento de Gestión de Incidentes de Seguridad de la Información.

6.12.2. Informes de debilidades de seguridad de información [ISO 27001 Cl A.16.1.3]

• La UCC deberá establecer la realización periódica de análisis de vulnerabilidad y riesgos (lo cual se deberá realizar según lo especificado en el documento Metodología de Gestión de Riesgos) sobre los activos de información parte del alcance del SGSI, se

debe de registrar todas las evaluaciones dando solución a los problemas encontrados y si es necesario se deberá modificar las políticas de seguridad de la información.

Adicionalmente, cualquier usuario deberá poder reportar vulnerabilidades detectadas o sospechas que se tengan al Coordinador de Seguridad de la Información, según los lineamientos definidos en el documento Procedimiento de Gestión de Incidentes de Seguridad de la Información. El Coordinador de Seguridad de la Información deberá ser el único personal autorizado para evaluar las debilidades reportadas. Si alguien no autorizado realiza alguna actividad de ese tipo, deberá ser interpretada como un mal uso del sistema y un incumplimiento a las políticas establecidas.

6.12.3. Evaluación y decisión sobre los eventos de seguridad de información [ISO 27001 Cl A.16.1.4]

• Todo evento que refiera a seguridad de la información deberá evaluarse y decidir si se trata como incidente de seguridad de la información, lo cual se deberá realizar según las indicaciones de la gestión de tratamiento de riesgos.

6.12.4. Respuesta a los incidentes de seguridad de información [ISO 27001 Cl A.16.1.5]

• Los eventos catalogados como incidentes de seguridad de la información deben responderse de acuerdo a lo definido en la Gestión de Tratamiento de Riesgos.

6.12.5. Aprendiendo de los incidentes de seguridad de la información [ISO 27001 Cl A.16.1.6]

• El Coordinador de Seguridad de la Información deberá registrar los incidentes ocurridos, analizará su impacto, la frecuencia y forma de resolución, con estos datos generará una estadística de comportamiento y respuesta ante los incidentes, se establecerá mejoras en las acciones de control y las políticas de seguridad de la

información; lo cual deberá realizarse según los lineamientos definidos en el documento Procedimiento de Gestión de Incidentes de Seguridad de la Información.

6.12.6. Recolección de evidencia [ISO 27001 Cl A.16.1.7]

• Se deben mantener las evidencias de los incidentes de seguridad de la información, lo cual se debe realizar según los lineamientos definidos en el documento Procedimiento de Gestión de Incidentes de Seguridad de la Información.

• Los mecanismos de control identificarán toda acción maliciosa sobre la información crítica que le pertenece a la UCC. Las actitudes sospechosas de un usuario serán registradas en detalle para usarse como evidencia y permita la aplicación de sanciones de acuerdo al impacto ocasionado por su acción.

6.13. Aspectos de Seguridad de la Información de Gestión de la Continuidad del Negocio (ISO 27001-A.17)

6.13.1. Planeando la continuidad de seguridad de información [ISO 27001 Cl A.17.1.1]

• La UCC deberá asegurar la continuidad de las operaciones en caso de una contingencia no prevista con el fin de reducir el impacto en el negocio. Para ello deberá existir un plan de contingencia debidamente documentado y administrado “in situ” para el desarrollo y mantenimiento de los servicios informáticos en la UCC denominado Plan de Contingencias Informático; el cual debe estar elaborado con base en los lineamientos y requerimientos de la seguridad de la información y debe estar sujeto a escalamiento y pruebas.

6.13.2. Implementación de la continuidad de seguridad de información [ISO 27001 Cl A.17.1.2]

• La UCC deberá contar con procedimientos que permitan hacer frente a contingencias y reducir la resiliencia, disminuyendo el impacto que pueda tener para la UCC.

La implementación de la continuidad de seguridad de la información debe realizarse según los lineamientos definidos en el documento Plan de Contingencias Informático.

6.13.3. Verificar, revisar y evaluar la continuidad de seguridad de la información [ISO 27001 Cl A.17.1.3]

• El Plan de Contingencias Informático debe recibir mantenimiento para que se encuentre actualizado al momento de ser probado y se encuentre apegado a la realidad de las operaciones en la UCC.

• Periódicamente el Coordinador de Seguridad de la Información, deberá revisar y probar la efectividad del Plan de Contingencias Informático vigente. Las pruebas consisten en simular varios escenarios posibles de emergencias y lograr la recuperación de información en el menor tiempo posible.

6.13.4. Disponibilidad de instalaciones de procesamiento de información [ISO 27001 Cl A.17.2.1]

• La UCC debe implementar con redundancia suficiente las instalaciones de procesamiento de información para cumplir con el requisito de disponibilidad.

Se deberá contar con máquinas virtualizadas para operación crítica de la UCC.

6.14. Cumplimiento (ISO 27001-A.18)

6.14.1. Identificación de la legislación aplicable y los requisitos contractuales [ISO 27001 Cl A.18.1.1]

• La UCC deberá establecer que ante cualquier presentación legal que se requiera y esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo para asegurar los requisitos regulatorios que apliquen.

6.14.2. Derechos de propiedad intelectual [ISO 27001 Cl A.18.1.2]

• Se tendrá un estricto control a la cantidad y vigencia de las licencias de software base (sistemas operativos), Base de Datos y aplicaciones de desarrollo comercial utilizadas por la UCC. El infringir esta norma pone en riesgo la imagen de la UCC ya que se puede interpretar como un uso de software no licenciado o ilegal, en consecuencia, puede perjudicar económica y legalmente a la empresa. Adicionalmente, los Contratos con terceros deberán contemplar aspectos referidos a los derechos de propiedad intelectual.

El personal del Área de Tecnologías de la Información correspondiente deberá mantener un archivo de todas las licencias adquiridas para futuras auditorías.

• El personal del área de Tecnologías de la Información realizará revisiones inopinadas a los equipos de la empresa con el fin de encontrar software ilegal, de ser encontrado, el usuario será responsable de las acciones administrativas, civiles y penales.

6.14.3. Protección de registros [ISO 27001 Cl A.18.1.3]

• Se deberán establecer los lineamientos que aseguren la protección de los registros contra pérdida, destrucción, falsificación y acceso no autorizado, lo cual se deberá realizar según los lineamientos definidos en el documento Procedimiento de Control de Información Documentada del SGSI.

6.14.4. Privacidad y protección de datos personales [ISO 27001 Cl A.18.1.4]

• Los registros de personal y sus datos privados deberán almacenarse en lugar seguro para evitar robo de información privada que pueda afectar la integridad del personal de la UCC.

6.14.5. Revisión independiente de seguridad de la información [ISO 27001 Cl A.18.2.1]

• El Coordinador de Seguridad de la Información debe realizar revisiones de seguridad cada 6 meses y un ente auditor externo deberá certificar la vigencia del SGSI una vez al año.
• Las auditorías al SGSI deberán realizarse siguiendo los lineamientos definidos en el documento Procedimiento de Auditoría Interna del SGSI.

6.14.6. Cumplimiento de las políticas y normas de seguridad [ISO 27001 Cl A.18.2.2]

• El Coordinador de Seguridad de la Información en conjunto con el Comité de Gestión de Seguridad de la Información son responsables del cumplimiento de todas las directivas, normas, procedimientos y estándares definidos para la UCC son cumplidas en su totalidad, las reuniones del comité para tal fin deberán quedar registradas en Actas de Reunión.
• Para evitar la ocurrencia o recurrencia de no conformidades existentes en el SGSI se deberán realizar las actividades definidas en el documento Procedimiento de Acciones Correctivas del SGSI.

6.14.7. Revisión de cumplimiento técnico [ISO 27001 Cl A.18.2.3]

• Todos los sistemas informáticos de la UCC deberán ser evaluados constantemente por el Coordinador de Seguridad de la Información en busca de vulnerabilidades con pruebas de penetración y aplicando los parches necesarios.

A6. DIRECTIVA DEL USO DE CONTRASEÑA EN EL ACCESO A LOS EQUIPOS INFORMÁTICOS Y APLICACIONES DE LOS SERVICIOS DE LA UNIVERSIDAD DE CIENCIAS COMERCIALES, CAMPUS LEÓN.

I. OBJETIVO

Establecer los procesos de gestión para una adecuada política de contraseñas y uso de acceso a los equipos informáticos y aplicaciones de los servicios de la UCC.

II. FINALIDAD

Controlar mediante una contraseña el acceso a un equipo (informático, de red, de comunicaciones, sistema contra incendio, sistema de acceso de personal, etc.) y a las aplicaciones de los servicios de la UCC; para resguardar la integridad, confidencialidad y disponibilidad de su respectiva información.

II. ALCANCE

La presente Política es de cumplimiento obligatorio para todo el personal de la Universidad, en específica al área de proyectos, indistintamente de su régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios o tengan acceso a la información de la Universidad.

IV. BASE LEGAL

4.1. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
4.2. Ley N° 27444, Ley del Procedimiento Administrativo General.

V. DISPOSICIONES GENERALES

5.1. La presente Directiva regula el correcto uso de las contraseñas y del acceso a los equipos informáticos y aplicaciones de los servicios de la Universidad.
5.2. El objetivo de que todo el proceso de comunicación sea gestionado de forma segura a la hora de acceder a los equipos informáticos, recae en la toma de una serie de medidas y buenas prácticas encaminadas a mejorar la seguridad.
5.3. Para cumplir este objetivo nos basamos en la norma ISO 27002 – control de accesos".

5.4. Buscamos el cumplimiento del Anexo de esta norma:

• A (Normativo) - Objetivos de Control y Controles de Referencia;

• A.9.4 Control de acceso a sistema y aplicación – Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones;

• A.9.4.1 Restricción de acceso a la información – Control: El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.

A.9.4.2 Procedimiento de ingreso seguro – Control: Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.

• A.9.4.3 Sistema de gestión de contraseñas – Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.

A.9.4.4 Uso de programas utilitarios privilegiados – Control: El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones debe ser restringido y controlarse estrictamente.

• A.9.4.5 Control de acceso al código fuente de los programas – Control: El acceso al código fuente de los programas debe ser restringido.

VI. DISPOSICIONES ESPECÍFICAS

6.1. Contraseña de acceso a los equipos

6.1.1 Todos los equipos (PC, laptop, tableta, teléfono, etc.) en uso, contarán con una contraseña de arranque para el encendido, la cual será conocida solo por el usuario del equipo.

6.1.2 La contraseña es personal e intransferible y sólo deberá ser utilizada por el usuario del equipo, quien será el único responsable de su confidencialidad.

6.1.3 Los usuarios de los equipos deben seguir las buenas prácticas de seguridad de la información en la generación y uso de contraseñas: mantener la confidencialidad de las contraseñas; no mantener registros de las contraseñas en por ejemplo papel, archivo digital con texto plano u otros medios utilizados para recordar la contraseña.

6.1.4 La contraseña no se debe transmitir verbalmente a través de líneas telefónicas, ni en texto mediante redes. Se debe utilizar un medio confiable para la comunicación de las mismas.

6.1.5 Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

Tener como mínimo ocho (08) caracteres hasta un máximo de quince (15).

• Tener mezcla de letras mayúsculas y minúsculas, números, caracteres especiales, acrónicos, acrónicos con números, acrónicos como frases.

• No usar nombres, números ni fechas de eventos relacionados con el usuario.

6.1.6 La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de 01 mes; concluido este plazo, el sistema solicitará el cambio de la clave para tener acceso al equipo.

6.1.7 La contraseña de acceso al equipo se bloqueará después de tres (03) intentos de acceso fallido.

6.1.8 Cuando el usuario abandone su equipo, deberá bloquearlo para evitar que otra persona lo use.

6.1.9 La Oficina de Tecnología de Información poseerá una ‘Contraseña de Administrador’ para poder acceder y/o cambiar dicha contraseña, ante la necesidad justificada y ausencia del responsable del equipo, previa solicitud y autorización del responsable del área involucrada.

6.2. Contraseña de acceso a la red

6.2.1 El acceso de los equipos informáticos a la red, tendrá como mecanismo de seguridad lógico, la utilización de una contraseña de red.

6.2.2 Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

• Tener como mínimo ocho (08) caracteres hasta un máximo de quince (15).

• Tener mezcla de letras mayúsculas y minúsculas, números, caracteres especiales, acrónicos, acrónicos con números, acrónicos como frases.

• No usar nombres, números ni fechas de eventos relacionados con el usuario.

6.2.3 Dicha contraseña es personal e intransferible y sólo deberá ser utilizada por el usuario del equipo, quien será el único responsable de su confidencialidad.

6.2.4 La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de 3 meses.

6.2.5 Recién después de utilizar tres (03) contraseñas diferentes se puede reutilizar una contraseña anterior.

6.2.6 La contraseña de acceso a la red se bloqueará después de tres (03) intentos de acceso fallido.

6.2.7 Ante el bloqueo de una contraseña de acceso a la red, el usuario debe comunicarse al área TIC, para desbloquear la contraseña.

6.2.8 Tener cuidado con los navegadores Web que ofrecen recordar la contraseña para una próxima visita a la página. Es importante entender cómo se guarda y dónde, y cuáles son los riesgos. Si existen dudas, no tomar la opción ofrecida.

6.3. Contraseña de acceso a las aplicaciones o sistemas de información

6.3.1 El acceso de los equipos informáticos a una aplicación o sistema de información, tendrá como mecanismo de seguridad lógica, la utilización de una contraseña.

6.3.2 Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

• Tener como mínimo doce (12) caracteres hasta un máximo de quince (15).

• Tener mezcla de letras mayúsculas y minúsculas, números, caracteres especiales, acrónicos, acrónicos con números, acrónicos como frases.

• No usar nombres, números ni fechas de eventos relacionados con el usuario.

6.3.3 La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de un (01) mes.

6.3.4 Los usuarios de los sistemas de información deben seguir las buenas prácticas de seguridad de la información en la generación y uso de contraseñas: mantener la confidencialidad de las contraseñas; no mantener registros de las contraseñas en por ejemplo papel, archivo digital con texto plano u otros medios utilizados para recordar la contraseña.

6.3.5 Debe restringirse totalmente el acceso a una aplicación o sistema de información hasta que haya sido debidamente autenticado y el proceso de conexión de los recursos haya terminado satisfactoriamente.

6.3.6 La conexión sólo permitirá al usuario acceder a la aplicación o sistema de información a la cual está autorizado de conformidad con los requerimientos de su trabajo.

6.3.7 Las contraseñas nunca deben ser almacenadas en los sistemas de información, debido a que personas no autorizadas podrían hacer mal uso de ellas.

6.3.8 No se debe ingresar, modificar y/o eliminar data por fuera de la aplicación; si fuera el caso debe contar con la autorización correspondiente.

6.3.9 En la medida de lo posible, el código fuente de los sistemas de información no debe incluir las contraseñas.

6.3.10 En el caso de utilizar contraseñas o PIN's (Personal Identification Numbers) generados automáticamente por el sistema de información; el programa o algoritmo de generación debe estar específicamente protegido.

6.3.11 Recién después de utilizar cinco (05) contraseñas diferentes se puede reutilizar una contraseña anterior.

6.3.12 Se debe revisar periódicamente los derechos de acceso de los usuarios y los perfiles en los servicios de tratamiento de información.

6.3.13 En la medida que los sistemas lo permitan, los intentos infructuosos de conexión deberán contabilizarse, estableciéndose hasta un máximo de 3 para proceder al bloqueo del usuario inutilizando su conexión. Estos intentos infructuosos deberán ser registrados como eventos de seguridad.

6.3.14 El usuario debe desconectarse al terminar su sesión. Siempre que la tecnología lo permita, el sistema deberá controlar los terminales inactivos de forma que proceda la desconexión automática luego de 30 minutos de permanecer en inactividad.

6.3.15 Evitar usar la misma contraseña en cuentas distintas; por ejemplo, para una aplicación, un correo electrónico y para una cuenta particular de Gmail. Si una de las cuentas es penetrada, el intruso probará la misma contraseña en las otras cuentas.

6.4. Contraseña de acceso a los Servidores (Windows, Linux, etc.)

6.4.1 Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

• Tener como mínimo doce (12) caracteres hasta un máximo de quince (15).

• Tener mezcla de letras mayúsculas y minúsculas, números, caracteres especiales, acrónicos, acrónicos con números, acrónicos como frases.

• No usar nombres, números ni fechas de eventos relacionados con el usuario.

6.4.2 Los usuarios de los servidores deben seguir las buenas prácticas de seguridad de la información en la generación y uso de contraseñas: mantener la confidencialidad de las contraseñas; no mantener registros de las contraseñas en por ejemplo papel, archivo digital con texto plano u otros medios utilizados para recordar la contraseña.

6.4.3 La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de tres (3) meses.

6.4.4 Recién después de utilizar cinco (05) contraseñas diferentes se puede reutilizar una contraseña anterior.

6.4.5 La contraseña de acceso al servidor se bloqueará después de tres (03) intentos de acceso fallido.

6.5. Contraseña de acceso a las Bases de Datos

6.5.1 Toda contraseña generada debe ser de difícil deducción para otras personas y fácil de recordar para el usuario, debiendo cumplir con las siguientes características:

• Tener como mínimo doce (12) caracteres hasta un máximo de quince (15).

• Tener mezcla de letras mayúsculas y minúsculas, números, caracteres especiales, acrónicos, acrónicos con números, acrónicos como frases.

• No usar nombres, números ni fechas de eventos relacionados con el usuario.

6.5.2 Los usuarios de las bases de datos deben seguir las buenas prácticas de seguridad de la información en la generación y uso de contraseñas: mantener la confidencialidad de las contraseñas; no mantener registros de las contraseñas en por ejemplo papel, archivo digital con texto plano u otros medios utilizados para recordar la contraseña.

6.5.3 La contraseña debe ser cambiada periódicamente, pudiendo ser modificada en cualquier momento por el usuario. La vigencia máxima de la contraseña es de tres (3) meses.

6.5.4 Recién después de utilizar cinco (05) contraseñas diferentes se puede reutilizar una contraseña anterior.
6.5.5 La contraseña de acceso a las bases de datos se bloqueará después de tres (03) intentos de acceso fallido.
6.5.6 Solo los administradores tienen acceso directo a las bases de datos; los usuarios solo a través de las aplicaciones.
6.5.7 No se otorgan accesos con privilegio OWNER o ADMIN a usuarios nominales.
6.5.8 Toda solicitud de acceso debe contar con la aprobación del Área de TI y Gerencia, en caso la base de datos sea de producción; del Jefe de Control de Calidad en caso la base de datos sea del ambiente de certificación; o del Jefe de Proyecto en caso la base de datos sea de desarrollo.

6.6. Contraseña de acceso a los equipos de Comunicaciones
6.6.1. Los equipos de comunicaciones forman parte de la red de datos, están ubicados en 2 áreas y contienen los gabinetes que albergan a los equipos de comunicaciones (switch de borde o de piso); por lo que debe implementarse un sistema de control de acceso automático o adoptar los controles pertinentes que permitan mitigar los riesgos inherentes al acceso no autorizado.
6.6.2. Se debe implementar un sistema de control de acceso biométrico que registre los eventos relacionados con la seguridad, para impedir que los equipos de comunicaciones sean manipulados por personal no autorizado.

6.7. Contraseña de acceso al Centro de Datos
6.7.1. El Centro de Datos tiene plataformas y/o sistemas de información donde se procesa y almacene información confidencial, interna o pública; por lo que debe implementarse un sistema de control de acceso automático o adoptar los controles pertinentes que permitan mitigar los riesgos inherentes al acceso no autorizado.

6.7.2. Se debe implementar un sistema de control de acceso biométrico que registre los eventos relacionados con la seguridad, para impedir que las plataformas o sistemas de información.

A7. DIRECTIVA SOBRE EL USO DEL SERVICIO DE INTERNET EN LA UNIVERSIDAD DE CIENCIAS COMERCIALES, CAMPUS LEÓN.

I. OBJETIVO

La presente Directiva tiene por objeto establecer los procedimientos para la administración, control, uso y aspectos de seguridad del servicio de internet en la UCC; así como precisar los riesgos y establecer las pautas en el uso de este servicio por los usuarios.

II. FINALIDAD

Definir los criterios que permitan establecer los niveles de acceso de navegación en Internet de conformidad a las necesidades de las diferentes dependencias la UCC, así como el uso responsable del servicio de Internet habilitado.

III. ALCANCE

La presente Política es de cumplimiento obligatorio para todo el personal de la Universidad, en específica al área de proyectos, indistintamente de su régimen laboral, modalidad de contratación o nivel jerárquico; así como por las personas naturales o jurídicas que prestan servicios o tengan acceso a la información de la Universidad.

IV. BASE LEGAL

4.1. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.

4.2. Ley N° 29139, Ley que modifica la Ley N° 28119, Ley que prohíbe el acceso de menores de edad a páginas Web de contenido pornográfico.

V. DISPOSICIONES GENERALES

5.1. Para mantener los niveles de Seguridad de la Información se requiere el uso controlado del servicio de Internet en la UCC.

5.2. El Área de Tecnología de Información es responsable de garantizar el correcto funcionamiento del servicio de Internet.

5.3. El directorio, la Gerencia y Jefaturas deberán expresar su autorización respecto a los permisos de navegación del personal a su cargo.

5.4. Todo usuario que requiera acceso al servicio de Internet en la UCC deberá solicitar la autorización correspondiente a través de su dependencia.

5.5. Los niveles y accesos de navegación en Internet para los trabajadores en la UCC serán establecidos de acuerdo a las necesidades del uso de la red, evaluados en cada caso particular, de acuerdo a las actividades asignadas a cada usuario.

VI. DISPOSICIONES ESPECÍFICAS

6.1. Autorización de accesos al servicio de Internet

a. Los jefes de área o gerencia deben remitir su autorización para los niveles de acceso de los trabajadores a su cargo mediante correo electrónico.

b. Recibido y evaluado el documento por el Área de Tecnología de Información, el encargado de Informática procederá a configurar los perfiles de usuario de acuerdo a la solicitud del área usuaria y notificará su realización.

6.2. Modificación de accesos al servicio de Internet

a. Cuando se requiera modificar (incrementar, disminuir) los accesos del servicio de navegación de Internet, los jefes de área deberán remitir su autorización mediante correo electrónico, dirigido a TIC.

b. Recibido y evaluado el documento por el Área de Tecnología de Información, el encargado de TI procederá a configurar los perfiles de usuario de acuerdo a la solicitud del área y notificará su realización.

6.3. Eliminación de accesos al servicio de Internet

a. La eliminación de accesos es inherente a la inhabilitación de la cuenta de usuario; sin embargo, cuando una Jefatura requiera la eliminación de accesos a Internet de un usuario sin implicancias de la cuenta de usuario, deberá remitir su solicitud mediante correo electrónico, dirigido a TIC.

b. Recibido y evaluado el encargado de Seguridad Informática procederá a configurar los perfiles de usuario de acuerdo a la solicitud del área usuaria y notificará su realización.

6.4. Deberes de los usuarios del servicio de Internet

a. Cerrar las sesiones de navegación y acceso web una vez finalizado su uso.

b. Respetar la privacidad de otros usuarios.

c. Cualquier acceso no autorizado deberá ser comunicado al Área de Tecnología de Información.

c. Respetar la confidencialidad de cierta información a la que pueda acceder, ya sea como parte de sus labores o por accidente.

6.5. Buen uso del servicio de Internet

a. Comunicación entre trabajadores internos y usuarios externos para cubrir las necesidades específicas de la Institución.

b. Soporte técnico para temas de tecnología de información.

c. Revisión de sitios Web de proveedores y empresas allegadas al Sector para obtener información de los productos, obtener referencia sobre marcos legales, información técnica y recursos.

d. Obtener información financiera, técnica, de actualidad, etc. relevante a las necesidades específicas de la UCC

e. Comunicación con otras empresas, socios estratégicos, etc.

f. El uso de Internet con fines de investigación y desarrollo personal, tales como capacitaciones, desarrollo de tesis, elaboración de monografías, entre otros; relativos a

estudios de capacitación y/o especialización, estará permitido únicamente fuera de horarios de oficina y bajo el conocimiento del jefe inmediato superior.

6.6. Prohibiciones en el uso del servicio de Internet

a. Acceder y utilizar el servicio de Internet sin las autorizaciones correspondientes, según lo descrito en el numeral 1 del acápite VI. Disposiciones Específicas.

b. Utilizar el acceso para cualquier propósito comercial o financiero de carácter personal.

c. Proporcionar información personal al hacer uso del servicio de Internet.

d. Ingresar a cuentas de usuarios que no sean las propias.

e. Afectar o paralizar algún servicio ofrecido por Internet originado en el mal uso de la red.

f. Facilitar u ofrecer a terceras personas, el acceso a internet que se le haya autorizado.

g. Acceder a los sitios de Internet no autorizados señalados en el Anexo 3 de la presente Directiva.

h. Utilizar los servicios de Internet para otros fines distintos a los de interés de la UCC.

i. Participar en cualquier actividad ilegal o criminal a través de un sitio Web.

j. Utilizar el servicio para copiar o extraer información, cuyo contenido pueda causar demandas legales a la UCC o dañar su imagen.

k. Utilizar el servicio para intentar el acceso a sistemas no autorizados de la UCC. Y/o de otras empresas o estados.

l. Utilizar el servicio para interrumpir, denegar, obstruir o interferir en las actividades de otra institución pública o privada.

m. Utilizar programas de mensajería en línea, salvo por orden expresa del Jefe inmediato.

n. Utilizar programas de búsqueda y descarga de archivos que generen tráfico en las comunicaciones de Internet y que sean ajenos a la labor del usuario.

o. Descargar o instalar cualquier tipo de software proxy u otros que intente saltar el firewall y sus restricciones.
p. Instalar software de servidor de páginas web. Los únicos servidores web autorizados se encuentran en el Data Center.
q. Descargar cualquier tipo de software en general.
r. Acceder o intentar acceder a Internet utilizando otras configuraciones de Proxy, DNS, puertas de enlace y otras; sin autorización del Administrador de Red.

s. Utilizar las herramientas de mensajería instantánea o Chat (p. e. Messenger, Yahoo! Messenger, AOL, WhatsApp, entre otros), redes sociales, videos en línea y correos electrónicos gratuitos, compras en línea, aplicaciones de escritorio remoto; salvo que exista la justificación de accesos mediante solicitud formal del Jefe inmediato superior a Gerencia. Solo está permitido el uso de las herramientas adquiridas por la UCC.
t. La habitualidad de visita a estos sitios no aceptables, constituye una infracción ética por parte de los empleados de la UCC.
u. Navegar o acceder a servicios de Internet desde los servidores, para bajar un parche, actualización de firmware o conectarse a un servicio técnico remoto; salvo que sea estrictamente necesario.

v.Acceder a sitios Web de “hacking” o sitios catalogados como inseguros que ponen en riesgo la integridad y/o confidencialidad de la información de la UCC.
w. Acceder a sitios Web con contenido racista o discriminatorio.
x. Descargar desde la Internet cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad intelectual, o archivos electrónicos para usos de no interés con la actividad de la UCC. Si por motivos laborales se requiere descargar algún aplicativo o archivo de gran volumen, debe coordinar con la respectiva autorización de TIC.

y. Publicar información de terceros en portales personales u otros, sin la autorización correspondiente del propietario de dicha información.

z. Publicar comentarios que no se encuentren en el ámbito de sus funciones o servicios en foros públicos, sitios de Chat, blog, correo electrónico o cualquier medio de publicación en Internet.

aa. Instalar y usar programas tipo “peer to peer” para el intercambio de archivos de Internet.

ab. Efectuar llamadas telefónicas usando algún software para este propósito. Solo está permitido el uso de herramientas adquiridas por la Universidad.

6.7. Restricciones al acceso a Intranet

Para las restricciones del acceso a Internet, TIC deberá tomar en cuenta las siguientes categorías:

a. Por defecto: Páginas que pueden ocasionar un riesgo de alto impacto en el servicio de Internet y a los sistemas informáticos de la UCC (p. e. páginas que podrían causar problemas legales, de imagen y económicos, páginas que ocupen un elevado ancho de banda y que podría ocasionar una interrupción o la caída del servicio).

b. Por seguridad: Páginas que pueden ocasionar un riesgo de mediano impacto en el servicio de Internet y a los sistemas informáticos de la UCC, tales como: compras, entretenimiento, redes sociales (p. e. YouTube, Facebook, Twitter, entre otros).

c. A solicitud: Páginas restringidas a recomendación del Comité de Seguridad de la Información de la UCC.

d. Páginas permitidas: Páginas Web de empresas públicas, bancos, proveedores y en general sitios con información necesaria para satisfacer las necesidades de las labores diarias, así como los servicios prestados por los usuarios que no impliquen riesgo en el servicio de Internet y a los sistemas informáticos de la UCC.

e. Páginas no permitidas: Las páginas no permitidas se indican en el Anexo 3: Cuadro de Perfiles de Navegación no Autorizados.

6.8. Uso del servicio de Internet

a. Los usuarios que utilizan el servicio de Internet deben tener precauciones con las páginas que ofrecen servicios gratuitos a cambio de una inscripción donde se utiliza un conjunto de datos. Se debe tener precaución con la información que se suministra. No debe suministrarse información de la UCC ni de su infraestructura tecnológica ni de sus comunicaciones.

b. El Área de Tecnología de Información implementará mecanismos de seguridad, como filtros de contenido, Proxy y Firewall que disminuyan la posibilidad de acceder a las redes de la UCC a personas no autorizadas. Como principio general se debe utilizar "todos los servicios que se encuentran deshabilitados a excepción de los que se encuentran explícitamente aprobados".

c. Sólo se podrá hacer uso de los servicios de Internet (navegación, correo y otros) a través del canal de comunicación provisto por la UCC. No se podrá efectuar conexiones a Internet vía modem o medios alternativos a no ser que se cuente con la autorización formal por parte de TIC.

d. Cuando por propósitos justificados para el desarrollo de las responsabilidades de un empleado de la UCC sea necesario obtener software desde Internet, éste será canalizado a través TIC. Las faltas al respecto serán monitoreadas e informadas jefe inmediato.

e. Se debe controlar la introducción de virus en forma intencional o accidental a través de archivos obtenidos de Internet.

f. En caso que algún usuario requiera tener acceso a un servicio no autorizado, por las tareas que tiene asignadas, el encargado de TI deberá evaluar la posibilidad de incorporar mecanismos que permitan asegurar la confidencialidad e integridad de la información transferida por ese medio y activar el servicio de darse el caso, previa autorización de Gerencia.

g. El uso de las herramientas de navegación y el acceso a Internet debe orientarse a cubrir las necesidades específicas de la UCC.

h. UCC se reserva el derecho de monitorear o hacer el seguimiento de la navegación Web que realicen los usuarios del servicio de Internet, pudiendo tomar medidas correctivas en caso de incumplimiento de la presente Directiva.

6.9. Uso del servicio de Intranet

a. El servicio de Intranet es una herramienta de uso interno de la UCC, mediante la cual se facilita la comunicación e interrelación entre el personal, permitiendo la distribución masiva, acceso oportuno y en tiempo real la información de interés general y de carácter interno.

b. La Oficina de Personal es el órgano encargado de autorizar la publicación y de verificar la actualización de la información en el servicio de Intranet.

c. La Oficina de Tecnología de Información es el órgano encargado de brindar el soporte y asistencia técnica para el funcionamiento del servicio de Intranet.

6.10. Uso del servicio del Portal Web

a. El Portal Web muestra, a nivel nacional e internacional -utilizando las facilidades de Internet- las acciones, proyectos, logros y servicios de la UCC.

b. El área de publicidad es la responsable de la elaboración del Portal Web de la UCC. y su contenido, el mismo que está en función de la información proporcionada por las diferentes dependencias y por las disposiciones de la Alta Dirección.

c. El mantenimiento y desarrollo del Portal Web de la UCC. será realizado por el Administrador Web (Web Master) o por quien haga sus veces, el cual será designado por el Gerente de la Universidad.

6.11. Auditoria y revisión del uso correcto de los servicios de Internet

a. El encargado de Soporte Técnico (Help Desk), se reserva el derecho de realizar revisiones de los registros de auditoría de conexiones a Internet, directorios de archivos personales y cualquier otra información almacenada sobre las estaciones de trabajo de la UCC, en cualquier momento y sin previo aviso, con el objeto de asegurar el cumplimiento de las políticas internas.

b. El Administrador de Red, preparará mensualmente un informa en base a la revisión, análisis y rarefacción ante incidentes reportados por el filtro de contenido, Firewall, Proxy Server u otra herramienta de seguridad de Internet; cuando se vislumbra un accionar u navegación irregular a fin de comunicarse a la Jefatura de la Oficina de Tecnología de Información.

c. El Administrador de Red deberá incorporar en sus actividades la revisión selectiva de los reportes de incidentes de acceso o uso inadecuado de Internet.

VII. DISPOSICIONES COMPLEMENTARIAS

7.1. La gerencia y Oficinas deberán difundir e incentivar una cultura de responsabilidad en la navegación por Internet entre todos los trabajadores de la UCC. referidos a la prevención y el correcto uso.

7.2. El área de Tecnología de Información, deberá aplicar las regulaciones sobre seguridad en la navegación por Internet como: filtros de contenido y advertencias sobre páginas de dudosa reputación.

7.3. La Oficina de Tecnología de Información, podrá suspender o inhabilitar definitivamente la cuenta, de comprobarse la difusión del contenido inadecuado y/o la afectación o paralización de algún servicio ofrecido por Internet originado en su mal uso.

7.4. Es recomendable que los usuarios lean las políticas de privacidad de las páginas Web que visite, las que informan a los usuarios sobre la confidencialidad de su información y como esta se comparte.

VIII. RESPONSABILIDADES

8.1. Las Oficinas de la UCC son responsables de velar por el cumplimiento de las disposiciones de la presente Directiva.

8.2. El incumplimiento de las disposiciones emitidas en la presente Directiva genera responsabilidad administrativa y de ameritar sanción alguna, ésta se establecerá

conforme a la normatividad que corresponda, sin prejuicio de las responsabilidades civiles y penales a que hubiera lugar.

8.3. La Oficina de Tecnología de Información es responsable de:

a. La supervisión del cumplimiento de la presente Directiva.

b. Establecer los lineamientos y directrices complementarias sobre el uso y acceso a Internet en concordancia con la normatividad vigente.

c. Brindar soporte a los usuarios sobre el correcto uso del servicio de Internet.

d. Administrar el servicio de Internet.

e. Controlar el otorgamiento de accesos de navegación en Internet.

8.4. El Equipo de Seguridad Informática es responsable de:

a. Brindar los accesos en función de las necesidades y niveles de acceso autorizados.

b. Suspender o cancelar los accesos de detectarse el uso inapropiado del servicio.

c. Mantener actualizada la bitácora de registro de accesos.

d. Facilitar información sobre el uso y consumo de Internet a solicitud de las áreas interesadas.

8.5. Los usuarios del servicio de Internet son responsables de:

a. Solicitar el acceso de uso de Internet según el desarrollo de las actividades en función del cargo que desempeña.

b. Hacer un uso adecuado del nivel de acceso autorizado.

CAPITULO V. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN.

5.1 Conclusiones

1. Se realizó un análisis de cumplimiento de los controles de la ISO/IEC 27001 para determinar la situación actual de la seguridad de la información en la Universidad de Ciencias Comerciales, campus León, encontrándose que existen incumplimientos significativos con respecto a la norma de referencia, sobre todo en los dominios de Organización de la seguridad de la información, Gestión de activos, Seguridad física y ambienta, Gestión de las comunicaciones y las operaciones, Gestión de incidentes de seguridad de la información y Cumplimiento.

2. Aplicando una lista de cotejo se pudo determinar que el nivel de cumplimiento de los controles que se implementan en la Institución respecto a los establecidos en la Norma ISO/IEC 27001 es del 44.3 %.

3. Se definieron las políticas de seguridad de la información, para cada uno de los siguientes dominios de la seguridad de la información: (1) Gestión de activos de información, (2) Seguridad física y del entorno, (3) Gestión de comunicaciones y operaciones, (4) Control de acceso, (5) Adquisición, desarrollo y mantenimiento de sistemas y (6) Cumplimiento.

5.2 Futuras Líneas de Investigación

Para dar continuidad a la presente investigación, se podría seguir desarrollando el tema:

-Realizando un análisis sobre los riesgos a los que se encuentra expuesta la información y el impacto que esto generaría en la institución al materializarse estos riesgos o amenazas.

-Puesto que esta investigación solo abarca el diagnóstico y la propuesta de algunas políticas, se podría continuar con la implementación del Sistema de Seguridad de la Información en un futuro estudio o investigación.

-Se puede expandir el alcance del estudio hacia las demás sedes de la Universidad de Ciencias Comerciales, dado que esta investigación fue realizada tomando en cuenta únicamente el campus León.

CAPITULO VI. RECOMENDACIONES.

1. Se recomienda que la Dirección de TIC (Tecnología de la Información y Comunicaciones) con apoyo de la coordinación de ciberseguridad revise de manera periódica el cumplimiento de la política de seguridad de la información por parte de todos los colaboradores de la Institución.

2. Se recomienda invertir en herramientas tecnológicas que contribuyan al fortalecimiento de la seguridad de la información en la Institución.

3. La coordinación de Ciberseguridad debe capacitar al personal administrativo, docentes y estudiantes para dar a conocer la importancia del uso de buenas prácticas en el manejo de la información.

4. Se recomienda que la coordinación de Ciberseguridad brinde acompañamiento al personal administrativo, docentes y estudiantes sobre la buena gestión de la información y de esta manera mitigar los peligros internos a los que pueda estar expuesta la información.

REFERENCIAS BIBLIOGRÁFICAS

Bertrán, J., & Francisco, F. (2014). Implementación del modelo de gestión de la seguridad de la información aplicando ISO 27000 en la empresa Coka Tours, Ambato - Ecuador.

- Mata, L. (2017). *"El enfoque cuantitativo de investigación"*. Obtenido de https://investigaliacr.com/investigacion/el-enfoque-cuantitativo-de-investigacion/?msclkid=9ac683aea56e11ec85b2ce53b6bd11f7
- Montaño Orrego, V. (2011). La gestión en la seguridad de la información. *Revista Pensamiento Americano*.
- Ochoa Arévalos, P. A. (2015). Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio. *Revista Tecnológica ESPOL*.
- Ramos, Y., Urrutia, O., & Bravo, A. (2013). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. *4to Congreso Internacional AmITIC 2017, Aplicando nuevas tecnologías*.
- Rodríguez, J. (2016). Diseño y creación de una política de seguridad de la información (SGSI) basado en la normativa ISO 27000 para la cooperativa construcción, comercio y producción.
- Sangoluisa, D. (2015). Definición de las políticas de seguridad de la información para la red convergente de la Presidencia de la República del Ecuador basado en las normas ISO 27000.
- Valencia-Duque, F. J. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Iberica de Sistemas y Tecnología de la Información*.

ANEXOS

Anexo 1-Entrevistas

1.1 Entrevista a Director de TIC.

Estimado MBa. Ulises Rivera, director de TIC de la Universidad de Ciencias Comerciales. Solicito su colaboración para contestar las siguientes preguntas. Las respuestas a las mismas serán utilizadas únicamente para fines investigativos. Muchas gracias de antemano.

1. ¿Considera usted importante que en la institución exista un conjunto de políticas para la seguridad de la información? ¿por qué?

2. ¿Se ha elaborado un inventario de los activos informáticos y recursos para el tratamiento de la información? ¿estos tienen definido un propietario o responsable que se haga cargo de su uso?

3. ¿Qué procedimiento formal de registro y retirada de usuarios se implementa en la institución, para el control de acceso a la red y sistemas informáticos con la asignación de roles y permisos claramente definidos? Ejemplifique.

4. ¿Qué procedimiento sobre el inicio de sesión a los sistemas informáticos se implementa actualmente en la institución y cómo se gestiona el uso, la protección y la duración de las contraseñas?

5. ¿Qué medidas se implementan para proteger el sistema de cableado estructurado de interferencias o daños?

6. ¿Se realiza mantenimiento preventivo y correctivo a los equipos informáticos? ¿Con qué frecuencia?

7. ¿Qué controles de detección, prevención y recuperación se implementan para la protección contra malware? ¿y qué procedimiento se aplican para la concienciación a los empleados o usuarios de los equipos informáticos respecto a dichos códigos maliciosos?
8. ¿Se realizan copias de seguridad o respaldos de información de los sistemas? ¿Con qué frecuencia se realizan dichos respaldos?

9. ¿Existe un plan de contingencia para dar respuesta a incidentes relacionados con la seguridad de la información?

10. ¿Qué medidas de seguridad de la red se implementan en la institución? Explique.

1.2 Entrevista a Coordinadora de Registro Académico.

Estimada Lic. Grethel Hernández, Coordinadora de Registro Académico, de la Universidad de Ciencias Comerciales, campus León. Solicito su colaboración para contestar las siguientes preguntas. Las respuestas a las mismas serán utilizadas únicamente para fines investigativos. Muchas gracias de antemano.

1. ¿Ha escuchado anteriormente el termino Sistema de Gestión de Seguridad de la información (SGSI)?

2. ¿Qué políticas de seguridad de la información se implementan actualmente en la coordinación de registro académico?

3. ¿De qué manera está clasificada la información en registro académico?? Explique

4. ¿Quiénes tiene acceso a la información de registro académico?

5. ¿Qué medidas se implementan durante el traslado de la información fuera de los límites físicos de la institución?

6. ¿Qué controles de entrada se implementan para proteger las áreas que contienen información sensible?

7. ¿Qué procedimiento implementa para identificar sus activos de información?

8. ¿Qué medidas se implementan para la protección de la información física ante desastres naturales?

9. ¿Se les brinda mantenimiento correctivo y preventivo a los equipos informáticos (actualización de antivirus)? ¿Con qué frecuencia?

10. ¿Qué controles de acceso a los sistemas de información se aplican en la coordinación de registro académico? ¿Se utiliza la misma contraseña para todos los sistemas

Anexo 2-Cronograma de Actividades

5.1 Cronograma de Actividades de Investigación

Tabla 6. *Cronograma de Actividades*

Actividades de Protocolo	15	30	15	30	15	15	30	15	28	15	30	15	30
	Octubre		Noviembre		Diciembre	Enero		Febrero		Marzo		Abril	Mayo
Validación del tema													
Capítulo I. Planteamiento de la Investigación													
Antecedentes, Justificación, Objetivos, Planteamiento del problema, supuestos o hipótesis, limitaciones													
Capítulo II. Marco Referencial													
Estado del arte/Fundamentos del Marco Referencial													
Capítulo III. Diseño Metodológico													
Tipo de investigación Área de estudio, Unidades de análisis													
Diseño de instrumentos de recolección de datos													
Confiabilidad y validez de instrumentos													
Operacionalización de variables													
Herramientas para el diseño de instrumentos, recolección de datos, procesamiento y análisis de la información													
Entrega de protocolo													
Entrega de Informe Final													

Fuente: Elaboración propia.

Anexo 3-Presupuesto

5.2 Presupuesto

Tabla 7. *Presupuesto*

PRESUPUESTO					
N°	**DESCRIPCIÓN**	**COSTO UNITARIO**	**UNIDAD**	**CANTIDAD**	**COSTO TOTAL**
1	Impresión de documento	350.00	UND	1	350.00
2	Copias	350.00	UND	2	700.00
3	Impresiones y copias para aplicar instrumentos.	150.00	UND	1	150.00
4	Viático transporte	250.00	Viajes	2	500.00
5	Viático alimentación	100.00	días	2	200.00
	TOTAL				**1,900**

Fuente: Elaboración propia.

UNIVERSIDAD DE CIENCIAS COMERCIALES
UCC - CAMPUS LEON.

UCC

COORDINACIÓN DE ARQUITECTURA, DISEÑO GRAFICO Y PUBLICITARIO E INGENIERIA DE SISTEMAS

Relación de Autores

Elaborado por:

MSc. Ing. Martha Elizabeth Aguinaga Mora – Docente

Revisado por:

MSc. Constantino Portocarrero – Coordinador de Investigación

Autorizado por:

Dra. Fabiola Somarriba – Vice Rectoría Académica