	UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA			
Universidad Francisco de Paula Santander Ocaña - Colombia	Documento: FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO	Código: F-AC-DBL-007	Fecha: 10-04-2012	Revisión: A
	Dependencia: DIVISIÓN DE BIBLIOTECA	Aprobado: SUBDIRECTOR ACADEMICO		Pág.: 1(1)

RESUMEN – TRABAJO DE GRADO

AUTORES	**LAURA MARCELA FELIZZOLA CONDE; ANDREA JOHANA NAVARRO CLARO; DIDIER FERNANDO GUERRERO SUMALAVE; ROGER OSWALDO LIZCANO RUIZ**
FACULTAD	**DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**EDWIN BARRIENTOS AVENDAÑO**
TITULO DE LA TESIS	**SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION SGSI BASADO EN EL ESTANDAR ISO 27001, EN LA UPC SECCIONAL AGUACHICA**

RESUMEN
(70 palabras aproximadamente)

MEDIANTE UNA AUDITORIA INTERNA SE VISUALIZA QUE NO EXISTE UN SISTEMA EN LA UPC AGUACHICA BASADO EN EL ESTÁNDAR ISO27001. EN ESTE PROYECTO SE REALIZA EL ANÁLISIS DE LA SITUACIÓN ACTUAL DETERMINANDO ELEMENTOS DE LA NORMA APLICABLES A LA INSTITUCIÓN, ESTABLECIENDO UN SISTEMA DE GESTIÓN Y MOSTRANDO LOS HALLAZGOS ENCONTRADOS, APLICABLES A LA INSTITUCIÓN (MINTIC 2016), ROLES Y RESPONSABILIDADES.

LOS PROCESOS PLANTEADOS PRETENDEN MINIMIZAR RIESGOS, PROTEGER ACTIVOS Y ESTABLECER PROCESOS.

CARACTERISTICAS

PAGINAS: 149	PLANOS:	ILUSTRACIONES: 5	CD-ROM: 1

Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, seccional Aguachica.

Didier Fernando Guerrero Sumalave

Andrea Johana Navarro Claro &

Roger Oswaldo Lizcano Ruiz

Laura Marcela Felizzola Conde.

Universidad Francisco de Paula Santander

Facultad de Ingenierías.

Especialización en Auditoria de Sistemas

Ocaña

2019

Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, seccional Aguachica.

Didier Fernando Guerrero Sumalave

Andrea Johana Navarro Claro &

Roger Oswaldo Lizcano Ruiz

Laura Marcela Felizzola Conde.

Proyecto de grado final presentado como requisito para optar el título de Especialista en Auditoria de Sistemas

Director

Mag. Edwin Barrientos Avendaño

Magister en Sistemas y Computación

Universidad Francisco de Paula Santander

Facultad de Ingenierías.

Especialización en Auditoria de Sistemas

Ocaña

2019

Contenido

Pág.

Lista de tablas

Pág.

Lista de figuras

Pág.

Lista de apéndices

Pág.

Introducción

La seguridad de la Información es un factor primordial en todos los ámbitos en una organización de tal manera que el siguiente trabajo de grado de la Especialización en Auditoria de Sistemas, lo iniciamos con un análisis de temas relacionados al estudio y conocimiento de la Norma ISO 27001, para asegurar la protección de los activos de información y otorgar confianza a las personas que hacen parte de la Universidad Popular del Cesar Seccional Aguachica tanto internas como externas, está norma adopta un enfoque por procesos para constituir, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI; esto a su vez, directa y estrechamente relacionado con las necesidades de la institución en el área de sistemas, de comunicaciones y tecnologías de la información. Por otra parte nos fundamentamos que este proyecto estuviese enmarcado en los más altos y actuales niveles y avances de la ciencia y la tecnología.

En diversas organizaciones la seguridad de la información es un tema al que no se le da la importancia que se requiere y más bien es tratada solo como un problema tecnológico, sin tomar en cuenta que la seguridad de la información es un problema organizativo y de gestión, lo que lleva a que dichas empresas no sean capaces de afrontar ataques provenientes de todos los ángulos. Ante estos escenarios, las empresas deben establecer estrategias y controles adecuados que garanticen una gestión segura y confiable en los procesos de cada dependencia, primando la protección de la información.

No es suficiente contar con tecnología sofisticada, la gestión implica conocer la situación de lo que se quiere tratar y tener claro hacia dónde se quiere llegar ir, con ello queremos decir, que hay que determinar un objetivo y tomar las acciones necesarias para conseguirlo. La tesis implica un modelo para la gestión de la seguridad de la organización con el fin de que se involucre a toda la organización y no solo al área encargada de implantar el modelo que para este caso sería la Oficina de T.I., lo cual traerá como resultado el éxito del proyecto tanto en su implantación como en su mantenimiento, para ello se debe fomentar el cambio cultural para concientizar a todas las personas que hacen parte de esta, acerca de la importancia y relevancia de la seguridad de los sistemas de información.

1. Título

Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, seccional Aguachica.

1.1 Planteamiento del problema

La Universidad Popular del Cesar es una institución de educación superior, se encuentra establecida en la ciudad de Aguachica como seccional desde 1996 para apoyar la extensión de la sede principal ubicada en la ciudad de Valledupar, con un tiempo de más de 20 años brindando la posibilidad a la comunidad de todo el Sur del Cesar y Sur de Bolívar de acceder a diferentes programas de pregrado como Administración de Empresas, Contaduría Pública, Economía, Ingeniería Agroindustrial, Ingeniería Ambiental y Sanitaria, Ingeniería de Sistemas y Tecnología Agropecuaria todo esto con altos estándares de calidad en sus procesos académicos y administrativos.

Hoy en día, la seguridad en las instituciones de educación superior y en las diferentes organizaciones no se limita solo a proteger activos como el dinero, los bienes y personas, también se debe optimizar la importancia de proteger uno de sus activos más valiosos, la información, la cual se convierte en el bien más preciado para todos los integrantes que directamente o

indirectamente contribuyen con el cumplimiento de los objetivos organizacionales propuestos en sus metas empresariales.

La Universidad Popular del Cesar, Seccional Aguachica, experimenta en los últimos periodos un incremento sustancial de estudiantes, durante los últimos 5 años se puede evidenciar el alto número de estudiantes matriculados como se observa en la siguiente tabla.

Tabla 1.
Estudiantes matriculados por periodos desde 2012 hasta el 2017

Periodo	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**
1	964	784	667	952	1130	1499
2	867	790	644	908	1140	1589

Información brindada por la oficina de registro y control de la Universidad Popular del Cesar, Seccional Aguachica.

Dentro de la Universidad Popular del Cesar, Seccional Aguachica el problema radica en que no se cuenta con una oficina de sistemas consolidada y organizada que brinde un soporte tecnológico con los estándares actuales y vigentes, ya que se trabaja de manera aislada y recursos como el servicio de internet, cableado estructurado, recursos de computo, servidores, no cuentan con políticas de seguridad establecida, los usuarios no cuentan con normas en el uso de los equipos de cómputo, realización de Backups, cambios periódicos de contraseñas de acceso a los sistemas de gestión y procesos, políticas de protección a la seguridad de la información, lo que compromete en gran parte grandes riesgos de confidencialidad, integridad, disponibilidad, autenticidad y no repudio en la ejecución de las tareas entre usuarios y sistemas informáticos.

Los procesos llevados a cabo dentro de cada uno de los estamentos de la Universidad no se encuentran enmarcados en un estándar específico que satisfaga las necesidades presentes en la institución de educación superior, lo que ocasiona que la Universidad y los sistemas de información sean susceptibles a una serie de amenazas que pueden someter los activos críticos de información a diversas formas de fraude, sabotaje, delitos informáticos o destrucción de la plataforma tecnológica, convirtiéndose en un riesgo potencial para este activo indispensable y para el óptimo desempeño de la institución, oficinas como registro y control, admisiones, financiera, biblioteca y sistemas informáticos como ACADEMUSOFT, MGA, SIIBUPC, se convierten en un blanco al presentar altos índices de vulnerabilidades al mantener un flujo importante de información de alta importancia.

1.2 Formulación del problema

¿El diseño de un sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, le proveerá a la Universidad Popular del Cesar Seccional Aguachica los elementos y mecanismos adecuados para mejorar la seguridad de la información de la institución y la gestión de los riesgos que se asocian al tratamiento y uso de la misma?

1.3 Objetivos

1.3.1 Objetivo general

Diseñar el sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, Seccional Aguachica.

1.3.2 Objetivos específicos:

1. Diagnosticar el estado de la seguridad de la información en la Universidad Popular del Cesar, Seccional Aguachica, para conocer sus amenazas, vulnerabilidades e impactos.
2. Determinar los elementos del estándar ISO 27001, que puedan ser aplicados en la Universidad Popular del Cesar, Seccional Aguachica.
3. Establecer el sistema de gestión de la seguridad de la información (SGSI) para la Universidad Popular del Cesar, Seccional Aguachica.
4. Realizar una prueba piloto utilizando las políticas del sistema de gestión de la seguridad de la información (SGSI) en la oficina de Tecnologías de la Información.

1.4 Justificación

La información es considerada por muchas organizaciones e instituciones el activo más importante, por lo cual es imprescindible protegerla de la mejor forma con ayuda de estrategias y controles, de tal forma que las amenazas a las que pueda estar expuesta no pongan en peligro los

objetivos misionales y la continuidad de proceso, en la Universidad Popular del Cesar Seccional Aguachica se hace necesario contar con un SGSI que mejore la manipulación, protección y permita disminuir y mitigar los riesgos y amenazas en sus sistemas de información y en los demás procesos que involucre la gestión de datos importantes para la institución.

> "Un Sistema de Gestión de Seguridad de la Información, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, revisar, mantener y mejorar la seguridad de la información" (Ana Andrés Luis Gómez, 2009, p 13).

La Seccional Aguachica, ha venido presentando un crecimiento durante los últimos 10 años lo que permite asegurar una proyección con altos índices de desarrollo para los años venideros, todo esto basado en aspectos tan importantes como lo son la infraestructura física, el mejoramiento en el ámbito tecnológico y la cantidad de estudiantes admitidos para los últimos periodos académicos, oficinas como Registro y control y Almacén e Inventario muestran en cifran contundentes.

Teniendo en cuenta lo anterior, se hace necesario realizar el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para la Universidad Popular del Cesar, Seccional Aguachica, que se basará en el estándar ISO 27001 enmarcada en una política de seguridad de la información para identificar, analizar y evaluar riesgos potenciales a los que está expuesta, tales como pérdida total o parcial de los datos, alteración de dichos datos, sabotaje a los sistemas de información que

actualmente posee la institución y que de gran manera contribuyen al desarrollo óptimo de los procesos académicos y administrativos que complementan los valores institucionales y misionales.

Los incidentes de seguridad siempre van a existir sin importar los controles que implementen las organizaciones. Sin embargo, se podrá conocer y tener claro cuáles son los incidentes más comunes que se presentan, lo que permitirá para la alta gerencia orientar las inversiones en seguridad hacia las brechas que mayor impacto pueden generar en caso que un incidente se materialice, todo esto con el objeto de poder detectarlo en el menor tiempo posible y así poder actuar según la criticidad del mismo en su mitigación y control, es aquí donde el SGSI cumple su papel más importante.

La ley 872 del 2003, establece que todas las instituciones y entidades del estado deben adoptar un sistema de gestión de la calidad, que les permita mejorar sus procesos y metodologías basado en el PHVA y con objetivos claros de concientizar el desarrollo y mejora continua, de igual forma el desarrollo de este proyecto permitirá generar a la alta gerencia las herramientas y estrategias para una toma de decisiones adecuada y oportuna en todo lo relacionado con la normatividad de Seguridad de la Información, administración de recursos tecnológicos, tiempos de respuesta y acción, mejora de procesos y procedimientos internos y externos que garanticen un mejor manejo de los datos y su tratamiento.

1.5 Hipótesis

Este estudio permitirá conocer cuáles son los riesgos, vulnerabilidades y amenazas que tiene la Universidad Popular del Cesar Seccional Aguachica en sus sistemas de información, y con la muestra piloto que se realizará en la actividades y procesos del encargado del área de sistemas, se logrará determinar cómo implementar las políticas del Sistema de Seguridad de la información basada en la Norma ISO 27001, lo cual permitirá mejorar la confianza en el manejo de los sistemas de información y comunicación de las diferentes dependencias.

También establecerá el sistema de gestión de la seguridad de la información (SGSI) para la Universidad Popular del Cesar, Seccional Aguachica, para que dentro de la organización sus procesos sean más eficientes y confiables, puesto que se manejan varios sistemas de información relevantes y muy importantes para cumplir los objetivos misionales de la Institución y suplir las necesidades de la comunidad estudiantil, docentes y egresados de la misma.

1.6 Delimitaciones

1.6.1 Delimitación geográfica.

El desarrollo del presente trabajo de grado se llevó a cabo en la ciudad de Aguachica - Cesar, específicamente en la Universidad Popular del Cesar Seccional Aguachica.

Aguachica segunda ciudad del departamento, está ubicada al Sur del departamento del Cesar, a los 8º 18’ 45” de latitud norte y 73º 37´37” de longitud oeste del meridiano de Greenwich, entre la cordillera oriental y el valle del río Magdalena, a una distancia de 301 kilómetro de Valledupar, la capital del Cesar. Su extensión territorial es de 876.26 kilómetros cuadrados que ocupa el 3,8% de la superficie del departamento. Limita por el norte con el municipio de La Gloria (Cesar), El Carmen (Norte Santander), por el este con Río de Oro (Cesar), por el sur con San Martín (Cesar) y Puerto Wilches (Santander), por el oeste con Gamarra (Cesar) y Morales (Bolívar).

El territorio de Aguachica tiene una zona montañosa al norte, representadas por las estribaciones noroccidentales de la cordillera oriental con elevaciones entre los 200 y 2.150 metros sobre el nivel del mar (msnm); al sur una zona de planicie o llanura regada por los ríos Lebrija y Magdalena y sus numerosas quebradas y arroyos hoy disminuidos drásticamente por la deforestación, su fisiografía oscila entre los 50 y los 200 msnm. Presenta un clima con temperatura promedio de 28 ºC. y precipitación media anual de 1.835 mm, con dos periodos de lluvias al año.

1.6.2 Delimitación temporal.

El proyecto tuvo una duración de 3 meses, teniendo en cuenta las actividades realizadas el cronograma de actividades en las tres fases del proyecto.

1.6.3 Delimitación conceptual.

El presente proyecto tuvo como cobertura la Universidad Popular del Cesar Seccional Aguachica, pretendiendo desarrollar un adecuado sistema de gestión de seguridad de la información basado en el estándar ISO 27001, en dicha Institución.

Académicamente, el proyecto se encuentra enmarcado dentro del área de la Ingeniería de Sistemas aplicando conocimientos en las siguientes áreas:

1. Metodología de la investigación
2. Investigación de mercados
3. Estadística
4. Formulación y Evaluación de proyectos
5. Tecnologías de la información
6. Redes y telecomunicaciones

1.6.4 Delimitación operativa.

Este proyecto se desarrolló para el mejoramiento de las siguientes áreas de la Universidad: Registro y Control Académico, Recursos Bibliográficos, Dirección Administrativa y Financiera y Direcciones de Departamento en cuanto a seguridad informática, pues son las dependencias más vulnerables y expuestas a cualquier alteración en los sistemas de información, debido a que los estudiantes, docentes y personal externo tiene acceso a estas.

Una de los factores que pudieron obstruir el buen desarrollo de la presente investigación, fue la falta de tiempo por parte de los investigadores, poca información referente al tema que se investigó, información veraz y confiable por parte de los funcionarios a la hora de realizar la entrevista o encuesta, problemas climáticos (lluvia), entre otros.

2. Marco referencial

2.1 Marco histórico

2.1.1 Antecedentes

Desde la antigüedad, la información ha estado siempre presente. El ser humano ha llevado datos importantes como bienes y propiedades por medio de registros escritos, logrando así mantener de una u otra forma el control de sus pertenencias y tomar decisiones de acuerdo a dicha información para obtener beneficios.

Si se compara lo anterior con el mundo actual aún se mantiene esa idea pero la cantidad de información que se genera en el mundo contemporáneo es extremadamente grande, en donde nace la necesidad de administrar de forma segura y eficiente la información.

A continuación se referencian algunos trabajos de investigación que fueron afines al tema desarrollado; realizando comparativos para analizar similitudes y diferencias existentes r entre las investigaciones llevadas a cabo en diferentes contextos geográficos, a saber:

Internacional: en este ámbito se encontraron diversos trabajos, entre los cuales se referencian los siguientes:

TÍTULO: Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la corporación metropolitana de salud.

AUTOR(ES): Álvarez Zurita Flor María, García Guzmán Pamela Anabel

INSTITUCIÓN: Corporación Metropolitana de la Salud

FECHA: Octubre de 2007

CIUDAD: Quito Ecuador

RESUMEN: en el presente proyecto de titulación se pretende dar una adecuada solución de seguridad a la Corporación Metropolitana de la Salud, tomando como base los estándares internacionales.

El primer capítulo proporciona los lineamientos básicos de la seguridad de la información, una visión general de la gestión de riesgos así como las diferentes alternativas para el tratamiento de los riesgos identificados la evolución de la norma 27001, y finalmente nos da una descripción de la norma ISO 270001:2005, en donde señala la seguridad de la información no se trata sólo de aspectos tecnológicos sino su objetivo es organizar la seguridad de la información. El segundo capítulo se presenta una breve descripción de los 11 dominios del estándar ISO 17799, en el cual se documenta los procesos y procedimientos que ayudan a garantizar la seguridad de la información en la CMS.

En el tercer capítulo se muestra el análisis de la situación actual de la CMS, a partir de este resultado se identifican los activos más importantes para la empresa y se realiza una identificación, análisis y evaluación de vulnerabilidades en la CMS, para posteriormente realizar una selección de controles y objetivos de control de la Norma ISO 1779. (ALVAREZ ZURITA & GARCIA GUZMAN, 2007).

TÍTULO: Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix.

AUTOR: Miguel Leopoldo Villacís Espinosa

INSTITUCIÓN: Universidad Politécnica Salesiana Sede Quito

FECHA: Febrero de 2016

RESUMEN: El presente proyecto de titulación se enmarca en el diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para el centro de datos Ecuatronix Cía. Ltda.

El punto de inicio fue conocer la actualización de la norma ISO/IEC 27001:2013 para tener en cuenta los nuevos objetivos de control y controles a ser implementados, seguidamente de ello se continuó con el reconocimiento del centro de datos de la compañía para definir los activos de la información, y tener claro las amenazas o ataques de los que pueden ser víctimas estos activos,

así como también se realizó un análisis de los riesgos para definir el criterio de mitigación de los mismo. (VILLACIS ESPINOSA, 2016)

Nacional: Haciendo revisión en este tema se encontraron varios proyectos de investigación que son similares al que se está realizando en la presente investigación, por lo cual en este ámbito se escogieron los más relevantes, entre los cuales se referencian los siguientes:

TÍTULO: diseño de políticas de seguridad informática basadas en la norma NTC-ISO-IEC 27001:2013 para la universidad de Cartagena centro tutorial Mompox bolívar.

AUTOR: Manuel Esteban Ureche Ospino

INSTITUCIÓN: Universidad Nacional Abierta y A Distancia UNAD

FECHA: 06 Abril de 2017

RESUMEN: El presente trabajo de grado tiene como propósito diseñar las políticas de seguridad informática para Universidad de Cartagena Centro Tutorial Mompox, Teniendo en cuenta el análisis de riesgos y vulnerabilidades, tomando como referencia la norma NTC-ISO-IEC 27001:2013, es por ello que en este proyecto se platea el diseño de las políticas de seguridad informática. El propósito de este proyecto es proporcionar y garantizar la seguridad de la información de los recursos informáticos de la Universidad de Cartagena Centro Tutorial Mompox.

El proyecto se apoya en estudios realizados a los estudiantes de la Universidad de Cartagena Centro Tutorial Mompox y personal administrativo, donde se desarrollaron varias entrevistas al personal que administra el área de sistemas y recursos informáticos, de acuerdo a la información levantada se tomó una muestra de acuerdo a las necesidades de seguridad, utilizando estadística no probabilística donde se evidencia que no existen políticas de seguridad informática que se apliquen para este centro tutorial. (URECHE OSPINO, 2017)

TÍTULO: Guía de buenas prácticas de seguridad de la información en contextos de micro, pequeñas y medianas empresas de la región.

AUTOR: Gerardo Ayala González, Julián Alberto

INSTITUCIÓN: Universidad Tecnológica de Pereira.

FECHA: 3 febrero de 2011.

RESUMEN: Este documento se centra en la aplicación de la norma ISO/IEC 27001 en atención a los numerales 4.2.2 Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de: la gestión apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que

brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización.

La anterior investigación se fundamenta en establecer un sistema de gestión de seguridad de la información el cual está orientado por el estándar ISO 27001 con el objetivo de establecer políticas de seguridad aplicando controles que permitan cumplir los objetivos de la misma en los cuales se analizaron temas como el análisis de riesgos en los cuales se orientaron bajo la metodología ISO 27005 con las cuales pudieron establecer controles que mitigaran los riesgos inminentes de la organización e implantando el sistema de gestión de seguridad de la información. (AYALA GONZALES & ALBERTO, 2011)

TÍTULO: Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001

AUTOR: Alba Elisa Córdoba Suárez

INSTITUCIÓN: Universidad Nacional Abierta y Distancia "UNAD"

FECHA: Mayo de 2015

RESUMEN: El gobierno nacional dispone mediante leyes y decretos que en las ciudades para el desarrollo urbano sean las curadurías urbanas o la oficina de planeación municipal las encargadas de otorgar licencias urbanísticas en todas sus modalidades. Por lo tanto el Curador

Urbano es un particular con función pública encargado de estudiar, tramitar y expedir licencias urbanísticas a todos los interesados que presenten solicitud de obtención de licencia. Su función es verificar el cumplimiento de las normas urbanísticas y de edificaciones vigentes, con autonomía en el ejercicio de sus funciones y responsable conforme a la ley.

Este proyecto se lleva a cabo para la Curaduría Urbana Segunda de Pasto la cual pretende cada día implementar políticas y controles de seguridad para proteger la información; mejorar la atención a sus usuarios, brindándoles eficiencia y calidad en la prestación de su servicio y asegurar la continuidad del proceso.

Este trabajo tiene como objetivo fundamental, diseñar un SGSI para el área de informática de la Curaduría Urbana Segunda de Pasto bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la empresa, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PHVA (Planificar, hacer, verificar y actuar). (CORDOBA SUAREZ, 2015)

Regional: los investigadores indagamos sobre trabajos que tuvieron alguna relación con el que se está llevando a cabo a nivel regional hallamos un proyecto de investigación con alguna similitud al que estamos realizando:

TÍTULO: Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, Cesar.

AUTOR(ES): Meneses Martínez, Alexander, Ramírez Camargo, Erney Alberto, Merchán Villalba, María Alejandra, Suarez De La Cruz, Yaditza.

INSTITUCIÓN: Universidad Francisco de Paula Santander Ocaña.

FECHA: 6-feb-2017

RESUMEN: El objetivo principal de este proyecto consiste en la elaboración del diseño del sistema de gestión de seguridad de la información para los procesos que son soportados por el área de sistemas de la cámara de comercio de Aguachica, cesar, basado en la norma internacional ISO/IEC 27001: 2013, en donde seguimos el ciclo PHVA, llegando solo a la fase del plan, en donde identificamos los activos, salvaguardas y planteamos las políticas de seguridad pertinentes para la entidad. (MENESES MARTINEZ, RAMIREZ CAMARGO, MERCHAN VILLALBA, & SUAREZ DE LA CRUZ, 2017).

TÍTULO: Evaluación de la seguridad en la información para la terminal de transportes de la ciudad de Ocaña norte de Santander, basados en la norma ISO/IEC 27001

AUTOR: Sanjuán Muñoz, Willigton

INSTITUCIÓN: Universidad Francisco de Paula Santander Ocaña

FECHA: 16-may-2017

RESUMEN: Los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total. (SANJUAN MUÑOZ, 2017).

2.2 Marco conceptual

Este marco se referencia a la serie de términos que al momento de los investigadores iniciar su trabajo desconocían y que en el momento de ir avanzando se encontraron con ellos abriéndose así la estructura mental, ampliándose en los conocimientos y apropiándose con ello de un mayor horizonte conceptual. A continuación se exponen algunos términos importantes y relevantes para la presente investigación:

Acción correctiva: Acción para eliminar la causa de una no conformidad y evitar que vuelva a ocurrir. (ISO 9000, 2015)

Acción preventiva: Acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencial no deseable. (ISO 9000, 2015)

Activo: Cualquier cosa que tiene valor para la organización. (NTC 5411-1:2006)

Alcance: el alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones. (ISO 9000, 2015)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000,2013)

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000,2013)

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta. (ISO/IEC 27000,2013)

CID: Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información. (ISO/IEC 27000,2013)

Evaluación de riesgos: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (Guía ISO/IEC 73:2002)

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (ISO/IEC 27000,2013)

PDCA: El ciclo PHVA permite a una organización asegurarse de que sus procesos cuenten con recursos y se gestionen adecuadamente, y que las oportunidades de mejora se determinen y se actúe en consecuencia. (ISO 9001, 2015)

Política de seguridad: Su objetivo es brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. (ISO 27001, 2013)

Riesgo: Efecto de la incertidumbre. (ISO 9000, 2015)

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. (NTC-ISO/IEC 17799:2006)

SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (ISO 27001, 2013)

Tratamiento de riesgos: proceso de selección e implementación de medidas para modificar el riesgo. (Guía ISO/IEC 73:2002)

2.3 Marco contextual

Este proyecto de investigación se llevó a cabo en todas las dependencias la Universidad Popular del Cesar Seccional Aguachica donde se realizó el diseño del sistema de gestión de seguridad de la información basada en el estándar ISO 27001, tomando como muestra piloto la Oficina de Tecnologías de la Información.

Para conocer un poco de la Universidad Popular del Cesar Seccional Aguachica, se dará a conocer su historia y crecimiento.

2.3.1 Historia aprobación de la seccional Aguachica

La Resolución 1022 del 14 de mayo de 2002 expedida por el Ministerio de Educación Nacional y firmada por el Ministro Francisco Lloreda Mera, no fue fácil su consecución. Desde el mismo momento que iniciamos las actividades académicas en el año de 1996 se hizo un estudio de factibilidad con el objeto de tener el código y la aprobación de Seccional, este estudio de factibilidad fue fundamental para que el Ministerio de Hacienda tomara como referente y adjudicará los recursos que se incorporaron desde 1998. En 1998 la Rectoría en cabeza del Dr. Roberto Daza Suárez logró la aprobación como Seccional, por parte del Consejo Superior Universitario el 27 de diciembre de 1997, en virtud de que la ley 30 de 1992 no definió cuál era el procedimiento lógico para obtener la aprobación de Seccional. Así el Consejo Superior Universitario expidió el Acuerdo N° 033 del 22 de diciembre de 1997 de Creación de Seccional, básico para tramitar ante el ICFES, y a su vez este ante el Ministerio de Educación Nacional el

reconocimiento como Seccional. Desde este momento se inicia entre la Rectoría y la Dirección del ICFES misivas y comunicaciones, sustentando por parte del Consejo Superior Universitario el fundamento legal del trámite para la aprobación de la Universidad en Aguachica. En 1998 se presenta un documento que es clave para la obtención de aprobación de Seccional exigido por la ley 30 de 1992, y es un convenio firmado entre el Ministerio de Hacienda y el ente territorial donde va a funcionar la Universidad y definir los recursos con los cuales funcionará la Seccional. Este convenio logró proyectarse en la Seccional de Aguachica y ser firmado por el Alcalde Municipal Dr. Israel Obregón Ropero, donde definió los recursos por parte del Municipio para la Universidad, igual que iba firmado por el Rector Dr. Roberto Daza Suárez. El convenio debía ser firmado por el Ministro de Hacienda Dr. Juan Camilo Restrepo y el Ministro de Educación Nacional Dr. Germán Bula. No sería recomendable mencionar aquí la incompetencia por una de las instituciones oficiales, como fue el ICFES, quien bajo su responsabilidad el documento original desapareció, sin embargo lo hacemos para dejar en claro que la Universidad hizo ingentes esfuerzos para legalizar su situación. La Universidad logró que el Ministro de Hacienda Dr. Juan Camilo Restrepo firmará el convenio y fuera remitido al Ministerio Educación Nacional para su firma, sin embargo el Ministerio de Educación Nacional lo remitió al ICFES para obtener el concepto respectivo. Sólo en el año 2000 la Universidad a través de una información, no formal, por parte de un funcionario del ICFES se supo que el convenio en mención había desaparecido y por tanto la aprobación de la Seccional estaba en duda.

A partir de este momento la Universidad empieza a demostrar con datos el buen desarrollo del proyecto de la Seccional y se hizo un requerimiento por parte del ICFES, se presenta una última documentación en septiembre de 2001, esta documentación se presentó en 76 documentos, un

número aproximado de 2000 páginas y un peso aproximado de 150 kilos. Bajo la dirección de Bertha Rojas Directora de Programas de Pregrado y posgrado, el ICFES analiza la documentación presentada y en el año 2001 emite concepto ante el Ministerio de Educación Nacional el cual lo considera pertinente a través de la Dirección de Educación Superior quien da el concepto favorable para que en mayo de 2002 se expida la autorización al Consejo Superior Universitario, el funcionamiento de la Universidad Popular del Cesar – Seccional Aguachica, bajo el número de la Resolución 1022 inicialmente citada. Es importante aclarar que cuando se inició la presentación de documentos ante el ICFES, la Dirección de aprobación de programas informalmente comunicó a la Universidad que una vez aprobada la Seccional los programas que hacían parte de la solicitud de aprobación de la Seccional que fueron Administración de Empresas, Contaduría Pública, Ingeniería de Sistemas, Ingeniería Agroindustrial y Enfermería, automáticamente serían aprobadas, sin embargo, una vez aprobada la Seccional con la Resolución 1022 la Universidad ha tenido que presentar nuevos trámites para la aprobación de los programas de Ingenierías y Salud, por cuanto así lo exigen los Decretos de Estándares de Calidad aprobados a partir del año 2001. Igualmente cabe señalar que el objetivo del gobierno central al aprobar el funcionamiento de la Seccional hacen que la administración de la Universidad en el Municipio de Aguachica tenga la administración de manera relativamente autónoma, es decir, que administre los recursos que le aporta la nación y, los recursos propios, de acuerdo a sus necesidades presentadas cada año al Consejo Superior Universitario. Podemos decir que hasta el momento se están logrando los objetivos por la Seccional, sólo falta que el Consejo Superior Universitario expida Acuerdos para que la estructura orgánica y de personal permita la ejecución de sus recursos.

La UPC está ubicada en la carrera 40 vía al mar, Barrio Nueva Colombia en la ciudad de Aguachica – Cesar. (UNIVERSIDAD POPULAR DEL CESAR, 2017)

2.4 Marco teórico

Al aplicar los contenidos teóricos a la investigación, se resaltan las teorías las cuales se han enfocado, a través de los años, para realizar un sistema de gestión de seguridad de la información, que sea apropiado para alcanzar el éxito deseado y se adapte a las necesidades presentes en la organización que desee implantarlo.

2.4.1 ¿Qué es la norma ISO 27001?

La norma ISO 27001 adopta un proceso enfocado para establecer, implantar, funcionar, seguir, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información de la organización.

La ISO 27001 está establecida por la International Organisation for Standardization (ISO) y es la norma utilizada para la certificación. Reemplaza la BS 7799 y provee de una norma internacional del Sistema de Seguridad de la Información. Basada en la BS 7799, ha sido reorganizada para alinearse con otras normas internacionales. Se han incluido algunos nuevos controles, p. ej. El énfasis en la gestión de incidentes de seguridad de la información y principios OECD.

La norma también se perfila bajo otras normas como ISO/IEC 17799:2005, ISO/IEC 13335-1:2004, ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000, ISO/IEC TR 18044:2004 y "Guía OECD para los sistemas de Seguridad de la Información y Redes – Hacia una cultura de seguridad" que facilita consejos para implantar la seguridad de la información.

De acuerdo a otras normas de sistemas de gestión ISO 27001 está alineada con otros sistemas de gestión, y apoya la implementación y funcionamiento estable e integrado con normas de gestión relacionadas.

Características de la ISO 27001

- Armonización con normas de sistemas de gestión como ISO 9001 e ISO 14001.
- Énfasis y continuo proceso de mejora de su sistema de gestión de seguridad de la información.
- Aclaración de requisitos para la documentación y archivos.
- Valoración de riesgos y procesos de gestión utilizando un modelo de proceso Plan, Do, Check, Act –PDCA (Planificar, Realizar, Controlar, Actuar). (DNV-GL, S.F)

2.4.2 Introducción a ISO 27002 (ISO 27002)

La norma ISO 27002 se publicó originalmente como un cambio de nombre de la norma ISO 17799 existente, un código de prácticas para la seguridad de la información. Básicamente esboza

cientos de controles potenciales y mecanismos de control, los cuales pueden ser implementados, en teoría, sujetos a la guía proporcionada dentro de ISO 27001.

La norma "estableció directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización". Los controles reales enumerados en la norma están destinados a abordar los requisitos específicos identificados mediante una evaluación formal de riesgos. La norma también pretende proporcionar una guía para el desarrollo de "normas de seguridad organizativa y prácticas de gestión de la seguridad eficaces y para ayudar a crear confianza en las actividades inter organizacionales". (PORTAL WEB 27000.org, S.F)

La base de la norma era originalmente un documento publicado por el gobierno del Reino Unido, que se convirtió en un estándar 'apropiado' en 1995, cuando fue reeditado por BSI como BS7799. En 2000 se volvió a publicar, esta vez por ISO, como ISO 17799. Una nueva versión de esto apareció en 2005, junto con una nueva publicación, ISO 27001. Estos dos documentos están destinados a ser utilizados en conjunto, con un complemento del otro.

En 2013 se publicó la versión actual. ISO 27002: 2013 contiene 114 controles, en contraposición a los 133 documentados dentro de la versión 2005. Sin embargo, para granularidad adicional, se presentan en catorce secciones, en lugar de los once originales.

Por último, cabe señalar que a lo largo de los años se han desarrollado o están en desarrollo varias versiones específicas de la industria de la ISO 27002 (por ejemplo, sector de la salud, fabricación, etc.).

ISO/IEC 27001:2013.

ISO/IEC 27001:2013 tiene como prioridad proteger

a) La confidencialidad de la información
b) La integridad de la información
c) La Disponibilidad de la información ISO/IEC 27001 se divide en 10 secciones las cuales se describen a continuación:

Sección 0 – Introducción – explica el objetivo de ISO/IEC 27001:2013 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hacen referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información. **Sección 9** – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo

PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Otras normas relacionadas con seguridad de la información: ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO/IEC 27001:2013. ISO/IEC 27001:2013 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799. (GUERRERO MELO & SUAREZ CASTRELLON, 2016)

2.4.3 Diferencia entre la Norma 27002 vs. 27001.

La diferencia está en que la ISO 27002 no distingue entre los controles que son aplicables a una organización determinada y los que no lo son. Por otro lado, la ISO 27001 exige la realización de una evaluación de riesgos sobre cada control para identificar si es necesario disminuir los riesgos y, en caso que sea necesario, hasta qué punto deben aplicarse. (KOSUTIC, S.F)

2.5 Marco legal

Los siguientes documentos mencionados en el presente trabajo de investigación fueron indispensables para la aplicación y desarrollo de este documento.

Continuamente se desea implementar un Sistema de Gestión, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos y afines que sean aplicables en el desarrollo de sus actividades. Pero en lo que se refiere específicamente a seguridad de la información, estas son las Leyes vigentes al día de hoy:

ISO 27001. Esta norma internacional fue publicada el 25 de septiembre del 2013, como evolución de su homóloga liberada en 2005, en la norma se especifican los requisitos para establecer, implementar, mantener y mejorar un Sistema de gestión de la seguridad de la información, en donde se valoran y se realiza un tratamiento de los riesgos los cuales son de tipo general y se pueden aplicar a cualquier tipo de organización.

Los cambios en esta nueva versión estipulan la reducción de 133 controles a solo 114, la creación de 3 nuevos dominios sumados a los 11 anteriores y un total de 130 requisitos de gestión, lo que permite poder realizar el diseño, implantación y mantenimiento de todo el conjunto de procesos que gestionan y protegen los elementos que garantizan las características más importantes de la información (Confidencialidad, Integridad y Disponibilidad).

Ley 23 De 1982 Sobre derechos de autor. Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. (Ley 23 de 1982, 2014).

Ley 44 de 1993. Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal. Ley N° 44 de 1993 (5 de febrero) modifica y adiciona la Ley N° 23 de 1982 y se modifica la Ley N° 29 de 1944. Mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derechos. (INNOVACION UNAL, 2017)

Ley 1273 Del 5 De Enero De 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (CONGRESO DE COLOMBIA, 2009)

El 5 de Enero de 2009 se decretó la Ley 1273 de 2009, la cual añade dos nuevos capítulos al Código Penal Colombiano: Capítulo Primero: De los atentados contra la confidencialidad, la 18 integridad y la disponibilidad de los datos y de los sistemas informáticos; Capítulo Segundo: De los atentados informáticos y otras infracciones.

Esta Ley está muy ligada a la ISO 27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (LEY ESTATUTARIA 1581 DE 2012.).

3. Diseño metodológico

La metodología utilizada para dar cumplimiento a los objetivos específicos definidos para poder alcanzar el objetivo general del proyecto, en el marco de referencia de la norma ISO/IEC 27001:2013, especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para el diseño de un Sistema de Gestión de Seguridad de la Información para la Universidad Popular del Cesar Seccional Aguachica.

Teniendo en cuenta que el objeto del estudio de establecer el Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para la Universidad Popular del Cesar, Secciona Aguachica, se requirió caracterizar el centro del estudio, identificar los objetos que tienen dicha característica, describir el contexto en el cual se desarrolló, cuantificar que tan grande es la problemática, esto permitió buscar el alcance de los objetivos propuestos en el proyecto.

En un primer momento se diagnosticó el estado de la seguridad de la información en la Universidad Popular del Cesar, Seccional Aguachica, realizando una auditoria interna basada en la norma ISO 27001, y fue socializada con los miembros directivos.

Seguidamente se realizó un análisis documental de la normativa y también de los procesos internos de la institución para así poder determinar los elementos del estándar ISO 27001, que pueden ser aplicados.

Una vez identificados los elementos aplicables se seleccionaron aquellos con los que se podría establecer el sistema de gestión de la seguridad de la información (SGSI) y se documentó dentro de esta investigación.

Finalmente utilizando las políticas del sistema de gestión de la seguridad de la información (SGSI) se realizaron actividades en la oficina de Tecnologías de la Información, con el fin de buscar pruebas de aceptación y de aplicación.

3.1 Tipo de investigación

Para el desarrollo se acudió a la investigación Descriptiva porque se buscó especificar las propiedades, características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Describe tendencias de un grupo o población. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas. (HERNANDEZ SAMPIERI, 2010)

Basados en que el fin del estudio es establecer el Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 2007, tomando como muestra piloto la Oficina

de Tecnologías de la Información de la Universidad Popular del Cesar Seccional Aguachica, para lograr este fin se necesitó caracterizar el objeto de estudio, identificar que tiene dicha característica, describir el contexto en el cual se está desarrollando, medir que tan grande es la problemática.

Conjuntamente a la anterior metodología, también se utilizó el CICLO PHVA en la investigación, esta es la metodología es establecida por la Organización Internacional de Estandarización (ISO) para el desarrollo de un sistema de gestión de seguridad de la información, el cual consiste en ciclo PHVA (Planear, Hacer, Verificar y Actuar).

3.6 Población y muestra

Considerando que la población objeto de la investigación, cuantitativamente es reducida, la muestra se estableció a conveniencia con las dependencias donde la manipulación de información muestra mayor volumen y los procesos requieran de un cuidado importante por la importancia de la información manejada, por lo que se determinó una muestra de tres oficinas (Registro y control, Oficina de Financiera, Laboratorios de sistemas) para la realización del proyecto.

3.7 Técnicas de recolección de la información

(Mendez, 1999.) define a las fuentes y técnicas para recolección de la información como los hechos o documentos a los que acude el investigador y que le permiten tener información, también señala que las técnicas son los medios empleados para recolectar información, entre los cuales se usan encuestas, entrevistas no estructuradas, observación directa y listas de chequeos, realizadas

al personal administrativo y los directamente involucrados con los procesos de manejo de información de la Universidad Popular del Cesar Seccional Aguachica. (p.143)

Según (VASQUEZ CASIELLES, TRESPALACIOS GUTIERREZ, & BELLO ACEBRON, 2005) las encuestas son instrumentos de investigación descriptiva que precisan identificar a priori las preguntas a realizar, las personas seleccionadas en una muestra representativa de la población, especificar las respuestas y determinar el método empleado para recoger la información que se vaya obteniendo. (p.35)

Por otra parte la observación directa es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, sin intervención, con el fin de tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación. Observar científicamente significa observar con un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación. (PUENTE, 2009).

4. Resultados

4.1 Diagnóstico del estado de la seguridad de la información en la universidad popular del cesar, seccional Aguachica

El diagnóstico del estado de la seguridad de la información para la Universidad Popular Del Cesar, Seccional Aguachica se realizó por medio de una auditoria interna, donde se determinaron los requisitos de las partes interesadas pertinentes a seguridad de la información (NTC-ISO-IEC 27001, 4.2 b), a continuación se describen los resultados.

4.1.1 Contexto de la organización.

La Universidad Popular del Cesar, se crea en el año 1976 mediante Acto legislativo por la cual el instituto Tecnológico Universitario del Cesar, se transforma en la Universidad Popular del Cesar y se dictan otras disposiciones. A través del Congreso de Colombia se Decretó la creación de la Universidad Popular del Cesar como establecimiento público con sede principal en la ciudad de Valledupar.

En el cual en el Artículo primero reza "Créase la Universidad Popular del Cesar, como establecimiento público autónomo con personería jurídica, cuyo objetivo principal será la

investigación y la docencia a través de programas que conduzcan la obtención de licenciaturas, grados profesionales y títulos académicos, como el de doctor.

Como iniciativa del representante de los ex rectores de la Universidad Popular del Cesar en el Consejo Superior Universitario, Dr. Vicente Baños Galvis, se presentó el proyecto de acuerdo, en el mes de septiembre de 1995, para funcionamiento en extensión de los programas Administración de Empresas y Contaduría Pública en el Municipio de Aguachica. Esta iniciativa se sustentó bajo los siguientes lineamientos: Porque se consideraba necesario que se extendiera el funcionamiento de la Universidad Popular del Cesar hacia la región Sur del Departamento del Cesar, pues el estudio de factibilidad elaborado en 1992 por los profesores Simón Martínez Guarnes y la profesora Carmen Patricia Guerrero, dieron como resultado que el Municipio de Aguachica presentaba las condiciones básicas para el funcionamiento de la Universidad.

Los programas extendidos: Administración de Empresas y Contaduría Pública, presentaban la facilidad de hacerlos funcionar de manera inmediata sin mucha exigencia en inversión por parte de la Universidad. Con la aprobación del Acuerdo N° 033 del 22 de diciembre de 1995, por parte del Consejo Superior Universitario, se dio vía libre para que empezaran a funcionar en Aguachica los programas antes citados en extensión. Para concretar este propósito el 21 de enero de 1996 se firmó en Aguachica un convenio interinstitucional entre la Gobernación del Cesar, Dr. Mauricio Pimiento Barrera; la alcaldía de Aguachica Dr. Luís Fernando Rincón López (QEPD) y la Universidad Popular del Cesar Dr. José Antonio Murgas. Este convenio definió los compromisos económicos que cada institución aportaría para el funcionamiento de la extensión en el Municipio de Aguachica. Es de anotar que sólo la Gobernación cumplió con los recursos comprometidos en

el convenio que en los dos años (1996 – 1997) sumaron aproximadamente $140.000.000 millones; el Municipio de Aguachica cumplió en el primer año de 1996 aportando $15.000.000 millones y la Universidad Popular del Cesar bajo la rectoría del Dr. José Antonio Murgas, hizo que los primeros recursos recibidos por concepto de matrícula durante la vigencia 1996 fueron transferidos a la Universidad Popular del Cesar – Valledupar y sólo a partir de la vigencia de 1997, por presión del Consejo Superior Universitario, se logró que los recursos captados por matrícula en Aguachica hicieran parte de su presupuesto. (UNIVERSIDAD POPULAR DEL CESAR, 2017)

4.1.2 Objetivos organizacionales.

La (UNIVERSIDAD POPULAR DEL CESAR, 2016) establece por medio de su proyecto educativo institucional sus objetivos organizacionales así:

- Garantizar a la sociedad el cumplimiento de su misión y visión en cuanto a la calidad de la educación, mediante la implementación de procesos de Autoevaluación, acreditación de sus programas y autorregulación en procura de asegurar la calidad y la excelencia.
- Cumplir las funciones de docencia, con el fin de generar y transmitir el conocimiento a través de metodologías que interrelacionen lo humanístico y lo tecnológico en los estudios propios de cada profesión; en el marco de una educación general, propiciando un escenario para la actividad inter, multi y transdiciplinaria.
- Fortalecer la competitividad, fomentando procesos de innovación, coordinación y supervisión de los proyectos de investigación; asegurando una estrecha interacción entre el Sistema Nacional de Ciencia, Tecnología e Innovación, la Universidad Popular del Cesar y el sector productivo.

- Propender por un conocimiento de la sociedad colombiana a través del fortalecimiento de la comunidad de investigadores de las Ciencias Básicas, Aplicadas, Sociales y Humanas.
- Realizar labores de extensión científica, cultural y de servicio social hacia la comunidad.
- Brindar formación científica, pedagógica, técnica y tecnológica de alto nivel al personal docente e investigadores, como respuesta a garantizar una educación de calidad en sus diferentes niveles y modalidades de formación.
- Promover la conformación de comunidades académicas y científicas, en redes altamente especializadas de conocimiento en el contexto de la educación superior, con la respectiva incorporación de las nuevas tecnologías de la información y la comunicación.
- Extender los programas académicos en el contexto regional para satisfacer las necesidades sociales, culturales, económicas, políticas y educativas de las comunidades interesadas.
- Consolidar y dinamizar el sostenimiento de la comunidad académica Upecista, fortaleciendo las capacidades individuales y colectivas para producir conocimientos educativos, científicos, sociales, económicos y culturales pertinentes.
- Además de los objetivos en comento, la Universidad Popular del Cesar cumplirá aquellos que regulan la Educación Superior en Colombia expresados en la Constitución y la Ley.
- Profundizar en la formación integral de los colombianos dentro de las modalidades y calidades de la Educación Superior, capacitándolos para cumplir las funciones profesionales, investigativas y de servicio social que requiere el país.
- Trabajar por la creación, el desarrollo, la transmisión del conocimiento en todas sus formas y expresiones, promoviendo su utilización en todos los campos para solucionar las necesidades del país.
- Prestar a la comunidad un servicio con calidad, el cual hace referencia a los resultados

académicos, a los medios y procesos empleados, a la infraestructura institucional, a las dimensiones cualitativas y cuantitativas del mismo y a las condiciones en que se desarrolla cada institución.

- Ser factor de desarrollo científico, cultural, económico, político y ético a nivel nacional y regional, actuando armónicamente entre sí con las demás estructuras educativas y formativas.
- Contribuir al desarrollo de los niveles educativos que le preceden para facilitar el logro de sus correspondientes fines.
- Promover la formación y la consolidación de comunidades académicas y la articulación con sus homólogas a nivel regional, nacional e internacional.
- Promover la preservación de un medio ambiente sano y fomentar la educación y cultura ecológica.
- Conservar y fomentar, el patrimonio cultural del país1.

4.1.3 Misión y Visión.

Misión. La Universidad Popular del Cesar, como institución de educación superior oficial del orden nacional, forma personas responsables social y culturalmente; con una educación de calidad, integral e inclusiva, rigor científico y tecnológico; mediante las diferentes modalidades y metodologías de educación, a través de programas pertinentes al contexto, dentro de la diversidad de campos disciplinares, en un marco de libertad de pensamiento; que consolide la construcción

[1] Acuerdo 011 31 de marzo de 216 PEI, Pág. 33.

de saberes, para contribuir a la solución de problemas y conflictos, en un ambiente sostenible, con visibilidad nacional e internacional.

Visión. En el año 2025, la Universidad Popular del Cesar será una Institución de Educación Superior de alta calidad, incluyente y transformadora; comprometida en el desarrollo sustentable de la Región, con visibilidad nacional y alcance internacional.

4.1.4 Estructura.

4.1.4.1 Organigrama General.

La estructura general de la Universidad Popular del Cesar Seccional Aguachica es jerárquica, el nivel más alto lo comprende la Vicerrectoría de Seccional, de la cual se desprenden dos grandes direcciones, la Dirección administrativa y financiera y la Dirección Académica. Cada una de ellas lidera a nivel funcional y operativo las demás áreas de la institución.

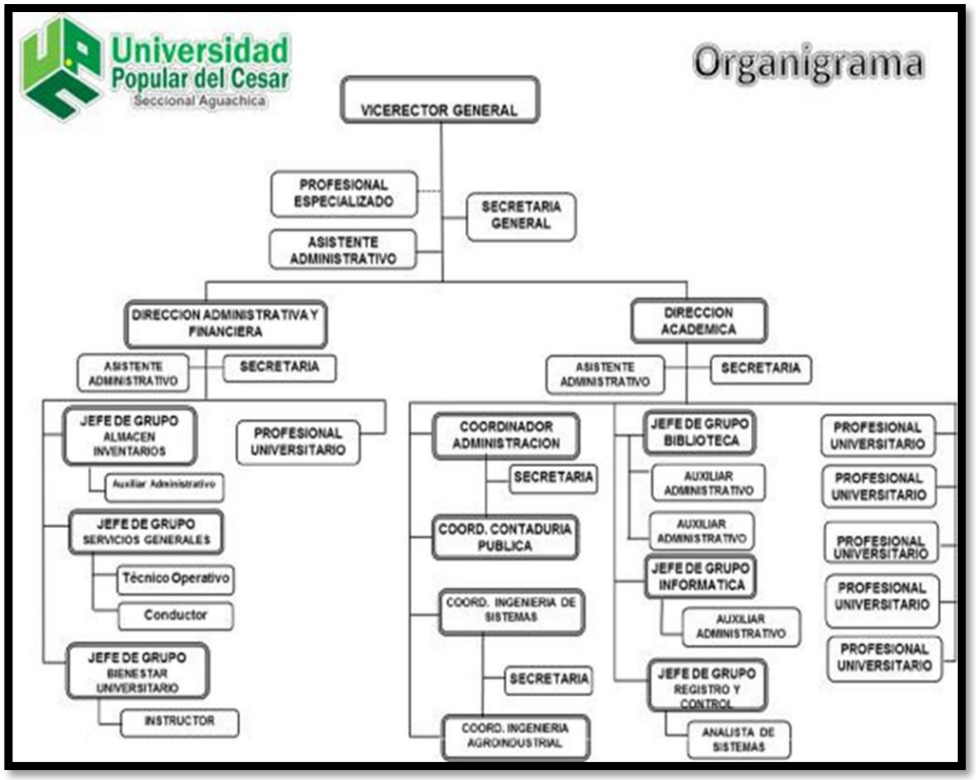


Figura 1. Organigrama de la Universidad Popular del Cesar Seccional Aguachica.
Fuente: Universidad Popular del Cesar Seccional Aguachica.

4.1.4.2 Mapa de procesos.

Teniendo en cuenta los procesos de la Universidad Popular del Cesar Seccional Aguachica soportados por sus dependencias y sistemas de información los cuales permiten que los procesos se desarrollen de manera ágil y óptima, la seccional opera de acuerdo al siguiente mapa de macro procesos:

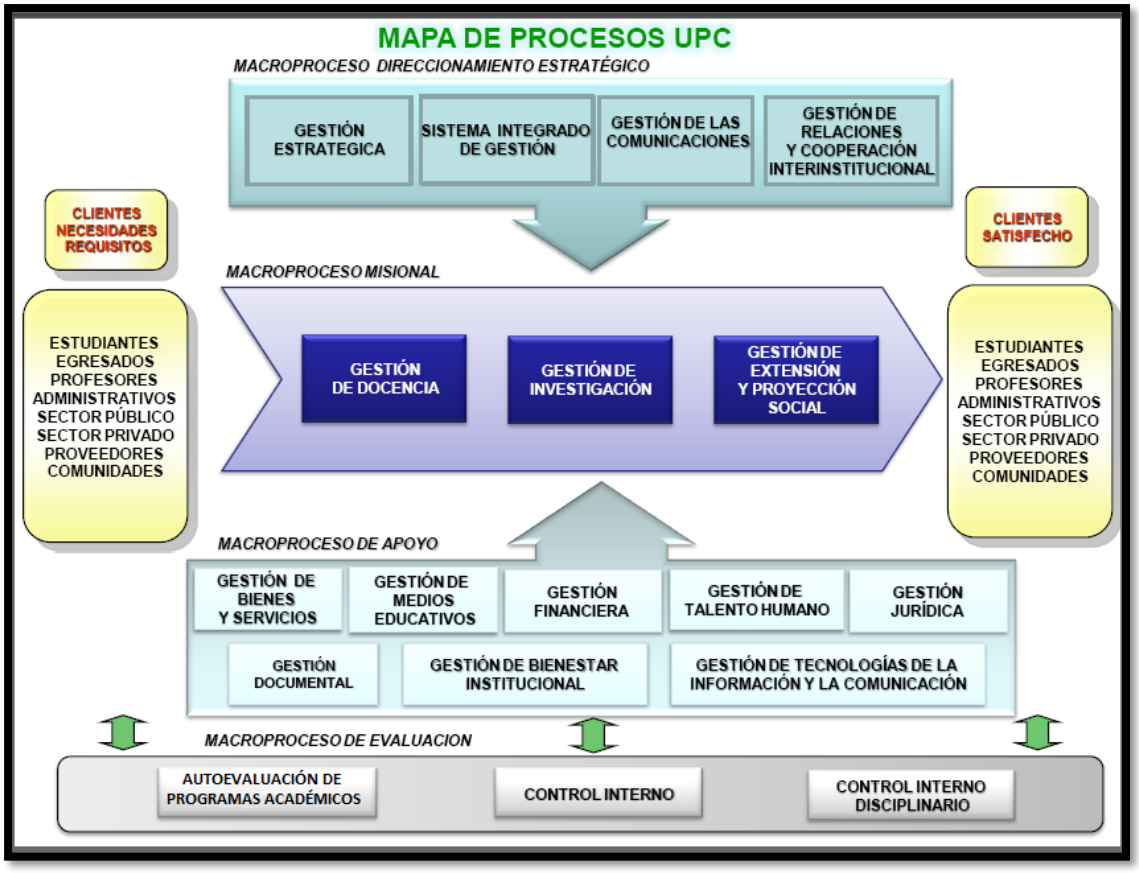


Figura 2. Mapa de procesos de la Universidad Popular del Cesar seccional Aguachica.
Fuente: Universidad Popular del Cesar Seccional Aguachica.

La Universidad Popular del Cesar Seccional Aguachica actualmente cuenta con un equipo de personal de 33 Funcionarios de planta, 2 docentes de planta, un equipo de personal en el área de servicios generales de 7 personas, 1 contratista en el área de sistemas y soporte TIC, 1 contratista como apoyo en el área de Dirección académica, teniendo un total 44 personas, de los cuales el 70% tiene a cargo equipos de cómputo para realizar sus labores diarias.

4.1.5 Infraestructura Tecnológica de la Universidad Popular del Cesar Seccional Aguachica.

La institución cuenta con 5 nodos establecidos en puntos estratégicos de manera que se pueda tener conexión a cualquier dependencia dentro del área de trabajo general, estos nodos están establecidos de la siguiente forma:

Tabla 2.

Características nodo principal (Llegada del canal dedicado)

	Característica
Topología de red física	Estrella extendida
Canal dedicado Colombus fibra óptica	80 Megas
Router	Cisco catalist 3560-X
Balanceador	Peplink Balance 560
Controladora Wifi	Ruckus Factor 1200
Router	Raisecom Fibra Colombus
Ubicación	Segundo Piso
Tipo de Rack	Armario bastidor 42 Ru
Servidor	HP Proliant

Fuente: Autores del proyecto.

Tabla 3.

Características nodo Sala de Informática.

	Característica
Topología de red física	Estrella extendida
Router	Cisco catalist 2960
Ubicación	Sala de Informática
Tipo de Rack	Armario bastidor 30 Ru

Fuente: Autores del proyecto.

Tabla 4.

Características nodo Bienestar Universitario

	Característica
Topología de red física	Estrella extendida
Router	Cisco catalist 2960
Ubicación	Bienestar Universitario
Tipo de Rack	Armario bastidor 30 Ru

Fuente: Autores del proyecto.

Tabla 5.

Características nodo Registro y control

	Característica
Topología de red física	Estrella extendida
Router	Cisco catalist 3560-X
Ubicación	Registro y Control
Tipo de Rack	Armario bastidor 11 Ru

Fuente: Autores del proyecto.

Tabla 6.

Características nodo Laboratorio de Redes y Telecomunicaciones

	Característica
Topología de red física	Estrella extendida
Router	Cisco catalist 3560-X
Ubicación	Laboratorio de Redes y telecomunicaciones
Tipo de Rack	Rack de piso

Fuente: Autores del proyecto.

4.1.5.1 Esquema lógico de red.

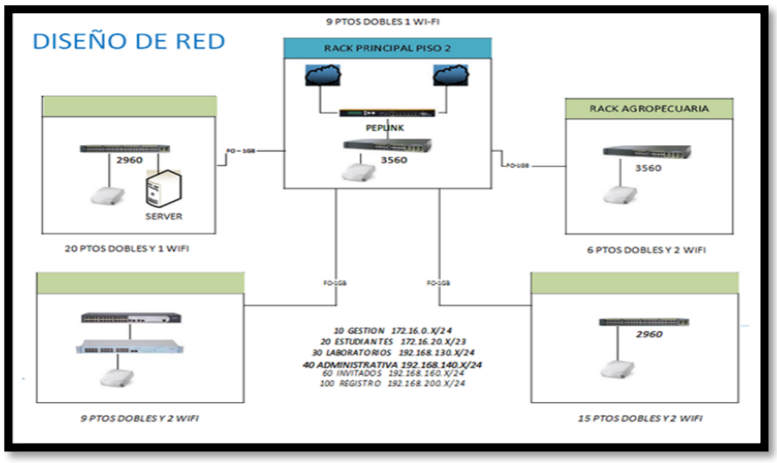


Figura 3. Diseño y distribución lógico de la Red Universidad Popular del Cesar Seccional Aguachica.

Fuente. Autores del proyecto

4.1.5.2 Sistemas de información que utiliza la Universidad Popular del Cesar Seccional Aguachica.

Tabla 7.

Sistemas de información usados por la Universidad Popular del Cesar Aguachica

	Descripción
Academusoft	Sistema de información que integra un gran número módulos para el manejo funcional de cada componente administrativo y académico de la institución, Este campus tiene módulos como: Admisiones, Registro académico, Recursos Académicos, Carga Académica, Matrícula Académica, Matricula Financiera, Recursos Físicos, Horarios, Grados, Egresados entre otros, este sistema es

	Descripción
	usado por diversas Oficinas y es el de mayor importancia para la institución.
Sysman	Software para el registro de Inventario usado en la dependencia de Almacén
Hemeroteca – Siibupc	Sistema usado por la Biblioteca para el Registro, Inventario, Categorización, Control, Préstamo y Devolución de los elementos bibliográficos de la dependencia.

Fuente: Autores del proyecto

4.1.5.3 Servidores

Tabla 8.

Servidores

	Función	Referencia	Sistema Operativo
Servidor 1	Aula Virtual UPC	Dell	Virtualizado (Windows, Debían)
Servidor 2	Practicas Laboratorio	Hp Proliant	Virtualizado(Ubuntu Server)

Fuente: Autores del proyecto.

4.1.6 Informe de Auditoria.

Con el fin de diagnosticar el estado de la seguridad de la información en la Universidad Popular del Cesar, Seccional Aguachica, para conocer sus amenazas, vulnerabilidades e impactos, se realizó una auditoria interna de gestión con base a los requisitos del estándar ISO 27001, con los siguientes resultados:

4.1.6.1 Objetivo de la Auditoria.

Diagnosticar los requisitos de las partes interesadas pertinentes a seguridad de la información, con el fin de comprender las necesidades y expectativas referentes a esta, y determinar una línea base para el diseño del sistema de gestión de la seguridad de la información

4.1.6.1.1 Específicos.

- Evaluar las necesidades y expectativas pertinentes al sistema de gestión de la seguridad de la información en directivos, funcionarios y estudiantes de la Universidad Popular del Cesar Seccional Aguachica
- Identificar las situaciones problemáticas actuales de gestión de la seguridad de la información
- Establecer posibles causas y soluciones potenciales para el análisis de la información

4.1.6.2 Alcance de la auditoria.

Para los efectos del diagnóstico esta auditoria se evaluaron once procedimientos del sistema de gestión para las áreas administrativas de la Universidad Popular del Cesar, de acuerdo a las actividades o funciones a evaluar relacionadas en la tabla 9.

Tabla 9.

Alcance de la auditoria

Universidad Popular Del Cesar Seccional Aguachica			Fecha Inicial			Fecha Final		
			Dias	**Mes**	**Año**	**Dias**	**Mes**	**Año**
			08	**08**	**17**	**10**	**08**	**17**
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
EA-001	Identificar el grado de uso de políticas de seguridad.	Encuesta						
EA-002	Identificar el conocimiento sobre seguridad de la información en los empleados de la UPC Aguachica.	Encuesta						
EA-003	Seguridad Física y Ambiental	Encuesta						
EA-004	Control de Accesos	Encuesta						
EA-005	Seguridad en las Redes y Telecomunicaciones	Encuesta						
EA-006	Compra, Desarrollo y mantenimiento en los sistemas de información.	Encuesta						
EA-007	Administración y Gestión de los Activos presentes.	Encuesta						
EA-008	Identificar la seguridad con respecto a RH (Recursos humanos y	Encuesta						

Universidad Popular Del Cesar Seccional Aguachica			Fecha Inicial			Fecha Final		
			Dias	Mes	Año	Dias	Mes	Año
			08	08	17	10	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
	control interno)							
EA-009	Aspectos de Seguridad de la información con respecto a la continuidad del proceso.	Encuesta						
EA-010	Gestión y Bitácora de problemas de Seguridad de la información.	Encuesta						
EA-011	Identificar el conocimiento sobre seguridad de la información en los estudiantes de la UPC Aguachica.	Encuesta						

Fuente. Autores del proyecto.

4.1.6.3 Actores auditados

La auditoría se realizó con la totalidad de los funcionarios administrativos de la Universidad Popular del Cesar Seccional Aguachica, alcanzando 31 funcionarios.

4.1.6.4 Plan general de auditoria

El plan de auditoria consta de la elaboración del plan de trabajo, la investigación preliminar, la guía para el dictamen de la auditoria y el diseño de los instrumentos de recolección de información, los cuales se relacionan a continuación:

4.1.6.4.1 Plan de trabajo

Tabla 10.

Plan de trabajo de la auditoria

Etapa	**Descripcion**	**Actividad a desarrollar**	**Numero de participantes**	**Periodo estimado**	
				INICIO	**FIN**
1	Identificar la actividad que desarrolla la institución, su estructura y los servicios que ofrece con el fin de realizar una adecuada auditoria	Visitar las áreas que van a ser auditadas	Didier Fernando Guerrero Sumalave	1/08/17	5/08/17
		Verificar manual de funciones y organigrama	Laura Marcela Felizzola Conde		
		Determinar el alcance y objetivos.	Roger Oswaldo Lizcano Ruiz		
		Seleccionar las técnicas y métodos de recolección de la	Andrea Johanna Navarro Claro		

Etapa	Descripcion	Actividad a desarrollar	Numero de participantes	Periodo estimado	
				INICIO	FIN
		información. Realizar y hacer entrega del acta de inicio de auditoria.			
2	Ejecutar cada una de las herramientas que se van a utilizar para el proceso de auditoria	Realizar la entrevista. Efectuar la encuesta. Llevar a cabo las listas de chequeo. Realizar las pruebas que sean necesarias.	Didier Fernando Guerrero Sumalave Laura Marcela Felizzola Conde Roger Oswaldo Lizcano Ruiz Andrea Johanna Navarro	8/08/17	10/08/17
3	En esta etapa se lleva a cabo la verificación de la información recolectada y se da a conocer las situaciones encontradas, se entrega el dictamen y	Identificar las situaciones relevantes. Socializar los hallazgos con el grupo de auditores y auditados.	Didier Fernando Guerrero Sumalave Laura Marcela Felizzola Conde	11/08/17	16/08/17

Etapa	Descripcion	Actividad a desarrollar	Numero de participantes	Periodo estimado INICIO	FIN
	recomendaciones necesarias.	Elaborar el dictamen final. Presentar informe final a las partes interesadas.	Roger Oswaldo Lizcano Ruiz Andrea Johanna Navarro		

Fuente. Autores del proyecto.

Ver Apéndice 1. Carta de inicio de la Auditoria

4.1.6.5 Guía de auditoria fase investigación preliminar.

Tabla 11.

Guía de auditoria fase investigación preliminar.

	Universidad Popular del Cesar Seccional Aguachica		Fecha Inicial			Fecha Final		
			Dias	Mes	Año	Dias	Mes	Año
			01	08	17	05	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
IP-001	Visita preliminar a la institución a auditar	Observación.						
IP-002	Realizar una identificación	Realizar una verificación						

Universidad Popular del Cesar Seccional Aguachica			Fecha Inicial			Fecha Final		
			Dias	Mes	Año	Dias	Mes	Año
			01	08	17	05	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
	de la estructura organizacional de la Universidad Popular del Cesar Seccional Aguachica y las funciones de cada empleado.	documental del Organigrama, Objetivos Misionales, Manual de funciones y procedimientos, Inventarios y estructura lógica y física.						
IP-003	Crear y documentar el alcance y objetivo de la Auditoria.	Documento.						
IP-004	Establecer las dependencias y Personal a Auditar.	Observación y Documentación.						
IP-005	Diseñar los documentos de Recolección de Información.	Documentación.						
IP-006	Entrega del Acta de Iniciación de la	Documentación.						

	Universidad Popular del Cesar Seccional Aguachica		Fecha Inicial			Fecha Final		
			Dias	Mes	Año	Dias	Mes	Año
			01	08	17	05	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
	Auditoria a la alta gerencia.							

Fuente. Autores del proyecto.

4.1.6.5.1 Guía de auditoria fase dictamen de la auditoria.

Tabla 12.

Guía de auditoria fase dictamen de la auditoria.

	Universidad Popular del Cesar Seccional Aguachica		Fecha inicial			Fecha final		
			Días	Mes	Año	Días	Mes	Año
			11	08	17	16	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
DA-001	Analizar la información que se recolecto y agrupar y recopilar las situaciones encontradas.	Documentación.						
DA-002	Reunir al equipo de Auditoria y el personal auditado para comentar las	Reunión, Documentación						

Universidad Popular del Cesar Seccional Aguachica			Fecha inicial			Fecha final		
			Días	Mes	Año	Días	Mes	Año
			11	08	17	16	08	17
Referencia	**Actividad o Función a evaluar**	**Técnica de evaluación**	**Calificación**			**Observación**		
	situaciones encontradas y determinar causas y soluciones.							
DA-003	Elaborar el Informe final.	Documento						
DA-004	Realizar reunión con la alta gerencia y presentar el informe final.	Reunión						

Fuente. Autores del Proyecto.

4.1.6.5.2 Instrumentos de Recolección de Información.

Para la recolección de información se diseñaron tres tipos de encuestas, orientadas a diferentes actores, entre ellos participaron Administrativos, el Analista de Sistemas y por último el Jefe de Laboratorios. Las encuestas fueron de tipo escrito y oral y se busca obtener información de percepción. Diseño de instrumentos Apéndices 2, 3 y 4.

4.1.6.6 Dictamen

Dentro de los principales hallazgos se pueden identificar los relacionados a continuación, Ver Apéndice **5,** donde presentan los resultados de la aplicación de la auditoria.

- No existen unas políticas de seguridad de la información adecuadas para el tratamiento de seguridad confidencial de la UPCSA.
- Falta de buenas prácticas en el uso de contraseñas de acceso para los equipos y Sistema de información Academusoft en las distintas dependencias de la UPCSA
- Ausencia de realización de copias de seguridad y restauración (Backus) de información en dependencias como Registro y control, Financiera, biblioteca y Coordinaciones.
- Malas condiciones físicas y de espacio en la oficina de Registro y Control, teniendo en cuenta la importancia de la información que se almacena físicamente.
- Malos manejos en los almacenamientos de información en medios magnéticos en las diferentes dependencias de la UPCSA.
- Se encuentra un incumplimiento en algunas funciones de los administrativos.
- No se cuenta con un manual de seguridad de la información aprobado e implementado para esta dependencia.
- Uso de datos personales en contraseñas para acceso a equipos de cómputo y sistema de información Academusoft.
- Falta de políticas para la seguridad en la entrada de personas que no están autorizadas a manipular información de la dependencia.

- Se Observó que no existe un control pertinente para el manejo de Dispositivos como Pendrive o Quemadoras, Lo comprende una falla de seguridad importante.
- No existe un sistema de seguridad o video vigilancia para las áreas donde se comprometa la información de mayor importancia de la UPCSA.
- No se cuenta con un sistema de contingencia para la continuidad de la energía eléctrica en la UPCSA en caso de una falla de este tipo.
- La UPCSA en algunas dependencias y equipos de cómputo no cuenta con sistemas de UPS que permita el funcionamiento por lo menos de 10 min para realizar el correcto cierre y apagado de las aplicaciones en caso de una falla eléctrica.
- La UPCSA no cuenta con un equipo de hardware para realizar filtrado de contenido web.
- La UPCSA no cuenta con un DATA CENTER centralizado, cuenta con 5 nodos de comunicaciones en diferentes lugares de la institución, lo que no permite poder monitorear de mejor manera las actividades dentro de la red de datos y demás.
- No existe una oficina de control interno dentro de la UPCSA que garantice que los administrativos estén realizando las labores del manual de funciones de manera correcta.
- La UPCSA no cuenta con un sistema de alarma y detección de humo que esté conectada a la central de bomberos.
- No se tiene claridad por parte de los administrativos para la no instalación de software licenciado no adquirido por la UPCSA y de uso prohibido en los equipos de cómputo.
- No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos.

- No se tiene documentado el control y bitácora para el registro de las actividades o acontecimientos dentro de la red de datos, como fallas en el servicio, direcciones IP'S con alto consumo de ancho de banda.
- No se cuentan con políticas de control formal para la trasferencia de información por cualquier medio.
- Nunca se han realizado auditorias de sistemas a la red y cableado estructurado.
- No existe un control de visitantes al momento de ingresar a la UPCSA, no son llevados en acompañamiento por el grupo de vigilancia contratado hacia la dependencia a visitar.
- No existen controles como biométricos o bitácoras de acceso a los diferentes Rack de equipos ubicados en distintos puntos de la UPCSA.
- La entrada no cuenta con una cámara de seguridad para el control de acceso, grabación y monitorización del personal que ingresa a la UPCSA.
- Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás.
- Los días no laborales se observa que algunos lugares dentro de la UPCSA no cuentan con el respectivo cierre para el no ingreso de estudiantes o invitados, lo que genera grandes riesgos en la seguridad de los sistemas de información.
- Se observa que el Ingeniero de soporte aunque registra en un informe mensual los cambios o soportes que realiza en las diferentes dependencias, estos cambios de hardware y software no queda registrados en una bitácora o formato de control de cambios.
- Algunos equipos no cuentan con contraseña de acceso que restrinja a otros usuarios el ingreso al sistema operativo.

- Los equipos de la UPCSA no cuentan con antivirus licenciado o algún dispositivo de hardware firewall que controle accesos a la red no autorizados, se usa un antivirus gratuito de Microsoft.
- Existen los extintores en sitios estratégicos pero no se cuenta con un control de cambios o tiempos en el mantenimiento de los mismos.
- No existe un plan de contingencia en caso de emergencias o desastres naturales.
- No existe un control o bitácora para cambios y accesos a los Rack de comunicaciones (nodos) por parte del encargado del área de Redes de la UPCSA.
- No existen herramientas para la protección contra código malicioso.
- No se realiza gestión y registro de incidentes de la seguridad de la información.
- No existe un control de las llaves para el acceso a dependencias importantes, algunos funcionarios cuentan con llaves y copias lo que podría generar problemas de seguridad, por las noches los vigilantes manejan las llaves.
- No existe una política de cambio de cerraduras para las dependencias importantes y de alto riesgo.
- No existe un control para deshabilitar los puertos de red que puedan provocar Riesgo en la conexión de visitantes o personas externas a la UPCSA.
- No se realiza un cambio periódico a las claves de acceso a la Red Inalámbrica difundidas dentro de la UPCSA.
- No existe un monitoreo y registro permanente de la cantidad de usuarios de la red inalámbrica, durante los momentos de más afluencia dentro de la UPCSA.

- Se considera que la UPCSA no es demasiado grande por lo cual no se cuenta con un equipo de Firewall para el control del ancho de banda de fibra óptica por lo que se permite que todas las redes accedan al mismo medio.
- No existe una oficina de Sistemas o soporte con un equipo de Ingenieros que soporten todo el Sistema de seguridad de la información, dentro de la UPCSA.
- Se observa que en la dependencia de Biblioteca aunque se tienen cámaras de seguridad y se realiza la grabación durante el 80% de las horas laborales, el equipo no tiene normas mínimas de control de acceso y cualquier persona puede acceder a esta información.
- No existe dentro de la UPCSA un método de cifrado de información, para las dependencias de manejo de datos de alto riesgo.
- Desconocimiento del uso de la nube y el drive para el almacenamiento seguro de información, como medio externo para evitar problemas de seguridad en los equipos locales.
- No existen políticas de control de riesgo en los laboratorios de informática y dependencias para mitigar los incidentes que puedan suceder dentro de la UPCSA.
- Falta de entrenamiento y capacitación al colectivo de administrativos sobre seguridad de la información.
- Falta de políticas de control y detección de Ransomware y malware dentro de la dependencias de la UPCSA.
- Falta de políticas de seguridad en el control de acceso y proceso de Subcontratación de servicios y terceros.
- Los terceros ingresan a áreas restringidas sin recibir primero permiso de la alta gerencia.

- No se realiza una inspección de posibles dispositivos tecnológicos en la entrada cuando ingresan visitantes y personal administrativo.
- Se observó en varias ocasiones de la auditoria que no se realiza por parte del servicio de vigilancia contratado la solicitud de carnet o credenciales adecuadas para el ingreso del personal a la UPCSA.

4.1.6.7 Oficio de Entrega del dictamen

Una vez efectuada la auditoria y la elaboración del informe, procede la entrega de los dictámenes a la vicerrectoría, con el fin de socializar los resultados de la misma, para esto se realizó un oficio de entrega que se relaciona a continuación, Ver Apéndice 6.

Tabla 13.

Oficio de entrega del dictamen

Aguachica – Cesar, 08 de agosto del 2017
Dra. Carmen Socorro Guzmán Rodriguez **Vicerrectora (e)**
Universidad Popular del Cesar Seccional Aguachica
Teniendo en cuenta el proceso de mejora continua que se viene presentando dentro de la Universidad Popular del Cesar, Seccional Aguachica, se realizó la auditoría con el objetivo de detectar gran parte de inconsistencias en relación con el tratamiento de la seguridad de la información dentro de las dependencias donde se utiliza información importante y critica que comprometa los objetivos misionales de la institución, por esta razón se presenta ante usted de

manera oficial el resultado obtenido, la cual se practicó desde el 01 de Agosto del 2017 hasta el 16 de Agosto del 2017.

A continuación se presentan las deducciones obtenidas durante el siguiente proceso.

Durante este tiempo se efectuaron actividades de auditoria dando como prioridad el análisis de los procesos relacionados con el uso de información importante por parte de las dependencias que soportan los objetivos misionales de la Universidad Popular del Cesar Seccional Aguachica, temas como la estructura organizacional, infraestructura de red, esquema lógico, sistemas de información, Bases de datos locales y en red, Software, Hardware, todo esto basado en el estándar ISO:IEC 27001: 2013, para este análisis se usó diferentes tipos de instrumentos de recolección de información como entrevistas, listas de chequeo, encuestas y cuestionarios.

Se dictamino como análisis final que las medidas que se implementan para salvaguardar la integridad, disponibilidad y confidencialidad de la información que se maneja, no están debidamente estructuradas y basadas en políticas de seguridad de la información establecidas por la alta gerencia, que permitan proteger mediante directivas el bien más importante para la institución y así poder cumplir con los objetivos misionales como razón de ser. Por todo esto se mencionan las fallas generales en las que recaen repetidamente y provoca ineficiencias en los procesos y personal administrativo, siendo este último la línea más fácil de romper dentro de un sin número de inconsistencias encontradas, como primera observación debemos mencionar que la institución carece de unas políticas establecidas para el tratamiento de la seguridad de la información, no se cuenta con unas directivas que permita realizar mediante controles el seguimiento de las funciones y actividades que se realicen por parte de los usuarios en sus diferentes dependencias, a pesar de que se cuenta con un manual de funciones, este no es regularmente actualizado por parte de los directivos y encargados, esta falla se debe a que dentro de la institución no está establecido formalmente una oficina de sistemas que se encargue de esta labor así como la socialización con el personal administrativo de nuevos cambios y mejoras en los pocos controles que se imparten dentro de diferentes procesos.

La falta de un manual de políticas de la información es una falla de gran importancia y relevancia, puesto que no se llevan controles, no se registran incidentes con respecto al manejo de información, no se realizan los respectivos Backus de datos necesarios, lo que impide realizar planes de contingencia y una toma de decisiones rápida en estos eventos.

Los funcionarios de la institución no reciben capacitaciones para conocer de la mejor forma las buenas prácticas para el tratamiento de la información y evitar así poner en riesgo la integridad, disponibilidad y confidencialidad de los datos de los sistemas de información dentro de dependencias como Registro y control, oficina administrativa y financiera, Biblioteca, Postgrados y laboratorios de computo entre otras, este desconocimiento no solo genera un importante riesgo sino que a su vez no les permite evitar recurrir en un sinfín de incidentes con el tratamiento de la información y lo que relaciona a ella.

La Institución no cuenta con un plan de contingencias que permita reaccionar a incidentes de seguridad en caso de presentarse, se observó que no se cuenta con la medidas convenientes como señalización, salidas de emergencia, avisos y guías de entradas y salidas, seguimiento de elementos como extintores, botiquín y herramientas de control de accidentes para conocer su estado, mejora o cambio.

Se cuenta con falencias en el tema de seguridad física de las instalaciones, no se tiene un sistema de video vigilancia que registre temas como entrada y salida de personal administrativo, estudiantado y visitantes a la institución, a pesar de que se cuenta con un contratista en el área de seguridad con el personal calificado, los visitantes puede tener acceso a todas las áreas de la institución siendo esto un grave problema de seguridad, en algunos casos son acompañados por el vigilante hasta la entrevista con el funcionario pero en otras ocasiones el procedimiento no se realiza de la mejor forma y se pone en riesgo el lugar.

No existe un encargado de implementar políticas de seguridad, controlar y monitorear ciertos procesos que requieren un seguimiento importante, aunque se cuenta con un contratista dedicado a labores relacionados con cableado estructurado y todo lo que tiene que ver con las conexiones de servicio de internet y fibra óptica, es necesario y sería de gran importancia organizar un área

dedicado a temas de implementación y verificación de dichas políticas y así poder minimizar en gran parte los riesgos en los que se puede incurrir en las diferentes dependencias dentro de la organización.
Elaborado Por
Didier Fernando Guerrero Sumalave Laura Marcela Felizzola Conde Andrea Navarro Claro Roger Oswaldo Lizcano Ruiz

Dictamen auditoría Universidad Popular del Cesar Seccional Aguachica.

Fuente: Los autores

4.2 Elementos del estándar ISO 27001, aplicables en la Universidad Popular del Cesar, Seccional Aguachica.

Considerando los aspectos del contexto organizacional de la Universidad Popular del Cesar Seccional Aguachica, su estructura, procesos, recursos humanos y técnicos y sus objetivos misionales, se puede identificar que la concentración de la información se halla en los aspectos académicos y financieros. Sin embargo, no hay que olvidar que al hablar de sistemas interrelacionamos cada aspecto y cada actor de la organización, convirtiendo cada necesidad en una posible fuente de información.

Para determinar qué elementos del estándar ISO 27001, son susceptibles de ser aplicados en la Universidad Popular del Cesar, Seccional Aguachica, empezamos identificando que la institución no cuenta con ninguna herramienta para garantizar la seguridad de la información, y

que solo se pretende iniciar un proceso de conceptualización y diseño, como fase preliminar de un pretendido sistema de gestión de seguridad de la información.

De acuerdo al primer capítulo del estándar ISO 27001, Objeto y Campo de Aplicación que reza "*Esta norma, especifica los requisitos para Establecer, Implementar, Mantener y Mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización*" (ISO/IEC 27001, 2013) Pág. 1. Podemos ver claramente el fundamento del ciclo P-H-V-A, el cual es la base para determinar las fases de planificación, ejecución, verificación y mejoras.

Tabla 14.

Relación entre los objetivos del estándar ISO 27001 y el ciclo P-H-V-A

OBJETIVOS DEL ESTANDAR ISO 27001	**CICLO P-H-V-A**
ESTABLECER	PLANEAR
IMPLEMENTAR	HACER
MANTENER	VERIFICAR
MEJORAR	ACTUAR

En este sentido, se utilizó la Herramienta de Diagnostico de Seguridad y Privacidad de la Información elaborada por el MINTIC del 9 de junio de 2017, definida para adoptar el Modelo de Seguridad y Privacidad de la Información en el marco del Programa Gobierno en Línea, ya que al ser la Universidad una entidad del Orden Nacional, le es aplicable.

La Herramienta de Diagnostico de Seguridad y Privacidad de la Información establece, *El "Instrumento de Evaluación MSPI" Es una herramienta que fue creada con el fin de identificar

el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”. Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de la misma. (MinTIC, 2017)

4.2.1 Elementos de identificación de la línea base de seguridad de la información.

A continuación se relacionan, el resumen de los resultados de la evaluación de controles y la evaluación de modelo del ciclo P-H-V-A:

Tabla 15.

Instrumento de Evaluación MSPI aplicado a la Universidad Popular del Cesar. Seccional Aguachica

No.	Evaluación de Efectividad de controles			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	**Inexistente**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	12	100	**Inicial**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	0	100	**Inexistente**
A.8	GESTIÓN DE ACTIVOS	32	100	**Repetible**
A.9	CONTROL DE ACCESO	5	100	**Inicial**
A.10	CRIPTOGRAFÍA	0	100	**Inexistente**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	**Inicial**
A.12	SEGURIDAD DE LAS OPERACIONES	11	100	**Inicial**
A.13	SEGURIDAD DE LAS COMUNICACIONES	14	100	**Inicial**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	5	100	**Inicial**
A.15	RELACIONES CON LOS PROVEEDORES	0	100	**Inexistente**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	**Inexistente**

No.	Evaluación de Efectividad de controles			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL PROCESO	10	100	**Inicial**
A.18	CUMPLIMIENTO	36,5	100	**Repetible**
Promedio Evaluación De Controles		**10**	**100**	**Inicial**

4.2.2 Elementos del componente de planificación aplicables a la Universidad

Como se determinó anteriormente, la línea base del sistema de gestión de información se encuentra en su etapa inexistente o inicial, por esta razón, los elementos aplicables a la UPC SA deben ser aquellos asociados al componente de planificación (Ver Apéndice 7), el cual incluye[2],

- Alcance MSPI (Modelo de Seguridad y Privacidad de la Información): Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.
- Políticas de seguridad y privacidad de la información: 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 la partes externas pertinentes
- Procedimientos de control documental del MSPI : La información documentada se debe controlar
- Roles y responsabilidades para la seguridad de la información: Se deben definir y asignar todas las responsabilidades de la seguridad de la información
- Inventario de activos: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Identificación y valoración de riesgos: Metodología de análisis y valoración de riesgos e informe de análisis de riesgos
- Toma de conciencia, educación y formación en la seguridad de la información: Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la

[2] Tomado de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información

educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

4.3 Establecimiento del sistema de gestión de la seguridad de la información (SGSI) para la Universidad Popular del Cesar, Seccional Aguachica.

Con el fin, de iniciar una estrategia organizacional, para establecer los principios de un Sistema de Gestión de Información para la Universidad Popular del Cesar Seccional Aguachica, que beneficie a todas las partes interesadas y fortalezca las herramientas para el cumplimiento de su misión, la cual es formar personas con una educación de calidad, se establece una política de seguridad de la información, que proporcionara los elementos para gestión adecuada de la misma.

Contenido:

- Objetivo
- Alcance
- Declaración de la política de seguridad de la información
- Roles y responsabilidades
- Inventario de activos
- Identificación y valoración de riesgos
- Plan de capacitación

4.3.1 Objetivo

Establecer los elementos primarios del componente de planificación del sistema de gestión de la información de la Universidad Popular del Cesar Seccional Aguachica, con el fin de iniciar una estrategia para la futura implementación, mantenimiento y mejora continua de la información.

4.3.2 Alcance.

Al ser Universidad Popular del Cesar Seccional Aguachica, una institución superior de carácter oficial, estas directrices aplican para toda la institución, sus funcionarios, contratistas, terceros y comunidad en general.

4.3.3 Declaración de la política de seguridad de la información.

La siguiente política fue toma como base, del modelo de Política General De Seguridad Y Privacidad De La Información, proporcionado por el Min Tic, en el documento Elaboración de la política general de seguridad y privacidad de la información. (MinTic, 2016):

La dirección de la Universidad Popular del Cesar Seccional Aguachica, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Universidad Popular del Cesar Seccional Aguachica, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, estudiantes, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, estudiantes, practicantes y usuarios de la Universidad Popular del Cesar Seccional Aguachica
- Garantizar la continuidad del proceso frente a incidentes.
- La Universidad Popular del Cesar Seccional Aguachica, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información,

soportado en lineamientos claros alineados a las necesidades del proceso, y a los requerimientos regulatorios.

A continuación se establecen 12 principios de seguridad que soportan el SGSI de La Universidad Popular del Cesar Seccional Aguachica:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de proceso o terceros.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA protegerá la información generada, procesada o resguardada por los procesos de proceso, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o usuarios), o como resultado de un servicio interno en outsourcing.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de proceso, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA protegerá su información de las amenazas originadas por parte del personal.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA controlará la operación de sus procesos de proceso garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA implementará control de acceso a la información, sistemas y recursos de red.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA garantizará la disponibilidad de sus procesos de proceso y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4.3.4 Roles y responsabilidades

La vicerrectoría de seccional, como parte de la alta dirección, será en todo caso la responsable de establecer, implementar, mantener y mejorar el sistema de gestión de la información, apoyada en los líderes de sus procesos misionales. Para el apoyo en las áreas de operación se recomiendan los siguientes roles:

- **Responsable / área:** Control interno/Vicerrectoría

  Revisiones de seguridad de la información

  Revisión independiente de la seguridad de la información

  Cumplimiento con las políticas y normas de seguridad.

  Cumplimiento

  Auditoría interna plan

  Auditoría interna ejecución y subsanación de hallazgos y brechas

- **Responsable / área:** Gestión humana/ Dirección administrativa y financiera

  Selección e investigación de antecedentes

  Términos y condiciones del empleo

- **Responsable / área:** Registro y control académico/ Coordinador de registro y control

  Selección, admisión y matricula

  Gestión de información académica

- **Responsable / área:** Dirección administrativa y financiera

  Liquidación y presupuesto

  Ejecución presupuestal

  Terminación y cambio de empleo

  Gestión de activos

  Cumplimiento

- **Responsable / área:** Almacén e inventario/ Jefe de almacén

  Gestión de inventario

  Ingreso y salida de almacén

  Almacén Responsable

- **Responsable / área:** Responsable de compras y adquisiciones/ Dirección administrativa y financiera

  Relaciones con los proveedores

  Seguridad de la información en las relaciones con los proveedores

  Gestión de la prestación de servicios de proveedores

- **Responsable / área:** Responsable de la continuidad/ Vicerrector

  Aspectos de seguridad de la información de la gestión de la continuidad del proceso

  Continuidad de la seguridad de la información

  Planificación de la continuidad de la seguridad de la información

  Implementación de la continuidad de la seguridad de la información

  Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

  Redundancias

  Disponibilidad de instalaciones de procesamiento de información

- **Responsable / área:** Responsable de la seguridad física/ Jefe de mantenimiento, tecnología

  Seguridad física y del entorno

Áreas seguras

Perímetro de seguridad física

Áreas de despacho y carga

Visita al centro de cómputo

- **Responsable / área:** Responsable de SI/Jefe de oficina de tecnología

  Políticas de seguridad de la información

  Organización de la seguridad de la información

  Seguridad de los recursos humanos

  Criptografía

  Seguridad física y del entorno

  Seguridad de las operaciones

  Procedimientos operacionales y responsabilidades

  Procedimientos de operación documentados

  Gestión de cambios

  Gestión de capacidad

  Separación de los ambientes de desarrollo, pruebas y operación

  Protección contra códigos maliciosos

  Copias de respaldo

  Registro y seguimiento

  Registro de eventos

  Protección de la información de registro

  Registros del administrador y del operador

Sincronización de relojes

Control de software operacional

Instalación de software en sistemas operativos

Gestión de la vulnerabilidad técnica

Gestión de las vulnerabilidades técnicas

Restricciones sobre la instalación de software

Consideraciones sobre auditorías de sistemas de información

Controles sobre auditorías de sistemas de información

Seguridad de las comunicaciones

Gestión de la seguridad de las redes

Transferencia de información

Adquisición, desarrollo y mantenimiento de sistemas

Requisitos de seguridad de los sistemas de información

Seguridad en los procesos de desarrollo y de soporte

Datos de prueba

Gestión de incidentes de seguridad de la información

Alcance MSPI (modelo de seguridad y privacidad de la información)

Identificación y valoración de riesgos

Tratamiento de riesgos de seguridad de la información

Toma de conciencia, educación y formación en la seguridad de la información

Planificación y control operacional

Implementación del plan de tratamiento de riesgos

Indicadores de gestión del MSPI

Plan de seguimiento, evaluación y análisis del MSPI

Evaluación del plan de tratamiento de riesgos

Plan de seguimiento, evaluación y análisis del MSPI

Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos interdisciplinarios de la entidad

Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información.

La entidad conoce su papel dentro del estado colombiano, identifica y comunica a las partes interesadas la infraestructura crítica.

Las prioridades relacionadas con la misión, objetivos y actividades de la entidad son establecidas y comunicadas.

La gestión de riesgos tiene en cuenta los riesgos de ciber seguridad

Detección de actividades anómalas

Respuesta a incidentes de ciber seguridad, planes de recuperación y restauración

- **Responsable / área:** Responsable de tics/Monitores

  Teletrabajo

  Manejo de medios

  Derechos de propiedad intelectual.

  Control de acceso

  Seguridad de las operaciones

  Procedimientos operacionales y responsabilidades

  Copias de respaldo

Control de software operacional

Consideraciones sobre auditorías de sistemas de información

Seguridad de las comunicaciones

Gestión de la seguridad de las redes

Transferencia de información

Adquisición, desarrollo y mantenimiento de sistemas

Gestión de incidentes de seguridad de la información

Plan y estrategia de transición de ipv4 a ipv6

Implementación del plan de estrategia de transición de ipv4 a ipv6

Redundancias

- **Responsable / área:** Calidad/ Jefe de oficina de tecnología

  Procedimientos de control documental del MSPI

Fuente: Instrumento de evaluación MSPI MINTIC

4.3.5 Inventario de activos e Identificación y valoración de riesgos:

Para la realización del inventario de activos y la identificación y valoración del riesgo se tomó en cuenta la metodología de la Guía de gestión de riesgos del MINTIC, donde se establece la "Matriz de Calificación, Evaluación y respuesta a los Riesgos" (MINTIC, 2016) de la siguiente manera:

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Figura 4. Matriz de Calificación, Evaluación y respuesta a los Riesgos

4.3.5.1 Inventario de activos.

Se identificaron 13 activos generales del sistema de gestión de la seguridad de la información para la Universidad Popular del Cesar Seccional Aguachica, estos compilan tres grandes procesos Alta dirección, Gestión tecnológica y Gestión administrativa y financiera. Ver apéndice 8.

4.3.5.2. Identificación de riesgos.

Se identificaron 53 riesgos generales del sistema de gestión de la seguridad de la información para la Universidad Popular del Cesar Seccional Aguachica, asociados a los procesos Alta dirección, Gestión tecnológica y Gestión administrativa y financiera. Ver apéndice 9.

4.3.5.3 Identificación de Controles.

Se identificaron 51 riesgos generales del sistema de gestión de la seguridad de la información para la Universidad Popular del Cesar Seccional Aguachica, asociados a los riesgos de los procesos Alta dirección, Gestión tecnológica y Gestión administrativa y financiera. Ver apéndice 10.

4.3.6 Plan de capacitación

Como parte del establecimiento del sistema de gestión de seguridad de la información, es preciso diseñar un plan de capacitación para los procesos de alta dirección, gestión administrativa y financiera y gestión tecnológica, con el fin de crear una cultura de seguridad de la información. Para esto se propone el siguiente esquema de capacitaciones:

Tabla 16.

Plan de capacitación sistema de seguridad de la información 2018

Plan de Capacitación Sistema de Seguridad de la Información 2018																
Universidad Popular Del Cesar Seccional Aguachica																
Dependencias	**Necesidades de capacitacion**									**Soluciones de capacitacion**						
	Áreas temáticas	**Población objetivo por nivel**								**Modalidad de capacitación**	**Oferentes**	**Costos**	**Costos totales**	**Intensidad horaria**	**Fecha de ejecucion**	
		Prioridad	**Directivo**	**Asesor**	**Profesion**	**Técnico**	**Asistencia**	**Comité de**	**Docentes**							
	Políticas de seguridad y privacidad de la información	X	X	X	X	X	X	X	X	Seminario Taller	Sede Principal	-	-	120 horas	Primer o Segundo semestre de 2018	
	Reporte de incidentes de seguridad de la información		X	X	X				X	Seminario Taller	Sede principal	-	-	60 horas	Primer o Segundo semestre de 2018	
	Seguridad de las contraseñas, los controles del software malicioso, y los		X	X	X					Curso	Sede Principal	-	-	60 horas	Primer o Segundo semestre de 2018	

Plan de Capacitación Sistema de Seguridad de la Información 2018

Universidad Popular Del Cesar Seccional Aguachica

Dependencias	Necesidades de capacitacion									Soluciones de capacitacion					
	Áreas temáticas	Población objetivo por nivel								Modalidad de capacitación	Oferentes	Costos	Costos totales	Intensidad horaria	Fecha de ejecucion
		Prioridad	Directivo	Asesor	Profesion	Técnico	Asistencia	Comité de	Docentes						
	escritorios limpios														
	Equipo Especialización en Auditoria de Sistemas														

Como más adelante se puede ver, por medio del tercer objetivo se logró implementar la primera capacitación en el área temática Políticas de seguridad y privacidad de la información, implementando así el 33% de este plan de capacitación. Realizar una prueba piloto utilizando las políticas del sistema de gestión de la seguridad de la información (SGSI) en la oficina de Tecnologías de la Información.

4.4 Realizar una prueba piloto utilizando las políticas del sistema de gestión de la seguridad de la información (SGSI) en la oficina de tecnologías de la información.

4.4.1 Contexto de la oficina TI de la UPC Seccional Aguachica

La universidad popular del Cesar Seccional Aguachica, cuenta dentro de su estructura funcional con diferentes áreas administrativas que soportan los procesos de apoyo para así alcanzar la consecución de su misión y sus objetivos misionales. Dentro de estas áreas se encuentra la función que cumple el profesional ANALISTA DE SISTEMAS, de acuerdo al manual de funciones RESOLUCION RECTORAL 022 DEL 16 ENERO. 2018, la cual reza en el literal 1. "Velar por el manejo y utilización del Software y del hardware" y en el literal 6. Colaborar en la adecuada administración de los recursos informáticos.

Por otra parte para garantizar el manejo técnico cuenta con prestación de servicios de un profesional en Ingeniería de Sistemas que cumple con las siguientes actividades específicas,

- Atender y realizar mantenimiento a los servicios de la Red LAN de la Seccional de Aguachica de la Universidad Popular del Cesar, así como también, realizar acciones preventivas para mejorar su rendimiento.
- Solucionar las fallas en los servicios de la Red LAN de la Seccional de Aguachica de la Universidad Popular del Cesar.
- Realizar recomendaciones para la mejora de los servicios de la Red LAN de la Seccional.
- Segmentación de servicios de la Red LAN de la Seccional
- Reinstalación de aplicaciones y reconfiguración de servidores
- Instalación y configuración de nuevos equipos de la plataforma de Red de área local
- Solución a los problemas de red en su nivel físico (cableado o terminaciones dañadas o sucias, atenuación excesiva de la señal, insuficiente ancho de banda para el cableado, interferencia inalámbrica entre otros.
- Solución a los problemas en el nivel de red Ethernet e IP: identificación de dispositivos de red defectuosos, configuraciones de dispositivo incorrectas o no óptimas, problemas de autenticación y asociación, ancho de banda de red insuficiente.
- Solución a fallas a nivel de Switches y VLAN causados por inscripción de VLAN asignada incorrectamente y problemas de prioridad del tráfico (CoS/QoS).
- Capacitación y entrenamiento al recurso humano que la seccional disponga para la solución de problemas.
- Informar detalladamente sobre las fallas o las configuraciones aplicadas y con recomendaciones para la mejora de los servicios.

También se cuenta con un equipo de monitores que apoyan el desarrollo de las actividades de manejo técnico.

4.4.2 Metodología de la prueba piloto

Con el fin de realizar la prueba piloto del sistema de gestión de la de información propuesto, se inició por realizar la correspondiente capacitación en la política de seguridad de la información, esto con el fin de promover en la Seccional una cultura de prevención, seguidamente se estableció para cada premisa de la política un control aplicable a la misma y finalmente se aplicaron los check list de mantenimiento de computadores personales de acuerdo al formato institucional.

Figura 5. Metodología de la prueba piloto

4.4.3 Prueba 1. Capacitación en política de seguridad de la información

El equipo de trabajo de la Especialización en conjunto con el equipo de la oficina TI, coordinó y realizó la capacitación a los funcionarios en la política de seguridad de la información, con el fin de propiciar una cultura y una motivación a la protección de la información que se produce en cada una de las áreas. Ver anexo xxx listado de asistencia. Dentro de la capacitación se abordaron las premisas de dicha política:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, estudiantes, practicantes y usuarios de la UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA
- Garantizar la continuidad del proceso frente a incidentes.
- La UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del proceso, y a los requerimientos regulatorios.

Figura 6. Capacitación en política de seguridad dela información

4.4.4 Prueba 2. Establecimiento de controles en la oficina de TI de acuerdo a la política de seguridad de la información

El equipo de trabajo de la Especialización en conjunto con el equipo de la oficina TI, analizó y estableció el ciclo de controles pertinentes para la misma en función de la política de seguridad de la información y definió por medio de acta su responsabilidad en los mismos. Ver Acta de elaboración de controles en el apéndice 11.

Tabla 17.

Controles definidos para la oficina de TI

Premisa de la política	Control	Responsable
Minimizar el riesgo en las funciones más importantes de la entidad	Realizar mantenimiento para prevenir la pérdida o daño de los activos de información	Equipo de tecnologías de la información
Cumplir con los principios de seguridad de la información	Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de	Equipo de tecnologías de la información

Premisa de la política	Control	Responsable
	seguridad de la información y las cumplan	
Mantener la confianza de sus usuarios, socios y empleados	Brindar orientación y soporte para la seguridad de la información de acuerdo a los requisitos de la política	Equipo de tecnologías de la información
Apoyar la innovación tecnológica	Implementar nuevas herramientas para el control y seguimiento de la seguridad de la información	Equipo de tecnologías de la información
Proteger los activos tecnológicos	Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado al sistemas y servicios	Equipo de tecnologías de la información
Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información	Garantizar el cumplimiento de políticas, procedimientos e instructivos en materia de seguridad de la información institucionales	Equipo de tecnologías de la información
Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, estudiantes, practicantes y usuarios	Establecer una estrategia de socialización de la cultura de seguridad de la información por medio de correos institucionales y revisiones periódicas	Equipo de tecnologías de la información
Garantizar la continuidad del proceso frente a incidentes	Reparar y controlar los daños al acceso de la información	Equipo de tecnologías de la información

4.4.5 Prueba 3. Aplicación de los Check list de mantenimiento de computadores personales de acuerdo al formato institucional.

El equipo de trabajo de la Especialización en conjunto con el equipo de la oficina TI, aplico los formatos institucionales PARA EL MANTENIMIENTO DE COMPUTADORES PERSONALES aplicando así el control A.11.2.4 de la norma ISO 27001 el cual establece que “los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad”. Ver apéndice 12 y 13 .

5. Conclusiones

La Universidad Popular del Cesar Seccional Aguachica es una institución de educación superior que cuenta con activos de información, los cuales hacen parte de la producción de la misma, desde sus procesos misionales y de apoyo. Por otra parte cuenta con un equipo de trabajo para el proceso de gestión de tecnologías, que consta de un Analista de sistemas, un Ingeniero de Soporte y monitores que cumplen labores auxiliares.

Del primer objetivo se puede concluir que las medidas que se implementan para salvaguardar la integridad, disponibilidad y confidencialidad de la información que se manejan, no están debidamente estructuradas y ni basadas en políticas de seguridad de la información establecidas por la alta gerencia, que permitan proteger mediante directivas el bien más importante para la institución y así poder cumplir con los objetivos misionales como razón de ser. En ese mismo sentido se concluyó que existen necesidades de índole documental, humano, de infraestructura y de formación para abordar un sistema de gestión de seguridad de la información en la Universidad Popular del Cesar Aguachica.

En cuanto al segundo objetivo, la determinación de los elementos del estándar ISO 27001, que puedan ser aplicados en la Universidad Popular del Cesar, Seccional Aguachica, la investigación concluyo que se debe iniciar a documentar aquellos que correspondan a la fase de Planificación, donde se incluye el Alcance de un Modelo de Seguridad y Privacidad de la Información, Políticas

de seguridad y privacidad de la información, Procedimientos de control documental, Roles y responsabilidades para la seguridad de la información, Inventario de activos, Identificación y valoración de riesgos y Toma de conciencia, educación y formación en la seguridad de la información.

Para el tercer objetivo, el establecimiento del sistema de gestión de la seguridad de la información en la Universidad Popular Seccional Aguachica se definió la política de seguridad, roles y responsabilidades, así como el inventario de activos asociados a los procesos de alta dirección gestión tecnológica y gestión administrativa y financiera. En total científica varón 13 activos de información general, se realizó la identificación de riesgos estableciendo 53 riesgos y 51 controles asociados. Por otra parte se elaboró un plan de capacitación para promover la cultura de la seguridad de información ajustada a la realidad financiera de la seccional. En conclusión, este modelo de sistema de gestión de la seguridad de la información permitió a la Seccional contar con herramientas para conocer cuáles son los riesgos, se determinó cómo implementar las políticas del Sistema de Seguridad de la información basada en la Norma ISO 27001.

Finalmente, las pruebas efectuadas en el cuarto objetivo como piloto, permitieron realizar actividades de divulgación de la política de la seguridad de la información, articular esfuerzos con los encargados de los procesos de tecnologías, con lo cual se gestiona un mejor manejo en los procesos asociados a los sistemas de información y por último la verificación y aplicación de los procedimientos institucionales en cuanto al mantenimiento de los equipos de cómputos.

6. Recomendaciones

El equipo de investigación del presente trabajo se permite presentar de manera respetuosa, las siguientes recomendaciones respecto al manejo de la seguridad de la información en la Universidad Popular del Cesar Seccional Aguachica:

Se debe reconocer la importancia del establecimiento de un modelo de seguridad de la información, teniendo en cuenta la responsabilidad social que por su misión tiene la universidad con el estado y con la comunidad

Se debe realizar un esfuerzo financiero para establecer de manera formal el sistema de gestión de seguridad de la información

La seccional se debe articular con el proceso de gestión de tecnología de la sede central de Valledupar

Se debe promover la formación y capacitación con todos los actores de la comunidad académica en los temas de seguridad de la información

Finalmente, se debe garantizar la confiabilidad y veracidad de toda la información producida en las áreas y procesos de la Universidad Popular del Cesar Seccional Aguachica, para lo cual se recomienda seguir los principios de la política de seguridad establecida en este documento.

Referencias Bibliográficas

ALVAREZ ZURITA, F. M., & GARCIA GUZMAN, P. (2007). *Implementacion de un sistema de gestion de seguridad de la informacion basado en la norma ISO 27001, para la intranet de la corporacion metropolitana de salud.* Quito.

AYALA GONZALES, G., & ALBERTO, J. (2011). *Guia de buenas practicas de seguridad de la informacion en contextos de Micro, Pequeñas y Medianas empresas de la region.* Pereira.

CONGRESO DE COLOMBIA. (14 de 02 de 2009). *LEY 1273 DEL 2009*. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

CORDOBA SUAREZ, A. E. (2015). *Diseño e implementacion de un SGSI para el area de informatica de la curaduria urbana segunda de pasto bajo la norma ISO/IEC 27001*. Pasto.

DNV-GL. (S.F). *ISO 27001 - Sistema de Gestión de Seguridad de la Información*. Obtenido de https://www.dnvgl.es/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327

GUERRERO MELO, J., & SUAREZ CASTRELLON, F. J. (2016). *PLANEACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION APLICANDO LA NORMA ISO 27001:2013 EN AREA CONTABLE DE LA EMPRESA TRANSFORMADORES CDM.* OCAÑA.

HERNANDEZ SAMPIERI, R. -F.–B. (2010). *"Metodología de la investigación.* Mac Graw Hills/Interamericana Editores.

INNOVACION UNAL. (14 de 08 de 2017). *LEY 44 DE 1993*. Obtenido de DERECHOS DE AUTOR: http://innovacion.unal.edu.co/fileadmin/recursos/innovacion/docs/normatividad_pi/ley44_1993.pdf

ISO 27001. (2013). TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS.

ISO 9000. (2015). *Fundamentos y vocabulario.*

ISO 9001. (2015). Requisitos de un sistema de gestion de calidad.

ISO/IEC 27001. (2013). GESTION DE LA SEGURIDAD DE LA INFORMACION. REQUISITOS.

KOSUTIC, D. (S.F). *Diferencias y similitudes entre ISO 27001 e ISO 27002*. Obtenido de https://advisera.com/27001academy/es/knowledgebase/diferencias-y-similitudes-entre-iso-27001-e-iso-27002/

MENDEZ, C. (1999). *GUÍAS PARA ELABORAR DISEÑOS DE INVESTIGACIÓN EN CIENCIAS ECONÓMICAS, CONTABLES Y ADMINISTRATIVAS.* BOGOTA.

MENESES MARTINEZ, A., RAMIREZ CAMARGO, E. A., MERCHAN VILLALBA, M. A., & SUAREZ DE LA CRUZ, Y. (2017). *Diseño del sistema de gestion de seguridad SGSI basado en el estandar ISO 27001, para los procesos soportados en el area de sistemas de la camara de comercio de Aguachica, Cesar.* Aguachica.

MinTic. (2016). *Elaboración de la política general de seguridad y privacidad de la información*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINTIC. (2016). *GUIA DE GESTION DE RIESGO.* Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (2017). *Fortalecimiento de la gestión TI del estado*. Obtenido de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

PORTAL WEB 27000.org. (S.F). Obtenido de http://www.27000.org/iso-27002.htm

SANJUAN MUÑOZ, W. (2017). EVALUACION DE LA SEGURIDAD DE LA INFORMACION PARA LA TERMINAL DE TRANSPORTES DE LA CIUDAD DE OCAÑA NORTE DE SANTANDER. Ocaña.

UNIVERSIDAD POPULAR DEL CESAR. (2016). *Proyecto Educativo Institucional Acuerdo 011 31 de marzo de 216* . UPC.

UNIVERSIDAD POPULAR DEL CESAR. (2017). *http://aguachica.unicesar.edu.co*. Obtenido de http://aguachica.unicesar.edu.co/index.php?option=com_content&view=article&id=134&Itemid=306%20)

UNIVERSIDAD POPULAR DEL CESAR. (24 de Julio de 2017). *Página web UPC Seccional Aguachica* . Obtenido de http://aguachica.unicesar.edu.co/index.php?option=com_content&view=article&id=134&Itemid=306

URECHE OSPINO, M. E. (2017). *Diseño de politicas de seguridad de la informatica basadas en la norma NTC-IEC 27001:2013 para la universidad de cartagena centro tutorial Mompox Bolivar.* Mompox.

VASQUEZ CASIELLES, R., TRESPALACIOS GUTIERREZ, J., & BELLO ACEBRON, L. (2005). *INVESTIGACION DE MERCADO.* INTERNATIONAL THOMSON.

VILLACIS ESPINOSA, M. L. (2016). *Diseño de un sistema de gestion de la seguridad de la informacion (SGSI) basado en la norma ISO 27001:2013 para la red coorporativa de la empresa ecuatronix.* Quito.

Apéndices

Apéndice A. Carta de inicio de auditoria

Aguachica, 17 de julio de 2017

Recibí: Julio 17/17 11:00am

Ingeniero
ARLEY DOMINGUEZ QUINTERO
Vicerrector General
Universidad Popular del Cesar
Seccional Aguachica

Ref.: Inicio de auditoria

Estimado Ingeniero:

De acuerdo a lo señalado en la referencia, nos es grato informar a usted que conforme al programa de estudio de la Universidad Francisco de Paula Santander Ocaña y el trabajo de grado titulado ***DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, EN LA UNIVERSIDAD POPULAR DEL CESAR, SECCIONAL AGUACHICA,*** *para obtener el título de Especialistas en Auditoria de Sistemas, corresponde efectuar una auditoría en las dependencias de Registro y Control Académico, Recursos Bibliográficos, Dirección Administrativa y Financiera y Direcciones de Departamento en cuanto a seguridad informática, pues son las dependencias más vulnerables y expuestas a cualquier alteración en los sistemas de información, puesto que los estudiantes, docentes y personal externo tiene acceso a estas.*

Particularmente el grupo de estudiantes, integrado por las siguientes personas:

Nombre completo	***Código***
Roger Oswaldo Lizcano Ruiz	*850214*
Didier Fernando Guerrero Sumalave	*850219*
Andrea Johana Navarro Claro	*850215*
Laura Marcela Felizzola Conde	*850216*

Esta auditoría, está planificada para realizar su ejecución desde el 01 al 16 de agosto de la presente anualidad y tiene como objetivo diagnosticar los requisitos de las partes interesadas

pertinentes a la seguridad de la información, con el fin de comprender las necesidades y expectativas referentes a esta, y determinar una línea base para el diseño del sistema de gestión de la seguridad de la información para la Universidad Popular del Cesar – Seccional Aguachica, y con esto llevar a cabo una evaluación critica de las áreas involucradas mediante técnicas y procedimientos que permitan constatar si las actividades del sistema son correctas y están de acuerdo con la normativa institucional y general (basado en el estándar ISO 27001) que están establecidas y dar sugerencias a soluciones estratégicas de los hallazgos.

En disposición de ampliar cualquier información.

Atentamente,

Roger Oswaldo Lizcano Ruiz

Didier Fernando Guerrero Sumalave

Andrea Johana Navarro Claro

Laura Marcela Felizzola Conde

Apéndice B. Encuestas administrativo

SEP 2017)RIA SGSI PARA ADMINISTRATIVOS UPCSA

ENCUESTA.

Objetivo. Determinar el grado de conocimiento y el manejo de políticas de seguridad de la información para los administrativos de la Universidad Popular del Cesar Seccional Aguachica.

Población. 31 funcionarios.

Cantidad de preguntas 11.

✓

Marque con una (X) o un la respuesta que considere de su elección.

1. ***¿Conoce si la Universidad Popular del Cesar seccional Aguachica tiene implementado un Sistema de Gestión de seguridad de la información para los procesos que involucren el tratamiento de los datos generados?***

SI NO NS/NR

2. ***¿Dentro de los procesos que competen a su cargo o dependencia existen metodologías de respaldo de información que puedan evitar la pérdida o daño de la misma en casos especiales o fallas de su equipo de cómputo?***

SI NO NS/NR

3. ***¿Con que regularidad realiza el cambio de contraseña para su equipo de cómputo, correo institucional o cuentas que utilice en el desarrollo de sus labores diarias?***

1 VEZ A LA SEMANA ☐ 1 VEZ AL MES ☐ DE 3 A 6 MESES ☐ NUNCA ☐

4. ***¿Las contraseñas que normalmente utiliza en sus cuentas se forman con el conjunto de caracteres en minúscula, mayúscula, números y caracteres especiales?***

CON MUCHA FRECUENCIA ☐ CON POCA FRECUENCIA ☐ NUNCA ☐

5. ***¿Conoce si existen políticas de seguridad para el correcto mantenimiento preventivo y correctivo de su equipo de cómputo, Software de aplicativo y Sistema operativo funcional?***

☐ SI NO ☐ NS/NR ☐

6. ***¿Dentro de la institución se realizan procesos de gestión de riesgos para mitigar posibles incidentes y fortalecer las vulnerabilidades relacionadas a la gestión de la seguridad de la información?***

☐ CON MUCHA FRECUENCIA ☐ CON POCA FRECUENCIA ☐ NUNCA

7. ***¿Tiene conocimiento de si en su equipo de cómputo se encuentra instalado un software de antivirus y este se encuentra en estado activo y actualizado?***

SI ☐ NO ☐ NS/NR ☐

8. ***¿La institución cuenta con un departamento de sistemas encargado de priorizar y mantener procesos de gestión de la seguridad de la información, mitigación de riesgos y control de datos?***

SI NO NS/NR

9. ***¿La institución brinda mediante capacitaciones periódicas conocimiento sobre políticas de seguridad de la información, Gestión del riesgo y posibles delitos o fraudes de los que podría ser víctima?***

CON MUCHA FRECUENCIA CON POCA FRECUENCIA NUNCA

10. ***¿Cómo funcionario de la institución se le realiza la solicitud del carnet en la entrada por parte del equipo de vigilancia contratado?***

CON MUCHA FRECUENCIA CON POCA FRECUENCIA NUNCA

11. ***¿Durante los últimos meses ha recibido correos sospechosos o alertas de posibles virus y***

SI NO NS/NR

Apéndice C. Encuesta analista de sistemas

SEP 2017)RIA SGSI DE LA UPCSA

ENTREVISTA.

Objetivo. Dar una evaluación sobre los aspectos relacionados con la usencia del departamento de sistemas de la Universidad Popular del Cesar Seccional Aguachica.

Población. (Analista de sistemas de la Universidad Popular del Cesar Seccional Aguachica).

Cantidad de preguntas 5.

1. ***¿Dentro de la Universidad Popular del Cesar se ha planteado la posibilidad y viabilidad de contar con un departamento de sistemas y un Data center centralizado para mejorar y garantizar metodologías que controlen incidentes y riesgos latentes en contra de la seguridad de la información?***

2. ***¿De qué manera se controla el acceso a los rack de comunicación de la UPCSA, quien maneja las llaves y de qué manera se lleva el registro de cada acceso y modificación?***

3. ***¿Qué tipo de controles se utilizan para evitar que personas que no cuentan con autorización ingresen a áreas restringidas dentro de la Universidad Popular del Cesar Seccional Aguachica?***

4. ***¿Realiza revisiones de seguridad física a las instalaciones, con qué frecuencia las realiza?***

5. ***¿Realiza backups de la configuración de equipos de comunicación como Router y Switches para posteriores restauraciones?***

6. ***¿Lleva control de cambios de Hardware y Software en los mantenimientos preventivos y correctivos que realiza?***

7. ***¿De qué manera realiza el borrado de información de manera segura, cuenta con procedimientos ya establecidos?***

8. ***¿Existen controles para determinar si se habilita o deshabilita un punto de datos dentro del cableado estructurado, todos se encuentra por defecto habilitados?***

9. ***¿Existe un sistema de monitoreo de video vigilancia en las áreas restringidas de la UPCSA?***

10. ***¿Con que frecuencia realiza mantenimientos a equipos de cómputo, impresoras y cableado estructurado dentro de la Universidad Popular del Cesar seccional Aguachica?***

11. ¿Cómo se control el ingreso de otros equipos de cómputo por parte de usuarios externos o visitantes?

Apéndice D. Encuesta Jefe de laboratorio de sistemas

SEP 2017 ORIA SGSI DE LA UPCSA

ENTREVISTA.

Objetivo. Dar una evaluación sobre los aspectos relacionados con la organización de seguridad de la información de la Universidad Popular del Cesar Seccional Aguachica.

Población. (Jefe de laboratorios de informática Universidad Popular del Cesar Seccional Aguachica)

.

Cantidad de preguntas 5.

1. ***¿Dentro de los laboratorios de informática existen políticas de seguridad para evitar que los usuarios usen los equipos de cómputo para tratar de vulnerar áreas administrativas?***

2. ***¿Se cuenta con un cronograma de actividades para realizar tareas de mantenimiento preventivo y correctivo a los equipos de cómputo de los laboratorios destinados al uso general de los estudiantes y docentes de la seccional?***

3. ***¿El acceso al nodo de conexión de fibra y Router de la sala de informática es registrado en un formato al igual que los cambios generados dentro del mismo?***

4. ***¿El acceso a los laboratorios es monitoreado por un sistema de cámaras de vigilancia, donde se registre los acontecimientos y accesos a los equipos de conexión dentro del rack?***

5. ***¿Quién brinda acceso y manejo de las llaves de los laboratorios?***

6. ***¿Se registra en formatos el ingreso de cada usuario, y se monitorean las actividades que realiza durante su estadía dentro de los laboratorios de informática?***

7. ***¿Qué proceso se realiza para la selección y asignación de los monitores de laboratorio?***

Apéndice E. Situaciones encontradas en la auditoria

Institución	Áreas auditadas	Día	Mes	Año
Universidad Popular del Cesar Seccional Aguachica	**Oficina de Registro y Control – Financiera – Biblioteca – Laboratorios de informática – Coordinaciones de programas – Investigación- Encargado del área de Soporte y TIC**	**11**	**08**	**2017**

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
001	No existen unas políticas de seguridad de la información adecuadas para el tratamiento de seguridad confidencial de la UPCSA.	Falta de conocimiento de la importancia de establecer las políticas de seguridad de la información para tener un nivel alto de seguridad en el uso de la información.	Establecer e implementar las políticas de seguridad de la información.	2017	Vicerrectoría Ingeniero de soporte y apoyo TIC Director administrativo y financiero
002	Falta de buenas prácticas en el uso de	Falta de conocimiento de buenas prácticas de	Capacitación y socialización al personal de	1/09/2017 Capacitación al	Ingeniero de soporte y apoyo

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	contraseñas de acceso para los equipos y Sistema de información Academusoft en las distintas dependencias de la UPCSA	seguridad de la información.	la dependencia.	personal administrativo.	TIC
003	Ausencia de realización de copias de seguridad y restauración (Backus) de información en dependencias como Registro y control, Financiera, biblioteca y Coordinaciones.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Capacitación y socialización al personal de la dependencia. Creación de procedimientos para la generar Backus.	1/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
004	Malas condiciones físicas y de espacio en la oficina de Registro y Control, teniendo en cuenta la importancia de la información que	Lugar de trabajo y almacenamiento físico pequeño.	Trasladar a un lugar con más espacio y mejor organización para la dependencia.	2017	Vicerrectoría

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	se almacena físicamente.				
005	Malos manejos en los almacenamientos de información en medios magnéticos en las diferentes dependencias de la UPCSA.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Capacitación y socialización al personal de la dependencia.	1/09/2017	Ingeniero de soporte y apoyo TIC
006	Se encuentra un incumplimiento en algunas funciones de los administrativos.	Desconocimiento del manual de funciones y procedimientos.	Socialización al personal de la dependencia.	11/8/2017 Reunión con los administrativos de la dependencia,	Director administrativo y financiero
007	No se cuenta con un manual de seguridad de la información aprobado e implementado para esta dependencia.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Creación de un manual de seguridad de la información.	2017	Vicerrectoría Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
008	Uso de datos personales en contraseñas para acceso a equipos de cómputo y sistema de información Academusoft.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Socialización al personal de la dependencia.	1/09/2017 Capacitación al personal administrativo.	Ingeniero de soporte y apoyo TIC
009	Falta de políticas para la seguridad en la entrada de personas que no están autorizadas a manipular información de la dependencia.	Falta de políticas para el control y entrada de personal no autorizado a la dependencia de Registro y Control.	Creación de una política de ingreso y manipulación de la información.	2017	Vicerrectoría Ingeniero de soporte y apoyo TIC
010	Se Observó que no existe un control pertinente para el manejo de Dispositivos como Pendrive o Quemadoras, Lo comprende una falla de seguridad importante.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Creación de un control para el no uso de Pendrive y quemadoras de CD o DVD.	12/08/2017	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
011	No existe un sistema de seguridad o video vigilancia para las áreas donde se comprometa la información de mayor importancia de la UPCSA.	Falta de políticas de seguridad que permitan el monitoreo de áreas importantes dentro de la UPCSA.	Propuesta de implementación sistema de video seguridad.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
012	No se cuenta con un sistema de contingencia para la continuidad de la energía eléctrica en la UPCSA en caso de una falla de este tipo.	Falta de políticas que mejoren el objetivo de continuidad del proceso, evitar pares en los servicios de las instalaciones.	Socialización con el área administrativa para proponer una propuesta de implementación.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero Jefe de servicios generales.
013	La UPCSA en algunas dependencias y equipos de cómputo no cuenta con sistemas de UPS que permita el	Falta de conocimiento de buenas prácticas de seguridad de la información.	Presentar propuesta para la adquisición en 2018 de UPS para las oficinas de la UPCSA.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	funcionamiento por lo menos de 10 min para realizar el correcto cierre y apagado de las aplicaciones en caso de una falla eléctrica.				financiero
014	La UPCSA no cuenta con un equipo de hardware para realizar filtrado de contenido web.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Incluir dentro del presupuesto, la necesidad de adquirir un sistema de filtrado Web, Socialización con el encargado del departamento de Sistemas de la sede Principal.	18/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero Jefe del departamento Sistemas sede principal
015	La UPCSA no cuenta con un **DATA CENTER** centralizado, cuenta con 5 nodos de	Falta de políticas de centralización de información y datos.	Presentar propuesta para la adecuación de un espacio físico para el departamento de sistemas que tenga	15/09/2017	Ingeniero de soporte y apoyo TIC Director

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	comunicaciones en diferentes lugares de la institución, lo que no permite poder monitorear de mejor manera las actividades dentro de la red de datos y demás.		conexión con el Rack principal y permitir el monitoreo de los recursos de la UPCSA.		administrativo y financiero
016	No existe una oficina de control interno dentro de la UPCSA que garantice que los administrativos estén realizando las labores del manual de funciones de manera correcta.	No existe comité seccional de control interno.	Crear un comité de control interno para la UPCSA, que permita la conexión directa con control interno de la ciudad de Valledupar.	2017	Director administrativo y financiero
017	La UPCSA no cuenta con un sistema de alarma y detección de humo que esté conectada a la central de bomberos.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Socialización con el área administrativa para proponer una propuesta de implementación.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
					financiero Jefe de servicios generales.
018	No se tiene claridad por parte de los administrativos para la no instalación de software licenciado no adquirido por la UPCSA y de uso prohibido en los equipos de cómputo.	Desconocimiento del listado de software con el que cuenta la UPCSA.	Socialización del listado de software licenciado, capacitación sobre software libre y licenciado.	1/09/2017 Capacitación al personal administrativo.	Ingeniero de soporte y apoyo TIC Administrativos UPCSA.
019	No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Crear un comité de mejora de las políticas de la seguridad de la información, crear un procedimiento de borrado seguro.	2017	Director administrativo y financiero Administrativos UPCSA.
020	No se tiene documentado el control y bitácora para el	Falta de conocimiento de buenas prácticas de seguridad de la	Crear política para el registro de cada acontecimiento dentro de la	2017	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	registro de las actividades o acontecimientos dentro de la red de datos, como fallas en el servicio, direcciones IP'S con alto consumo de ancho de banda.	información.	red que reciba atención y monitoreo.		
021	No se cuentan con políticas de control formal para la trasferencia de información por cualquier medio.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Crear una política para limitar o establecer los correctos procedimientos sobre esta situación.	2017	Ingeniero de soporte y apoyo TIC
022	Nunca se han realizado auditorias de sistemas a la red y cableado estructurado.	Desconocimiento del control y mejora continua que permiten las auditorias en la red.	Desarrollar un plan de auditorías y concienciar a los funcionarios encargados del área de la	2017	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
			importancia de llevar registros de las actividades y Supervisión.		
023	No existe un control de visitantes al momento de ingresar a la UPCSA, no son llevados en acompañamiento por el grupo de vigilancia contratado hacia la dependencia a visitar.	Desconocimiento de las dificultades de permitir el ingreso de personas ajenas a sitios de manejo de información importante sin acompañante.	Crear una política de seguridad para mejor esta situación.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero Jefe de servicio generales.
024	No existen controles como biométricos o bitácoras de acceso a los diferentes Rack de equipos ubicados en distintos puntos de la UPCSA.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Plantear la adquisición para el 2018 de equipos de control biométrico.	Primer trimestre del 2018	Ingeniero de soporte y apoyo TIC Director administrativo y financiero

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
025	La entrada no cuenta con una cámara de seguridad para el control de acceso, grabación y monitorización del personal que ingresa a la UPCSA.	Falta de control de vigilancia como política de seguridad de la institución.	Socialización con el área administrativa para proponer una propuesta de implementación de señalización.	15/09/2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
026	Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás.	Desconocimiento de las políticas de seguridad de señalización.	Plantear la adquisición e implementación de la señalización	Octubre 2017	Director administrativo y financiero Jefe de servicios generales.
027	Los días no laborales se observa que algunos lugares dentro de la UPCSA no cuentan con el respectivo cierre para el no ingreso de estudiantes o invitados,	Falta de control de vigilancia como política de seguridad de la institución.	Crear una política de solicitud de acceso en días no laborales.	15/09/2017	Director administrativo y financiero Jefe de servicios generales

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	lo que genera grandes riesgos en la seguridad de los sistemas de información.				
028	Se observa que el Ingeniero de soporte aunque registra en un informe mensual los cambios o soportes que realiza en las diferentes dependencias, estos cambios de hardware y software no queda registrados en una bitácora o formato de control de cambios.	Falta de conocimiento de buenas prácticas de seguridad de la información.	Crear política de gestión de la seguridad para implementar un procedimiento donde se registren los cambios que se realicen en el hardware y software.	2017	Ingeniero de soporte y apoyo TIC
029	Algunos equipos no cuentan con contraseña de acceso que restrinja a otros usuarios el	Falta de conocimiento de buenas prácticas de seguridad de la información.	Crear una política de seguridad para mejor esta situación.	2017	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	ingreso al sistema operativo.				
030	Los equipos de la UPCSA no cuentan con antivirus licenciado o algún dispositivo de hardware firewall que controle accesos a la red no autorizados, se usa un antivirus gratuito de Microsoft.	Desconocimiento de las protecciones que conlleva usar un antivirus de paga.	Plantear la posibilidad de adquirir un antivirus licenciado para los equipos de la UPCSA.	2017	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
031	Existen los extintores en sitios estratégicos pero no se cuenta con un control de cambios o tiempos en el mantenimiento de los mismos.	Desconocimiento de aprovechamiento del control de estos equipos.	Crear una política de seguridad para controlar el tiempo y cambio de los extintores.	2017	Jefe de servicios generales
032	No existe un plan de contingencia en caso de	Desconocimiento o exceso de confianza por	Crear una política como plan de contingencia para	Octubre – Noviembre del	Director administrativo y

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	emergencias o desastres naturales.	parte de los administrativos de la UPCSA.	evacuación y emergencias.	2017	financiero Jefe de servicios generales
033	No existe un control o bitácora para cambios y accesos a los Rack de comunicaciones (nodos) por parte del encargado del área de Redes de la UPCSA.	Existe demasiada confianza con respecto a las políticas de acceso a los rack de comunicaciones.	Implementar controles de registro o biométricos, plantear la adquisición por parte de la UPCSA de equipo para mejorar este ítem.	2017-2018	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
034	No existen herramientas para la protección contra código malicioso.	Desconocimiento de los controles contra código malicioso ejecutado en el interior y exterior de la UPCSA.	Crear una política de seguridad para mejor esta situación.	2017	Ingeniero de soporte y apoyo TIC
035	No se realiza gestión y registro de incidentes de la seguridad de la información.	Falta de control y políticas de las seguridad para este evento.	Crear un comité con ayuda del equipo de soporte Tic, para registrar y gestionar distintos tipos de incidentes de seguridad.	Noviembre	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
036	No existe un control de las llaves para el acceso a dependencias importantes, algunos funcionarios cuentan con llaves y copias lo que podría generar problemas de seguridad, por las noches los vigilantes manejan las llaves.	Falta de políticas de control de acceso a las oficinas por parte del equipo de servicios generales y de vigilancia.	Crear un comité para el control y vigilancia de las llaves, así como de las políticas se seguridad con las copias que se le entregan a los funcionarios.	2017	Director administrativo y financiero Jefe de servicios generales
037	No existe una política de cambio de cerraduras para las dependencias importantes y de alto riesgo.	Exceso de confianza para este evento de control.	Implementar una política de cambio en determinado tiempo para asegurar el no uso de copias de las lleves por parte de los administrativos.	2017-2018	Director administrativo y financiero Jefe de servicios generales Contratista de equipo de vigilancia.

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
038	No existe un control para deshabilitar los puertos de red que puedan provocar Riesgo en la conexión de visitantes o personas externas a la UPCSA.	Falta de controles que determinen que puertos deben estar desactivados por ser potenciales puntos de acceso a la red para personal externo e internos.	Crear una política que permita determinar que puertos deben estar en estado off, llevar un control de que uso tiene y que equipos se conectan normalmente en esa área.	2017	Ingeniero de soporte y apoyo TIC
039	No se realiza un cambio periódico a las claves de acceso a la Red Inalámbrica difundidas dentro de la UPCSA.	Demasiada confianza para las políticas de cambio de este evento, las claves tienen más de dos años sin ser cambiadas.	Implementar por parte del analista de sistemas el cambio de las claves con la previa socialización con la alta gerencia.	18/09/2017	Ingeniero de soporte y apoyo TIC
040	No existe un monitoreo y registro permanente de la cantidad de usuarios de la red inalámbrica, durante los momentos de más afluencia dentro de la	Falta de control y políticas de las seguridad para este evento.	Crear una política por parte del equipo de soporte para monitorear en las horas de mayor afluencia dentro del Ruckus la cantidad de IP asignadas para equipos o dispositivos	18/09/2017	Equipo de Soporte.

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	UPCSA.				
041	Se considera que la UPCSA no es demasiado grande por lo cual no se cuenta con un equipo de Firewall para el control del ancho de banda de fibra óptica por lo que se permite que todas las redes accedan al mismo medio.	Falta de control de este medio, los administrativos y procesos académicos importantes se ven afectados por la falta de estas políticas de asignación de canal de fibra.	Crear una solicitud para la adquisición de un equipo de hardware o software que permita restringir en las diferentes Vlans que tano ancho de banda deben usar.	2017-2018	Ingeniero de soporte y apoyo TIC Director administrativo y financiero
042	No existe una oficina de Sistemas o soporte con un equipo de Ingenieros que soporten todo el Sistema de seguridad de la información, dentro de la UPCSA.	Falta de gestión de responsabilidades por parte de la institución para asignar el control de las políticas de seguridad.	Crear como apoyo al departamento de sistemas un equipo de soporte con ingenieros que participen del control de sistema de gestión de seguridad de la información.	2017-2018	Director administrativo y financiero Rector Universidad Popular del Cesar sede principal

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
043	Se observa que en la dependencia de Biblioteca aunque se tienen cámaras de seguridad y se realiza la grabación durante el 80% de las horas laborales, el equipo no tiene normas mínimas de control de acceso y cualquier persona puede acceder a esta información.	Falta de control y políticas de las seguridad para este evento, desconocimiento de las mínimas normas de control y seguridad de acceso al equipo de cómputo.	Socializar e implementar con el jefe de la biblioteca el adecuado uso de contraseñas de acceso y políticas de control al equipo que registra las grabaciones de las cámaras IP de vigilancia en esta dependencia.	19/09/2017	Ingeniero de soporte y apoyo TIC Jefe de Biblioteca
044	No existe dentro de la UPCSA un método de cifrado de información, para las dependencias de manejo de datos de alto riesgo.	Desconocimiento de los posibles robos de datos o accesos no autorizados por parte de personas ajenas a la institución.	Adquirir herramientas que permitan en los momentos que se necesite el cifrado de datos importantes para las dependencias que lo requieran.	2017	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
045	Desconocimiento del uso de la nube y el drive para el almacenamiento seguro de información, como medio externo para evitar problemas de seguridad en los equipos locales.	Falta de conocimiento por parte de los administrativos sobre el manejo de drive y la nube como medio de almacenamiento de información.	Capacitación y socialización sobre manejo de herramientas TIC.	1/09/2017 Capacitación al personal administrativo	Ingeniero de soporte y apoyo TIC Administrativos UPCSA.
046	No existen políticas de control de riesgo en los laboratorios de informática y dependencias para mitigar los incidentes que puedan suceder dentro de la UPCSA.	Desconocimiento de las políticas y controles que pueden mitigar el riesgo dentro los puestos de trabajo y laboratorios de cómputo de la UPCSA.	Crear políticas de mitigación de riesgo para los laboratorios y dependencias.	Octubre y Noviembre	Ingeniero de soporte y apoyo TIC
047	Falta de entrenamiento y capacitación al colectivo de	Desconocimiento sobre políticas de seguridad de la información.	Crear una capacitación para informar sobre gestión de seguridad de la	1/09/2017 Capacitación al personal	Ingeniero de soporte y apoyo TIC

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	administrativos sobre seguridad de la información.		información.	administrativo	Administrativos UPCSA.
048	Falta de políticas de control y detección de Ransomware y malware dentro de la dependencias de la UPCSA.	Exceso de confianza con el desconocimiento sobre correos con virus y codificación de la información sobre Ransomware y malware.	Socialización para informar sobre los distintos tipos de virus y amenazas dentro de la red y equipos de cómputo.	1/09/2017 Capacitación al personal administrativo	Ingeniero de soporte y apoyo TIC Administrativos UPCSA.
049	Falta de políticas de seguridad en el control de acceso y proceso de Subcontratación de servicios y terceros. Los terceros ingresan a áreas restringidas sin recibir primero permiso de la alta gerencia.	Falta de políticas de control de acceso a las oficinas por parte del equipo de servicios generales y de vigilancia.	Crear comité de mejoras para los procesos de subcontratación de terceros y políticas de acceso de los mismos.	18/09/2017	Director administrativo y financiero Jefe de servicios generales
050	No se realiza una inspección de posibles	Falta de políticas de control de acceso de	Crear una política para la revisión en la entrada de	Octubre	Director administrativo y

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
	dispositivos tecnológicos en la entrada cuando ingresan visitantes y personal administrativo.	elementos electrónicos que pueden ocasionar ataques informáticos dentro de la UPCSA.	cualquier tipo de equipo tecnológico como computador, Tablet y elementos extraños de conexión a la red, así mismo crear una anotación respectiva.		financiero Jefe de servicios generales
051	Se observó que en varias ocasiones de la auditoria que no se realiza por parte del servicio de vigilancia contratado la solicitud de carnet o credenciales adecuadas para el ingreso del personal a la UPCSA.	Falta de políticas para la verificación del personal administrativo mediante el carnet.	Crear una política para la verificación y solicitud por parte del equipo de vigilancia del respectivo carnet en la entrada de los administrativos durante las horas laborales.	octubre	Director administrativo y financiero Jefe de servicios generales

Ref.	Situación encontrada	Causas	Solución	Fecha de Solución	Responsable
		Elaborado Por Didier Fernando Guerrero Sumalave Laura Marcela Felizzola Conde Andrea Johanna Navarro Claro Roger Oswaldo Lizcano Ruiz	Aprobado Por Didier Fernando Guerrero Sumalave Laura Marcela Felizzola Conde Andrea Johanna Navarro Claro Roger Oswaldo Lizcano Ruiz		

Apéndice F. Recibido de Oficio de Entrega de dictamen

Aguachica, 25 de septiembre de 2017

Doctora

CARMEN SOCORRO GUZMAN RODRIGUEZ

Vicerrectora General

Universidad Popular del Cesar

Seccional Aguachica

Recibí
Sept 25 /17
Hora: 10:30 am

Estimada doctora

Teniendo en cuenta el proceso de mejora continua que se viene presentando dentro de la Universidad Popular del Cesar, Seccional Aguachica, se realizó la auditoría con el objetivo de detectar gran parte de inconsistencias en relación con el tratamiento de la seguridad de la información dentro de las dependencias donde se utiliza información importante y critica que comprometa los objetivos misionales de la institución, por esta razón se presenta ante usted de manera oficial el resultado obtenido, la cual se practicó desde el 01 de Agosto del 2017 hasta el 16 de Agosto del 2017.

En documento adjunto hacemos entrega del dictamen de dicha auditoría realizada a la Institución.

En espera de ampliar cualquier información.

Atentamente,

Roger Oswaldo Lizcano Ruiz

Laura Marcela Felizzola Conde

Andrea Johana Navarro Claro

Didier Fernando Guerrero Sumalave

Apéndice G. Elementos del componente planificación aplicables a la UPC Seccional Aguachica

Id	Cargo	Item	Descripción	Prueba	Mspi
P.1	Responsable SI	Alcance MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Documento del alcance que debe estar aprobado, socializado al interior de la Entidad, por la alta dirección. 1) Aspectos internos y externos referidos en el 4.1.: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
				capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3.	
				2) Los requisitos referidos en 4.2.:	
				a. Se debe determinar las partes interesadas que son pertinentes al SGSI.	
				b. Se debe determinar los requisitos de las partes interesadas.	
				Nota. Los requisitos	

Id	Cargo	Item	Descripción	Prueba	Mspi
				pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales.	
				3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores	
P.2		Políticas de seguridad y privacidad de la información	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 la partes externas pertinentes	a) Si se definen los objetivos, alcance de la política	componente planificación
				b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad	
				c) Si fue debidamente	

Id	Cargo	Item	Descripción	Prueba	Mspi
				aprobada y socializada al interior de la entidad por la alta dirección	
				Revise si la política: a)Define que es seguridad de la información	
				b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;	
				c) Los procesos para manejar las desviaciones y las excepciones.	
				Indague sobre los responsables designados	

Id	Cargo	Item	Descripción	Prueba	Mspi
				formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.	
P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que:	Formatos de procesos y procedimientos debidamente definidos, establecidos y aprobados por el comité que integre los	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
				sistemas de gestión institucional, por ejemplo el sistema de calidad SGC.	
			a. Esté disponible y adecuado para su uso, cuando y donde se requiere		
			b. Esté protegida adecuadamente.	1) Cómo se controla su distribución, acceso, recuperación y uso	
				2) Cómo se almacena y se asegura su preservación	
				3) Cómo se controlan los cambios	
P.4	Responsable SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	1) Tiene el SGSI suficiente apoyo de la alta dirección? Esto se ve reflejado en comités donde se discutan	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
				temas como la política de SI, los riesgos o incidentes.	
				2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?,	
				3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección)	
				4) Están definidas las	

Id	Cargo	Item	Descripción	Prueba	Mspi
				responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales?	
				5) Están definidos y documentados los niveles de autorización?	
				6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)	
P.5	Responsable SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información,	Inventario de activos de información, revisado y aprobado por la alta Dirección y	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
			y se debe elaborar y mantener un inventario de estos activos.	revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión. De acuerdo a NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su	

Id	Cargo	Item	Descripción	Prueba	Mspi
				misión y objetivos, dada su importancia y riesgos estratégicos.	
P.6	Responsable SI	Identificación y valoración de riesgos	Metodología de análisis y valoración de riesgos e informe de análisis de riesgos	Metodología y criterios de riesgo de seguridad, aprobado por la alta Dirección que incluya: 1. Criterios de Aceptación de Riesgos o tolerancia al riesgo que han sido informados por la alta Dirección. 2. Criterios para realizar evaluaciones de riesgos. a. Cuantas evaluaciones repetidas de riesgos se han realizado y que sus	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
				resultados consistentes, válidos y comparables.	
				b. Que se hayan identificado los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad de la información dentro del alcance.	
				c. Que se hayan identificado los dueños de los riesgos.	
				d. Que se hayan analizado los riesgos es decir:	
				- Evaluado las consecuencias (impacto) potenciales	

Id	Cargo	Item	Descripción	Prueba	Mspi
				si se materializan los riesgos identificados - Evaluado la probabilidad realista de que ocurran los riesgos identificados - Determinado los niveles de riesgo. e. Que se hayan evaluado los riesgos es decir: - Comparado los resultados del análisis de riesgos con los criterios definidos - Priorizado los riesgos analizados para el tratamiento de riesgos.	
P.9	Responsable SI	Toma de conciencia, educación y formación en la seguridad de la	Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas,	Plan de comunicación, sensibilización y capacitación, con los	componente planificación

Id	Cargo	Item	Descripción	Prueba	Mspi
		información	deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	respectivos soportes, revisado y aprobado por la alta Dirección. Buenas prácticas como: a) Desarrollar campañas, elaborar folletos y boletines. b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en	

Id	Cargo	Item	Descripción	Prueba	Mspi
				SI. d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia. e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido. f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base	

Id	Cargo	Item	Descripción	Prueba	Mspi
				(tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios). g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles.	

Apéndice H. .Inventarios de activos procesos generales Alta dirección, Gestión tecnológica y Gestión administrativa y financiera

Clasificación									Criticidad	Propiedad	
Cód.	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**
A-1	Alta dirección	Canales de comunicación	Incluye canales físicos y virtuales	Software	Red	Clasificada	A	1	ALTA	UPC	Oficinas
A-2	Alta dirección	Documentos	Físicas, Digitales y Verbales	Información	Oficinas productoras y receptoras de información	Pública	A	1	ALTA	UPC	Oficinas

Clasificación									Criticidad	Propiedad	
Cód.	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**
A-3	Gestión tecnológica	Equipos de cómputo	Incluye todos los tipos de equipos	Hardware	Oficinas productoras y receptoras de información	**Reservada**	**A**	**1**	**ALTA**	UPC	Oficinas
A-4	Gestión administrativa y financiera	Equipos de seguridad	Incluye todos los tipos de equipos	Hardware	Oficinas productoras y receptoras de información	**Reservada**	**A**	**1**	**ALTA**	UPC	Oficina tecnología
A-5	Gestión tecnológica	Equipos Tecnológicos	Incluye todos los tipos de equipos	Hardware	Oficinas productoras y receptoras de información	**Clasificada**	**A**	**1**	**ALTA**	UPC	Oficina tecnología
A-6	Gestión administrativa y financiera	Información académica y financiera	Físicas, Digitales y Verbales	Información	Oficinas productoras y receptoras de información	**Reservada**	**A**	**1**	**ALTA**	UPC	Dirección administrativa y financiera

Clasificación									Criticidad	Propiedad	
Cód.	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**
A-7	Gestión administrativa y financiera	Infraestructura física y tecnológica	Incluye todos los tipos de equipos	Hardware	Instalaciones de la UPC	Clasificada	A	1	ALTA	UPC	Dirección administrativa y financiera
A-8	Gestión tecnológica	Medios de almacenamiento extraíbles	Incluye todos los tipos de equipos	Hardware	Instalaciones de la UPC	Clasificada	A	1	ALTA	UPC	Oficinas
A-9	Gestión tecnológica	Nodos de comunicaciones	Físicas, Digitales y Verbales	Software	Instalaciones de la UPC	Clasificada	A	1	ALTA	UPC	Oficina tecnología
A-10	Alta dirección	Recurso humano	Empleados	Recurso humano	Instalaciones de la UPC	Pública	A	1	ALTA	UPC	Dirección administrativa y financiera

Clasificación									Criticidad	Propiedad	
Cód.	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**
A-11	Gestión tecnológica	Red de datos	Herramienta	Software	Instalaciones de la UPC	**Reservada**	**A**	**1**	**ALTA**	UPC	Oficina tecnología
A-12	Gestión administrativa y financiera	Servicios públicos	Incluye los necesarios para los sistemas de información	Otro	Instalaciones de la UPC	**Pública**	**A**	**2**	**ALTA**	UPC	Dirección administrativa y financiera
A-13	Gestión tecnológica	Software	Herramienta	Software	Oficinas productoras y receptoras de información	**Clasificada**	**A**	**1**	**ALTA**	UPC	Oficina tecnología

Apéndice I. Identificación de riegos procesos generales Alta dirección, Gestión tecnológica y Gestión administrativa y *financiera*

Código	Activo	RIESGO	Calificación		Tipo	Evaluación Zona de Riesgo
			Probabilidad	Impacto		
R-1	Canales de comunicación	No se cuentan con políticas de control formal para la trasferencia de información por cualquier medio.	3	4	Integridad	**E**
R-2	Canales de comunicación	No se realiza un cambio periódico a las claves de acceso a la Red Inalámbrica difundidas dentro de la UPCSA.	3	4	Disponibilidad	**E**
R-3	Canales de comunicación	No existe un monitoreo y registro permanente de la cantidad de usuarios de la red inalámbrica, durante los momentos de más afluencia dentro de la UPCSA.	4	4	Disponibilidad	**E**
R-4	Canales de comunicación	No se cuenta con un equipo de Firewall para el control del ancho de banda de	3	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
		fibra óptica por lo que se permite que todas las redes accedan al mismo medio.				
R-5	Canales de comunicación	Desconocimiento del uso de la nube y el drive para el almacenamiento seguro de información, como medio externo para evitar problemas de seguridad en los equipos locales.	3	4	Disponibilidad	**E**
R-6	Documentos	No se cuenta con un manual de seguridad de la información aprobado e implementado para esta dependencia.	4	4	Confidencialidad	**E**
R-7	Documentos	No se realiza gestión y registro de incidentes de la seguridad de la información.	3	4	Integridad	**E**
R-8	Documentos	Falta de políticas de seguridad en el control de acceso y proceso de Subcontratación de servicios y terceros.	4	4	Confidencialidad	**E**
R-9	Equipos de computo	Falta de buenas prácticas en el uso de contraseñas de acceso para los equipos y	4	4	Confidencialidad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
		Sistema de información Academusoft en las distintas dependencias de la UPCSA				
R-10	Equipos de computo	Ausencia de realización de copias de seguridad y restauración (Backus) de información en dependencias como Registro y control, Financiera, biblioteca y Coordinaciones.	4	4	Disponibilidad	**E**
R-11	Equipos de computo	Uso de datos personales en contraseñas para acceso a equipos de cómputo y sistema de información Academusoft.	4	4	Confidencialidad	**E**
R-12	Equipos de computo	La UPCSA en algunas dependencias y equipos de cómputo no cuenta con sistemas de UPS que permita el funcionamiento por lo menos de 10 min para realizar el correcto cierre y apagado de las aplicaciones en caso de una falla eléctrica.	4	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
R-13	Equipos de computo	La UPCSA no cuenta con un equipo de hardware para realizar filtrado de contenido web.	4	4	Confidencialidad	**E**
R-14	Equipos de computo	No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos.	3	4	Integridad	**E**
R-15	Equipos tecnológicos	No existen controles como biométricos o bitácoras de acceso a los diferentes Rack de equipos ubicados en distintos puntos de la UPCSA.	3	4	Integridad	**E**
R-16	Equipos de computo	Se observa que el Ingeniero de soporte aunque registra en un informe mensual los cambios o soportes que realiza en las diferentes dependencias, estos cambios de hardware y software no queda registrados en una bitácora o formato de control de cambios.	4	4	Confidencialidad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
R-17	Equipos de computo	Algunos equipos no cuentan con contraseña de acceso que restrinja a otros usuarios el ingreso al sistema operativo.	3	4	Confidencialidad	**E**
R-18	Equipos de computo	Los equipos de la UPCSA no cuentan con antivirus licenciado o algún dispositivo de hardware firewall que controle accesos a la red no autorizados, se usa un antivirus gratuito de Microsoft.	4	4	Integridad	**E**
R-19	Equipos de computo	Falta de políticas de control y detección de Ransomware y malware dentro de la dependencias de la UPCSA.	4	4	Integridad	**E**
R-20	Equipos de seguridad	La UPCSA no cuenta con un sistema de alarma y detección de humo que esté conectada a la central de bomberos.	4	4	Integridad	**E**
R-21	Equipos de seguridad	Existen los extintores en sitios estratégicos pero no se cuenta con un control de cambios o tiempos en el mantenimiento de los mismos.	4	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
R-22	Equipos de seguridad	No existe un plan de contingencia en caso de emergencias o desastres naturales.	4	4	Integridad	**E**
R-23	Equipos de seguridad	La dependencia de Biblioteca aunque se tienen cámaras de seguridad y se realiza la grabación durante el 80% de las horas laborales, el equipo no tiene normas mínimas de control de acceso y cualquier persona puede acceder a esta información.	3	4	Confidencialidad	**E**
R-24	Equipos de seguridad	No existe dentro de la UPCSA un método de cifrado de información, para las dependencias de manejo de datos de alto riesgo.	4	4	Confidencialidad	**E**
R-25	Equipos tecnológicos	No existe un control pertinente para el manejo de Dispositivos como Pendrive o Quemadoras, Lo comprende una falla de seguridad importante.	3	4	Disponibilidad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación Zona de Riesgo
			Probabilidad	Impacto		
R-26	Información académica y financiera	No existen unas políticas de seguridad de la información adecuadas para el tratamiento de seguridad confidencial de la UPCSA.	4	4	Confidencialidad	**E**
R-27	Infraestructura física y tecnológica	Malas condiciones físicas y de espacio en la oficina de Registro y Control, teniendo en cuenta la importancia de la información que se almacena físicamente.	3	4	Integridad	**E**
R-28	Infraestructura física y tecnológica	Falta de políticas para la seguridad en la entrada de personas que no están autorizadas a manipular información de la dependencia.	4	4	Integridad	**E**
R-29	Infraestructura física y tecnológica	No existe un sistema de seguridad o video vigilancia para las áreas donde se comprometa la información de mayor importancia de la UPCSA.	3	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación Zona de Riesgo
			Probabilidad	Impacto		
R-30	Infraestructura física y tecnológica	Nunca se han realizado auditorias de sistemas a la red y cableado estructurado.	4	4	Integridad	**E**
R-31	Infraestructura física y tecnológica	No existe un control de visitantes al momento de ingresar a la UPCSA, no son llevados en acompañamiento por el grupo de vigilancia contratado hacia la dependencia a visitar.	3	4	Integridad	**E**
R-32	Infraestructura física y tecnológica	La entrada no cuenta con una cámara de seguridad para el control de acceso, grabación y monitorización del personal que ingresa a la UPCSA.	4	4	Confidencialidad	**E**
R-33	Infraestructura física y tecnológica	Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás.	3	4	Integridad	**E**
R-34	Infraestructura física y tecnológica	Los días no laborales se observa que algunos lugares dentro de la UPCSA no cuentan con el respectivo cierre para el no ingreso de estudiantes o invitados, lo	4	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
		que genera grandes riesgos en la seguridad de los sistemas de información.				
R-35	Infraestructura física y tecnológica	No existe un control de las llaves para el acceso a dependencias importantes, algunos funcionarios cuentan con llaves y copias lo que podría generar problemas de seguridad, por las noches los vigilantes manejan las llaves.	3	4	Confidencialidad	**E**
R-36	Infraestructura física y tecnológica	No existe una política de cambio de cerraduras para las dependencias importantes y de alto riesgo.	4	4	Confidencialidad	**E**
R-37	Infraestructura física y tecnológica	No existe un control para deshabilitar los puertos de red que puedan provocar Riesgo en la conexión de visitantes o personas externas a la UPCSA.	3	4	Confidencialidad	**E**
R-38	Infraestructura física y tecnológica	No existen políticas de control de riesgo en los laboratorios de informática y	3	4	Integridad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
		dependencias para mitigar los incidentes que puedan suceder dentro de la UPCSA.				
R-39	Infraestructura física y tecnológica	No se realiza una inspección de posibles dispositivos tecnológicos en la entrada cuando ingresan visitantes y personal administrativo.	4	4	Integridad	**E**
R-40	Medios de almacenamiento extraíbles	Malos manejos en los almacenamientos de información en medios magnéticos en las diferentes dependencias de la UPCSA.	4	4	Integridad	**E**
R-41	Nodos de comunicaciones	La UPCSA no cuenta con un **DATA CENTER** centralizado, cuenta con 5 nodos de comunicaciones en diferentes lugares de la institución, lo que no permite poder monitorear de mejor manera las actividades dentro de la red de datos y demás.	3	4	Disponibilidad	**E**
R-42	Nodos de comunicaciones	No existe un control o bitácora para cambios y accesos a los Rack de	4	4	Disponibilidad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación
			Probabilidad	Impacto		Zona de Riesgo
		comunicaciones (nodos) por parte del encargado del área de Redes de la UPCSA.				
R-43	Nodos de comunicaciones	No existen herramientas para la protección contra código malicioso.	4	4	Integridad	**E**
R-44	Recurso humano	Incumplimiento en algunas funciones de los administrativos.	3	4	Integridad	**E**
R-45	Recurso humano	No existe una oficina de control interno dentro de la UPCSA que garantice que los administrativos estén realizando las labores del manual de funciones de manera correcta.	4	4	Confidencialidad	**E**
R-46	Recurso humano	No existe una oficina de Sistemas o soporte con un equipo de Ingenieros que soporten todo el Sistema de seguridad de la información, dentro de la UPCSA.	3	4	Disponibilidad	**E**
R-47	Recurso humano	Falta de entrenamiento y capacitación al colectivo de administrativos sobre seguridad de la información.	4	4	Disponibilidad	**E**

Código	Activo	RIESGO	Calificación		Tipo	Evaluación Zona de Riesgo
			Probabilidad	Impacto		
R-48	Recurso humano	El servicio de vigilancia contratado no realiza la solicitud de carné o credenciales adecuadas para el ingreso del personal a la UPCSA.	3	4	Integridad	**E**
R-49	Red de datos	No se tiene documentado el control y bitácora para el registro de las actividades o acontecimientos dentro de la red de datos, como fallas en el servicio, direcciones IP'S con alto consumo de ancho de banda.	4	4	Integridad	**E**
R-50	Servicios públicos	No se cuenta con un sistema de contingencia para la continuidad de la energía eléctrica en la UPCSA en caso de una falla de este tipo.	4	4	Integridad	**E**
R-51	Software	No se tiene claridad por parte de los administrativos para la no instalación de software licenciado no adquirido por la UPCSA y de uso prohibido en los equipos de cómputo.	3	4	Disponibilidad	**E**

Apéndice J. Identificación de controles procesos generales Alta dirección, Gestión tecnológica y Gestión administrativa y financiera

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-1	Canales de comunicación	No se cuentan con políticas de control formal para la trasferencia de información por cualquier medio.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política para limitar o establecer los correctos procedimientos sobre esta situación.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-2	Canales de Zcomunicación	No se realiza un cambio periódico a las claves de acceso a la Red Inalámbrica difundidas dentro de la UPCSA.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Implementar por parte del analista de sistemas el cambio de las claves con la previa socialización con la alta gerencia.	Correctivo	2	3	M	Asumir el riesgo

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-3	Canales de comunicación	No existe un monitoreo y registro permanente de la cantidad de usuarios de la red inalámbrica, durante los momentos de más afluencia dentro de la UPCSA.	4	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política por parte del equipo de soporte para monitorear en las horas de mayor afluencia dentro del Racks la cantidad de IP asignadas para equipos o dispositivos	Correctivo	1	3	M	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-4	Canales de comunicación	No se cuenta con un equipo de Firewall para el control del ancho de banda de fibra óptica por lo que se permite que todas las redes accedan al mismo medio.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una solicitud para la adquisición de un equipo de hardware o software que permita restringir en las diferentes Vlans que tano ancho de banda deben usar.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-5	Canales de comunicación	Desconocimiento del uso de la nube y el drive para el almacenamiento seguro de información, como medio externo para evitar problemas de seguridad en los equipos locales.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Capacitación y socialización sobre manejo de herramientas TIC.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-6	Documentos	No se cuenta con un manual de seguridad de la información aprobado e implementado para esta dependencia.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Creación de un manual de seguridad de la información.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-7	Documentos	No se realiza gestión y registro de incidentes de la seguridad de la información.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear un comité con ayuda del equipo de soporte Tic, para registrar y gestionar distintos tipos de incidentes de seguridad.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-8	Documentos	Falta de políticas de seguridad en el control de acceso y proceso de Subcontratación de servicios y terceros.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear comité de mejoras para los procesos de subcontratación de terceros y políticas de acceso de los mismos.	Correctivo	1	2	**B**	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-9	Equipos de computo	Falta de buenas prácticas en el uso de contraseñas de acceso para los equipos y Sistema de información Academusoft en las distintas dependencias de la UPCSA	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Capacitación y socialización al personal de la dependencia.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-10	Equipos de computo	Ausencia de realización de copias de seguridad y restauración (Backus) de información en dependencias como Registro y control, Financiera, biblioteca y Coordinaciones.	4	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Capacitación y socialización al personal de la dependencia.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-11	Equipos de computo	Uso de datos personales en contraseñas para acceso a equipos de cómputo y sistema de información Academusoft.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización al personal de la dependencia.	Correctivo	1	3	M	Asumir el riesgo

C-12	Equipos de computo	La UPCSA en algunas dependencias y equipos de cómputo no cuenta con sistemas de UPS que permita el funcionamiento por lo menos de 10 min para realizar el correcto cierre y apagado de las aplicaciones en caso de una falla eléctrica.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Presentar propuesta para la adquisición en 2018 de UPS para las oficinas de la UPCSA.	Correctivo	2	3	M	Asumir el riesgo, Reducir el Riesgo
C-13	Equipos de computo	La UPCSA no cuenta con un equipo de hardware para realizar filtrado	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Incluir dentro del presupuesto, la necesidad de adquirir un sistema de	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		de contenido web.						filtrado Web, Socialización con el encargado del departamento de Sistemas de la sede Principal.					

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-14	Equipos de computo	No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear un comité de mejora de las políticas de la seguridad de la información, crear un procedimiento de borrado seguro.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-15	Equipos tecnológicos	No existen controles como biométricos o bitácoras de acceso a los diferentes Rack de equipos ubicados en distintos puntos de la UPCSA.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Plantear la adquisición para el 2018 de equipos de control biométrico.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

C-16	Equipos de computo	Se observa que el Ingeniero de soporte aunque registra en un informe mensual los cambios o soportes que realiza en las diferentes dependencias, estos cambios de hardware y software no queda registrados en una bitácora o formato de control de cambios.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear política de gestión de la seguridad para implementar un procedimiento donde se registren los cambios que se realicen en el hardware y software.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir
C-17	Equipos de	Algunos equipos no cuentan con contraseña de	3	4	Confidencial	**E**	Reducir el Riesgo, Evitar,	Crear una política de seguridad	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		acceso que restrinja a otros usuarios el ingreso al sistema operativo.					Compartir o Transferir						

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-18	Equipos de computo	Los equipos de la UPCSA no cuentan con antivirus licenciado o algún dispositivo de hardware firewall que controle accesos a la red no autorizados, se usa un antivirus gratuito de Microsoft.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Plantear la posibilidad de adquirir un antivirus licenciado para los equipos de la UPCSA.	Correctivo	1	4	**B**	Asumir el riesgo

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-19	Equipos de computo	Falta de políticas de control y detección de Ransomware y malware dentro de la dependencias de la UPCSA.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización para informar sobre los distintos tipos de virus y amenazas dentro de la red y equipos de cómputo.	Correctivo	1	4	**A**	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-20	Equipos de seguridad	La UPCSA no cuenta con un sistema de alarma y detección de humo que esté conectada a la central de bomberos.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización con el área administrativa para proponer una propuesta de implementación.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-21	Equipos de seguridad	Existen los extintores en sitios estratégicos pero no se cuenta con un control de cambios o tiempos en el mantenimiento de los mismos.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política de seguridad para controlar el tiempo y cambio de los extintores.	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-22	Equipos de seguridad	No existe un plan de contingencia en caso de emergencias o desastres naturales.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política como plan de contingencia para evacuación y emergencias.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

C-23	Equipos de seguridad	La dependencia de Biblioteca aunque se tienen cámaras de seguridad y se realiza la grabación durante el 80% de las horas laborales, el equipo no tiene normas mínimas de control de acceso y cualquier persona puede acceder a esta información.	3	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socializar e implementar con el jefe de la biblioteca el adecuado uso de contraseñas de acceso y políticas de control al equipo que registra las grabaciones de las cámaras IP de vigilancia en esta dependencia.	Correctivo	1	4	**A**	Asumir el riesgo
C-24	Equipos de	No existe dentro de la UPCSA un método de cifrado de	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar,	Adquirir herramientas que permitan en los momentos	Correctivo	1	4	**A**	Asumir el riesgo, Reducir el Riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		información, para las dependencias de manejo de datos de alto riesgo.					Compartir o Transferir	que se necesite el cifrado de datos importantes para las dependencias que lo requieran.					

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-25	Equipos tecnológicos	No existe un control pertinente para el manejo de Dispositivos como Pendrive o Quemadoras, Lo comprende una falla de seguridad importante.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Creación de un control para el no uso de Pendrive y quemadoras de CD o DVD.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-26	Información académica y financiera	No existen unas políticas de seguridad de la información adecuadas para el tratamiento de seguridad confidencial de la UPCSA.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecer e implementar las políticas de seguridad de la información.	Correctivo	2	4	**A**	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-27	Infraestructura física y tecnológica	Malas condiciones físicas y de espacio en la oficina de Registro y Control, teniendo en cuenta la importancia de la información que se almacena físicamente.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Trasladar a un lugar con más espacio y mejor organización para la dependencia.	Correctivo	2	4	**A**	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-28	Infraestructura física y	Falta de políticas para la seguridad en la entrada de personas que no están autorizadas a manipular información de la dependencia.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Creación de una política de ingreso y manipulación de la información.	Correctivo	1	4	**A**	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-29	Infraestructura física y tecnológica	No existe un sistema de seguridad o video vigilancia para las áreas donde se comprometa la información de mayor importancia de la UPCSA.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Propuesta de implementación sistema de video seguridad.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-30	Infraestructura física y tecnológica	Nunca se han realizado auditorias de sistemas a la red y cableado estructurado.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Desarrollar un plan de auditorías y concienciar a los funcionarios encargados del área de la importancia de llevar registros de las actividades y Supervisión.	Correctivo	1	2	**B**	Asumir el riesgo

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-31	Infraestructura física y tecnológica	No existe un control de visitantes al momento de ingresar a la UPCSA, no son llevados en acompañamiento por el grupo de vigilancia contratado hacia la dependencia a visitar.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política de seguridad	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-32	Infraestructura física y tecnológica	La entrada no cuenta con una cámara de seguridad para el control de acceso, grabación y monitorización del personal que ingresa a la UPCSA.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización con el área administrativa para proponer una propuesta de implementación de señalización.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-33	Infraestructura física y	Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Plantear la adquisición e implementación de la señalización	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

C-34	Infraestructura física y tecnológica	Los días no laborales se observa que algunos lugares dentro de la UPCSA no cuentan con el respectivo cierre para el no ingreso de estudiantes o invitados, lo que genera grandes riesgos en la seguridad de los sistemas de información.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política de solicitud de acceso en días no laborales.	Correctivo	1	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir
C-35	Infraestructura física	No existe un control de las llaves para el acceso a dependencias	3	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear un comité para el control y vigilancia de las llaves, así como de las políticas	Correctivo	1	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		importantes, algunos funcionarios cuentan con llaves y copias lo que podría generar problemas de seguridad, por las noches los vigilantes manejan las llaves.						se seguridad con las copias que se le entregan a los funcionarios.					

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-36	Infraestructura física y tecnológica	No existe una política de cambio de cerraduras para las dependencias importantes y de alto riesgo.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Implementar una política de cambio en determinado tiempo para asegurar el no uso de copias de las lleves por parte de los administrativos.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-37	Infraestructura física y tecnológica	No existe un control para deshabilitar los puertos de red que puedan provocar Riesgo en la conexión de visitantes o personas externas a la UPCSA.	3	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política que permita determinar que puertos deben estar en estado off, llevar un control de que uso tiene y que equipos se conectan normalmente en esa área.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-38	Infraestructura física y tecnológica	No existen políticas de control de riesgo en los laboratorios de informática y dependencias para mitigar los incidentes que puedan suceder dentro de la UPCSA.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear políticas de mitigación de riesgo para los laboratorios y dependencias.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

C-39	Infraestructura física y tecnológica	No se realiza una inspección de posibles dispositivos tecnológicos en la entrada cuando ingresan visitantes y personal administrativo.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política para la revisión en la entrada de cualquier tipo de equipo tecnológico como computador, Tablet y elementos extraños de conexión a la red, así mismo crear una anotación respectiva.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir
C-40	Medios de	Malos manejos en los almacenamientos de información en medios	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Capacitación y socialización al personal de la dependencia.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		magnéticos en las diferentes dependencias de la UPCSA.											

C-41	Nodos de comunicaciones	La UPCSA no cuenta con un **DATA CENTER** centralizado, cuenta con 5 nodos de comunicaciones en diferentes lugares de la institución, lo que no permite poder monitorear de mejor manera las actividades dentro de la red de datos y demás.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Presentar propuesta para la adecuación de un espacio físico para el departamento de sistemas que tenga conexión con el Rack principal y permitir el monitoreo de los recursos de la UPCSA.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir
C-42	Nodos de	No existe un control o bitácora para cambios y	4	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar,	Implementar controles de registro o biométricos,	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
		accesos a los Rack de comunicaciones (nodos) por parte del encargado del área de Redes de la UPCSA.					Compartir o Transferir	plantear la adquisición por parte de la UPCSA de equipo para mejorar este ítem.					
C-43	Nodos de	No existen herramientas para la protección contra código malicioso.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política de seguridad	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-44	Recurso humano	Incumplimiento en algunas funciones de los administrativos.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización al personal de la dependencia.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-45	Recurso humano	No existe una oficina de control interno dentro de la UPCSA que garantice que los administrativos estén realizando las labores del manual de funciones de manera correcta.	4	4	Confidencialidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear un comité de control interno para la UPCSA, que permita la conexión directa con control interno de la ciudad de Valledupar.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-46	Recurso humano	No existe una oficina de Sistemas o soporte con un equipo de Ingenieros que soporten todo el Sistema de seguridad de la información, dentro de la UPCSA.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear como apoyo al departamento de sistemas un equipo de soporte con ingenieros que participen del control de sistema de gestión de seguridad de la información.	Correctivo	2	4	**A**	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-47	Recurso humano	Falta de entrenamiento y capacitación al colectivo de administrativos sobre seguridad de la información.	4	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una capacitación para informar sobre gestión de seguridad de la información.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-48	Recurso humano	El servicio de vigilancia contratado no realiza la solicitud de carné o credenciales adecuadas para el ingreso del personal a la UPCSA.	3	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear una política para la verificación y solicitud por parte del equipo de vigilancia del respectivo carnet en la entrada de los administrativos durante las horas laborales.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	Activo	Riesgo	Calificación		Tipo	Evaluación	Medida de Respuesta	controles	tipo de control	Nueva Calificación		Evaluación	Medida de Respuesta
			Probabilidad	Impacto		Zona de Riesgo				Probabilidad	Impacto	Zona de Riesgo	
C-49	Red de datos	No se tiene documentado el control y bitácora para el registro de las actividades o acontecimientos dentro de la red de datos, como fallas en el servicio, direcciones IP'S con alto consumo de ancho de banda.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Crear política para el registro de cada acontecimiento dentro de la red que reciba atención y monitoreo.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-50	Servicios públicos	No se cuenta con un sistema de contingencia para la continuidad de la energía eléctrica en la UPCSA en caso de una falla de este tipo.	4	4	Integridad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización con el área administrativa para proponer una propuesta de implementación.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Cód.	**Activo**	**Riesgo**	**Calificación**		**Tipo**	**Evaluación**	Medida de Respuesta	**controles**	**tipo de control**	**Nueva Calificación**		**Evaluación**	Medida de Respuesta
			Probabilidad	**Impacto**		**Zona de Riesgo**				**Probabilidad**	**Impacto**	**Zona de Riesgo**	
C-51	Software	No se tiene claridad por parte de los administrativos para la no instalación de software licenciado no adquirido por la UPCSA y de uso prohibido en los equipos de cómputo.	3	4	Disponibilidad	**E**	Reducir el Riesgo, Evitar, Compartir o Transferir	Socialización del listado de software licenciado, capacitación sobre software libre y licenciado.	Correctivo	1	3	M	Reducir el Riesgo, Evitar, Compartir o Transferir

Apéndice K. Acta de elaboración de controles

	UNIVERSIDAD POPULAR DEL CESAR	CÓDIGO: 306-110.1-PRO01-FOR03
		VERSIÓN: 1
	ACTA DE REUNIÓN Y SOCIALIZACIÓN	PÁG.: 1 de 3
		FECHA: 13/11/2009

Oficina de tecnologías de información

Empresa: UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA
Proceso: Proyecto Sistema de Gestión de Seguridad de la información
Fecha: 13 DE Diciembre DE 2017
Lugar: SALON 103
Duración (horas): 1 hora 30 Minutos
Participante(s):
PEDRO SOLANO Analista de sistemas UPC Seccional Aguachica
HENRY CONTRERAS RINCÓN Ingeniero de Soporte UPC Seccional Aguachica DIDIER FERNANDO GUERRERO Proponente de proyecto de especialización
ROYER LIZCANO Proponente de proyecto de especialización
LAURA FELIZZOLA Proponente de proyecto de especialización
ANDREA NAVARRO Proponente de proyecto de especialización

TEMAS TRATADOS:

OBJETIVO:

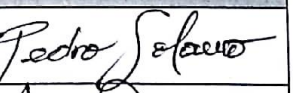
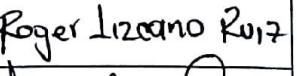
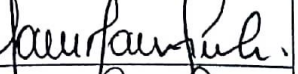
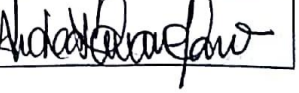
Analizar y establecer el ciclo de controles pertinentes para aplicar la política de seguridad de la información en la oficina de Tecnologías de la información

DESARROLLO

1. Se prepara la reunión agradeciendo al analista de sistemas de la UPC Seccional Aguachica el señor PEDRO SOLANO por su participación en la reunión para consolidar el inicio de un proceso nuevo para la universidad en cuanto a la seguridad de la información.
2. Se aclara que el Ingeniero DIDIER FERNANDO GUERRERO participara en la reunión desde la perspectiva de ingeniero de soporte y como miembro del equipo de la oficina de TI de la seccional.
3. Se inicia por resumir de manera general el objetivo del proyecto, los avances alcanzados a la fecha y la fase de la prueba piloto en la que se encuentra.
4. Se lee la política de seguridad de la información que se estableció para la seccional
5. Por cada punto se realiza una lluvia de ideas, el señor PEDRO SOLANO pregunta cómo se evidenciaría cada parte de esa política a lo que la proponente del proyecto LAURA FELIZZOLA responde que con el seguimiento trimestral que se realiza en la oficina como opción para el seguimiento
6. El Ingeniero DIDIER FERNANDO GUERRERO menciona que los miembros del equipo TI son los que deben velar por aplicar la política, no como una responsabilidad funcional sino como parte inherente de su trabajo
7. La proponente ANDREA NAVARRO propone que para cada premisa de la política se establezca un control asociado a la norma

8. Finalmente el proponente ROYER LIZCANO da un resumen de las ideas así:
Minimizar el riesgo en las funciones más importantes de la entidad/ Realizar mantenimiento para prevenir la pérdida o daño de los activos de información
Cumplir con los principios de seguridad de la información/Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan
Mantener la confianza de sus usuarios, socios y empleados/Brindar orientación y soporte para la seguridad de la información de acuerdo a los requisitos de la política Equipo de tecnologías de la información
Apoyar la innovación tecnológica/ Implementar nuevas herramientas para el control y seguimiento de la seguridad de la información
Proteger los activos tecnológicos/Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado al sistemas y servicios
Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información/ Garantizar el cumplimiento de políticas, procedimientos e instructivos en materia de seguridad de la información institucionales
Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, estudiantes, practicantes y usuarios/Establecer una estrategia de socialización de la cultura de seguridad de la información por medio de correos institucionales y revisiones periódicas
Garantizar la continuidad del proceso frente a incidentes/Reparar y controlar los daños al acceso de la información.

COMPROMISOS	Responsable	Fecha
Se estableció para el plan de acción del año 2018 los controles se incluirían como actividades de la oficina de TI	**Equipo TI UPC Seccional Aguachica**	**2018**

NOMBRE	CARGO	FIRMA
PEDRO SOLANO	Analista de Sistemas	
HENRY CONTRERAS RINCÓN	Ingeniero Soporte TI	
DIDIER FERNANDO GUERRERO	Apoyo Soporte TI	
ROYER LIZCANO	Profesional Universitario	
LAURA FELIZZOLA	Secretaria Grado 19	
ANDREA NAVARRO	Técnico	

Apéndice L. Lista de verificación para el mantenimiento físico de computadores

	UNIVERSIDAD POPULAR DEL CESAR	CÓDIGO: 308-160-PRO04- FOR01
		VERSIÓN: 1
	CHECK LIST PARA EL MANTENIMIENTO FÍSICO DE COMPUTADORES PERSONALES	PÁG.: 1 de 1

FECHA:	15 - Diciembre 2017	USUARIO:	Pedro H. Solano Y.
PLACA No.:	3630	OFICINA:	Sala Informática I

- ☒ 1. Revisar el estado de los cables de poder, cable de video, cable red, conectores RJ45 y canaleta.
- ☒ 2. Verificar si el computador cuenta con equipo de protección eléctrica: UPS, estabilizador. Revisar el estado de los mismos y registrar voltajes de salida, de no tener equipo de protección eléctrica; reportar.
- ☒ 3. Observar si el equipo tiene sellos de seguridad.
- ☒ 4. Revisar el estado del funcionamiento del equipo en cada uno de sus componentes: CPU, Pantalla, Ratón, Teclado y otros periféricos si aplica.
- ☒ 5. Apagar el equipo correctamente, desconectar toma corriente y demás periféricos.
- ☒ 6. Levantar o retirar la tapa de la torre.
- ☒ 7. Descargar la electricidad estática de las manos de quien manipulará el computador.
- ☒ 8. Retirar las memorias RAM y despejar el interior de la torre para facilitar limpieza.
- ☒ 9. Limpiar con sopladora el interior de la CPU incluyendo el interior de la fuente.
- ☒ 10. Limpiar con cepillo seco las ranuras de la memoria RAM.
- ☒ 11. Limpiar con toalla seca y libre de motas la(s) memoria(s) RAM, limpiar sus contactos con un borrador, volver a limpiar con toalla, reinstalar la(s) memoria(s) RAM en el computador, sellar y probar.
- ☒ 12. Volver a colocar sellos de seguridad si se requieren.
- ☒ 13. Limpiar con gel espumoso teclado, ratón, pantalla, torre e impresora.
- ☒ 14. Entregar el equipo a satisfacción del usuario final.

Las observaciones y demás detalles relacionados con este formato deben ser informados en la mesa de servicios.

OBSERVACIONES DEL TÉCNICO:
Realizar backup. al ordenador cada 3 meses.

FIRMA DEL USUARIO
Recibe a satisfacción

Apéndice M. Lista de verificación para el mantenimiento lógico de computadores

	UNIVERSIDAD POPULAR DEL CESAR	CÓDIGO: 308-160-PRO04-FOR02
		VERSIÓN: 1
	CHECK LIST PARA EL MANTENIMIENTO LÓGICO DE COMPUTADORES PERSONALES	PÁG.: 1 de 1

FECHA:	14 - Diciembre - 2017	USUARIO:	Pedro M. Solano Y.
PLACA No.:	3630	OFICINA:	Sala Informática I

- [x] 1. Si el computador se conecta por red inalámbrica debe conectarse a una red administrativa de la Universidad.
- [x] 2. Revisar si la dirección IP, puerta de enlace, máscara y DNS que tiene el computador están dentro de los parámetros citados en el documento: inventario de direcciones IP por dependencia.
- [x] 3. Asegurarse que no exista duplicidad de dirección IP y verificar navegación.
- [ ] 4. Revisar que el computador tenga activo Symantec Endpoint Protection.
- [x] 5. Verificar que UAC (Control de cuentas de usuario) esté activado.
- [x] 6. Revisar el comportamiento del computador, aplicaciones de inicio, archivos ocultos y memorias USB para detectar actividades de virus, si se detectan proceder a desinfectar y reparar.
- [x] 7. Verificar que el computador tenga el último service pack y habilitadas las actualizaciones automáticas, si el computador utiliza congelador de disco las actualizaciones deben permanecer deshabilitadas, si en la sede donde está el computador hay servidor WSUS(Windows Server Update Services) el computador debe configurarse para que se conecte a WSUS y anotar fecha del update.
- [x] 8. Verificar que el equipo se encuentra asociado al dominio; de otra forma proceder a su respectiva asociación y a la entrega de usuario y contraseña al usuario final. Esto aplica para equipos administrativos.
- [x] 9. Verificar el servicio de impresión de archivos..
- [x] 10. Revisar el software instalado según el documento aplicaciones licenciadas. Proceder a desinstalar software no licenciado, toolbars y malware informando al usuario.
- [x] 11. Verificar que Microsoft Office esté activado y funcionando.
- [ ] 12. Instalar CCLeaner y con él realizar limpieza de archivos temporales, registro del sistema y deshabilitar aplicaciones innecesarias de inicio.
- [ ] 13. Instalar agente OCS, registrar placa, colocar nota del update de WSUS y asignar grupo.

Las observaciones y demás detalles relacionados con este formato deben ser informados en la mesa de servicios.

OBSERVACIONES DEL TÉCNICO:

FIRMA DEL USUARIO
Recibe a satisfacción